МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Зам. директора по учебной работе
Пятигорского института (филиал)
СКФУ
Н.В. Данченко

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
Методы и средства криптографической защиты информации

Направление подготовки	**10.03.01 Информационная безопасность**
Направленность (профиль)	**Безопасность компьютерных систем**
Год начала обучения	2024
Форма обучения	очная
Реализуется в семестре	5 , 6

Введение

1. Назначение: для проверки знаний, умений и навыков текущего контроля и промежуточной аттестации.

2. ФОС является приложением к программе дисциплины Методы и средства криптографической защиты информации

3. Разработчик: Н.И. Битюцкая, доцент кафедры СУиИТ.

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель _____
(*Ф.И.О., должность*)

Члены комиссии: _____
(*Ф.И.О., должность*)

_____
(*Ф.И.О., должность*)

Представитель организации-работодателя _____
(*Ф.И.О., должность*)

Экспертное заключение:

_____

_____

«____»_____ 2024 г.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

1. Описание критериев оценивания компетенции на различных этапах их формирования, описание шкал оценивания

Компетенция (ии), индикатор (ы)	Уровни сформированности компетенци(ий),			
	Минимальный уровень не достигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
Компетенция: ОПК-3				
Результаты обучения по дисциплине: *Индикатор:* ИД-1.ОПК-3 Знает необходимые математические методы для решения задач обеспечения защиты информации.	Не знает необходимые математические методы для решения задач обеспечения защиты информации.	Недостаточно хорошо знает необходимые математические методы для решения задач обеспечения защиты информации.	Хорошо знает необходимые математические методы для решения задач обеспечения защиты информации.	Отлично знает необходимые математические методы для решения задач обеспечения защиты информации.
ИД-2.ОПК-3 Уметь: применять совокупность необходимых математических методов для решения задач обеспечения защиты информации	Не способен применять совокупность необходимых математических методов для решения задач обеспечения защиты информации	Недостаточно хорошо умеет применять совокупность необходимых математических методов для решения задач обеспечения защиты информации	Хорошо умеет применять совокупность необходимых математических методов для решения задач обеспечения защиты информации	Отлично умеет применять совокупность необходимых математических методов для решения задач обеспечения защиты информации
ИД-3.ОПК-3 Наделен навыками применения совокупности необходимых математических методов для решения задач обеспечения защиты информации.	Не владеет навыками применения совокупности необходимых математических методов для решения задач обеспечения защиты информации.	Недостаточно хорошо владеет навыками применения совокупности необходимых математических методов для решения задач обеспечения защиты информации.	Хорошо владеет навыками применения совокупности необходимых математических методов для решения задач обеспечения защиты	Отлично владеет навыками применения совокупности необходимых математических методов для решения задач обеспечения защиты информации.

			информации.	
Компетенция: ОПК-7				
Индикатор: ИД-1 ОПК-7 Знает языки программирования и системы разработки программных средств для решения профессиональных задач.	Не знает языки программирования и системы разработки программных средств для решения профессиональных задач.	Недостаточно хорошо знает языки программирования и системы разработки программных средств для решения профессиональных задач.	Хорошо знает языки программирования и системы разработки программных средств для решения профессиональных задач.	Отлично знает языки программирования и системы разработки программных средств для решения профессиональных задач.
ИД-2 ОПК-7 Способен выбирать необходимые языки программирования и системы разработки программных средств для решения профессиональных задач.	Не способен выбирать необходимые языки программирования и системы разработки программных средств для решения профессиональных задач.	Недостаточно хорошо умеет выбирать необходимые языки программирования и системы разработки программных средств для решения профессиональных задач.	Хорошо умеет выбирать необходимые языки программирования и системы разработки программных средств для решения профессиональных задач.	Отлично умеет выбирать необходимые языки программирования и системы разработки программных средств для решения профессиональных задач.
ИД-3 ОПК-7 Обладает навыками применения языков программирования и систем разработки программных средств для решения профессиональных задач.	Не обладает навыками применения языков программирования и систем разработки программных средств для решения профессиональных задач.	Имеет слабые навыки применения языков программирования и систем разработки программных средств для решения профессиональных задач.	Имеет хорошие навыки применения языков программирования и систем разработки программных средств для решения профессиональных задач.	Имеет отличные навыки применения языков программирования и систем разработки программных средств для решения профессиональных задач.
Компетенция: ОПК-9				
ИД-1 ОПК-9 Понимает корректность криптографических алгоритмов в	Не понимает корректность криптографических	Слабо понимает корректность криптографических алгоритмов	Хорошо понимает корректность криптографи	Отлично понимает корректность криптографич

современных программных комплексах. ИД-2 ОПК-9 Способен устанавливать причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям. ИД-3 ОПК-9 Владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	алгоритмов в современных программных комплексах. Не способен устанавливать причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям. Не владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	в современных программных комплексах. Недостаточно хорошо умеет устанавливать причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям. Недостаточно хорошо владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	ческих алгоритмов в современных программных комплексах. Хорошо умеет устанавливать причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям. Хорошо владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	еских алгоритмов в современных программных комплексах. Отлично умеет устанавливать причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям. Отлично владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.

