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

Математическое прикладное программное обеспечение для задач 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 во 2 семестре - в форме зачета, который направлен на оценку сформированности результатов обучения по дисциплине, соотнесенных с установленными в программе индикаторами достижения компетенций ОПК-5 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-5, 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 «Математическое прикладное программное обеспечение для задач защиты информации», 2 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 «Математическое прикладное программное обеспечение для задач 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-5 Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	1. знает современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы для решения профессиональных задач 3. умеет применять методы научных исследований в научной деятельности, в частности, при написании магистерской диссертации и научных статей 4. знает теоретические и эмпирические методы научных исследований

Вопросы теста для оценки сформированности компетенции ОПК-5

Вопрос 1. Современные системы шифрования можно разделить на два больших класса. Какие?
Ответ:

Решение: симметричные и ассиметричные.

Вопрос 2. К …… системам шифрования относятся такие системы, в которых для шифрования и для расшифрования используется один и тот же ключ

- ☐ **симметричным ✓**
- ☐ эллиптическим
- ☐ нейронным

(один вариант)

Вопрос 3. Какие шифры называются симметричными

Ответ:

Решение: используют один ключ для шифрования и расшифрования

Вопрос 4. Размер блока шифра AES (бит)

- ☐ **128 ✓**
- ☐ 64
- ☐ 32

(один вариант)

Вопрос 5. Какое количество наибольших общих делителей существует у пары чисел
Ответ:

Решение: одно

Вопрос 6. Найти две последние цифры чисел:17^61

- ☐ 3
- ☐ 2
- ☐ 5
- ☐ **17 ✓**

(один вариант)

[1] Правильные ответы выделены галочкой

Вопрос 7. Назовите теорему. Для любого простого p и любого a≥1, не делящегося на p, справедливо сравнение ap-1=1(mod p).

Ответ:

Решение: Теорема Ферма

Вопрос 8. Дискретный логарифм односторонней функции y = a^x(mod p) имеет вид:

- ☐ **x = logay(mod p) ✓**
- ☐ x = logpy(mod x)
- ☐ x = logpx(mod a)

(один вариант)

Вопрос 9. Найти результат выражения 3 mod 7

- ☐ 18
- ☐ 15
- ☐ **3 ✓**

(один вариант)

Вопрос 10. Как называется непустое множество A с набором операций?
Ответ:

Решение: алгебра.

Вопрос 11. Метод вычисления обратной функции «шаг младенца, шаг великана» при количестве десятичных знаков в записи p требует порядка … операций

- ☐ **2p^(1/2) ✓**
- ☐ p^p+1
- ☐ 2p^2

(один вариант)

Вопрос 12. Какие шифры называются одноалфавитными (моноалфавитными)?

Ответ:

Решение: используют один алфавит

Вопрос 13. 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 14. Функция Эйлера для m = p простое число, вычисляется по формуле

- ☐ **φ(p) = p−1 ✓**
- ☐ φ(p) = p
- ☐ φ(p) = p+1

(один вариант)

Вопрос 15. Являются ли сравнимыми по модулю пять числа 1 и -4
Ответ:

Решение: да

Вопрос 16. Дополните понятие коллизия. Коллизия - это ситуация, в которой для разных пар входных сообщений формируется ____ хэш- функция

Ответ:

Решение: одинаковая

Вопрос 17. Какая функция отображает электронные сообщения произвольной длины в значения фиксированной длины?

Ответ:

Решение: Хэш-функция

Вопрос 18. 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 19. Назовите первый криптографический алгоритм, который был основан на сложности разложения больших чисел на два исходных простых сомножителя

Ответ:

Решение: RSA

Вопрос 20. Какие шифры называются полиалфавитными (многоалфавитными)

Ответ:

Решение: используют более одного алфавита.

Вопрос 21. Дополните. Асимметричное шифрование — это метод шифрования данных, предполагающий использование двух ключей — ____ и _____

Ответ:

Решение: открытого, закрытого

Вопрос 22. 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 23. Размер ключа шифра ГОСТ 28147-89 (бит)

- ☐ 16
- ☐ 64
- ☐ 32
- ☐ **256** ✓

(один вариант)

Вопрос 24. Размер ключа шифра AES (бит)

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

(один вариант)

Вопрос 25. Как называется функция, для которой вычисление в одну сторону - простая задача, требующая немного времени, а вычисление обратной функции - задача сложная, требующая много лет вычислений?
Ответ:

Решение: односторонней

Вопрос 26. Дополните понятие алфавит. Алфавит А любого языка представляет собой множество упорядоченных кодов символов, обозначающих ____ этого языка
Ответ:

Решение: буквы

Вопрос 27. Вычислите 7 mod 11.
Ответ:

Решение: 7.

Вопрос 28. В каких единицах измеряется стойкость шифра по Шеннону
Ответ:

Решение: в битах

Вопрос 29. 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 30. Верно ли утверждение: хэш-функции классифицируют на ключевые и бесключевые?
Ответ:

Решение: да