Оценивание уровня сформированности компетенции по дисциплине осуществляется на основе «Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры - в федеральном государственном автономном образовательном учреждении высшего образования «Северо-Кавказский федеральный университет» в актуальной редакции.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		Форма обучения <u>очная</u> Семестры <u>5-6</u>	
1.	a	Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования: a) 1 b) 2 c) 3	ПК-2
2.	c	Что принято называть электронной подписью? a) зашифрованный текст b) текст c) присоединяемое к тексту его криптографическое преобразование	ОПК-3
3.	c	Выберите то, что используют для создания цифровой подписи: a) закрытый ключ получателя b) открытый ключ отправителя c) закрытый ключ отправителя d) открытый ключ получателя	ОПК-7
4.	a	Выберите то, что лучше всего описывает цифровую подпись: a) это метод переноса собственноручной подписи на электронный документ b) это метод шифрования конфиденциальной информации c) это метод, позволяющий получателю сообщения проверить его источник и убедиться в целостности сообщения	ОПК-9
5.	a	Количество раундов, выполняемых в DES: a) 16 b) 32 c) 64	ОПК-3
6.	b	В каком алгоритме символы оригинального текста меняются местами по определенному алгоритму, задаваемому секретным ключом? a) в алгоритме подстановки b) в алгоритме перестановки c) в алгоритме гаммирования	ОПК-7

7.	c	Выберите то, что указывает на изменение сообщения: a) изменился открытый ключ b) изменился закрытый ключ c) изменилась хэш-функция сообщения	ОПК-9
8.		Сформулируйте принцип Керкгоффса.	ОПК-3
9.		Дайте определение шифра с симметричным ключом.	ОПК-7
10.		Дайте определение шифра с симметричным ключом.	ОПК-9
11.		Как противостоять атаке грубой силы?	ОПК-3
12.		Как противостоять статистической атаке?	ОПК-7
13.		Поясните отличия между шифром подстановки (замены) и шифром перестановки.	ОПК-9
14.		Поясните отличия между моноалфавитными и многоалфавитными шифрами.	ОПК-3
15.		Перечислите основные компоненты современного блочного шифра.	ОПК-7
16.		Укажите различие между блочным шифром Фейстеля и не-Фейстеля.	ОПК-9
17.		Каков размер блока в DES?	ОПК-3
18.		Каков размер ключа шифра в DES?	ОПК-7
19.		В чем основное отличие детерменированных и вероятностных алгоритмов проверки чисел на простоту.	ОПК-9
20.		Приведите примеры вероятностных алгоритмов проверки чисел на простоту.	ОПК-3
21.		Как повысить вероятность правильного ответа при использовании теста Ферма проверки числа на простоту?	ОПК-7
22.		Какие алгоритмы проверки чисел на простоту являются эффективными, а какие нет?	ОПК-9
23.		Дайте определение односторонней функции.	ОПК-3
24.		Перечислите секретные параметры системы *RSA*.	ОПК-7
25.		Перечислите открытые параметры системы RSA.	ОПК-9
26.		Дайте определение хэш-функции.	ОПК-3
27.		Перечислите российские стандарты цифровой подписи.	ОПК-7
28.		Какие задачи позволяет решить цифровая подпись?	ОПК-9

2. Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации. Рейтинговая система оценки знаний студентов основана на использовании совокупности контрольных мероприятий по проверке пройденного материала (контрольных точек), оптимально расположенных на всем временном интервале изучения дисциплины. Принципы рейтинговой системы оценки знаний студентов основываются на положениях, описанных в Положении об организации образовательного процесса на основе рейтинговой системы оценки знаний студентов в ФГАОУ ВО «СКФУ».

Рейтинговая система оценки не предусмотрена для студентов, обучающихся на образовательных программах уровня высшего образования магистратуры, для обучающихся на образовательных программах уровня высшего образования бакалавриата заочной и очно-заочной формы обучения.

3. Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если теоретическое содержание курса освоено полностью, без пробелов; исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует в ответе дополнительный материал, все предусмотренные программой задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному; анализирует полученные результаты; проявляет самостоятельность при выполнении заданий.

Оценка «хорошо» выставляется студенту, если теоретическое содержание курса освоено полностью, необходимые практические компетенции в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.

Оценка «удовлетворительно» выставляется студенту, если теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, большинство предусмотренных программой заданий выполнено, но в них имеются ошибки, при ответе на поставленный вопрос студент допускает неточности, недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении программного материала.

Оценка «неудовлетворительно» выставляется студенту, если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, необходимые практические компетенции не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, качество их выполнения оценено числом баллов, близким к минимальному.