

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Грובה Татьяна Анатольевна

Должность: и.о. декана факультета математики и компьютерных наук имени
профессора Н.И. Червякова

Дата подписания: 19.06.2026 15:16:51

Уникальный программный ключ:

bd39d4208aa94cf4422feb787c81619d42de79a7

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета

математики и компьютерных наук
имени профессора Н.И. Червякова,
кандидат физико-математических
наук, доцент Грובה Т.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

Математическое и программное обеспечение защиты информации

Направление подготовки	01.04.02 Прикладная математика и информатика
Направленность (профиль)	Математическое моделирование
Форма обучения	очная
Год начала обучения	2026
Реализуется в	2 семестре

Введение

1. Назначение: ФОС предназначен для объективной оценки уровня сформированности компетенций.
2. ФОС является приложением к программе дисциплины (модуля) «Математическое и программное обеспечение защиты информации»
3. Разработчик Ионисян А.С., доцент кафедры математического моделирования.
4. Проведена экспертиза ФОС.
Члены экспертной группы:
Председатель Ляхов П.А., зав. кафедрой математического моделирования
Члены комиссии: Андрухив Л.В., доцент кафедры математического моделирования,
Журавлева И.А., доцент кафедры математического моделирования.
Представитель организации-работодателя Подопригора Н.Б., генеральный директор ООО «медицина ИТ»

Экспертное заключение
ФОС по дисциплине позволяет оценить уровень сформированности компетенций.
Приступить к апробации.
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 (Неудовлетво- рительно) 2 балла	Минимальн ый уровень (удовлетво- рительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
<i>Компетенция: ПК-7</i>				
<i>Индикатор ИД-1:</i> Проводит рецензирование научных статей, авторефератов и диссертаций, составление научных обзоров, рефератов и библиографии с использованием цифровых средств.	не знает методы рецензирования научных статей, авторефератов и диссертаций, составления научных обзоров, рефератов и библиографии с использованием цифровых средств	удовлетвори тельно знает методы рецензирова ния научных статей, автореферат ов и диссертаций , составления научных обзоров, рефератов и библиограф ии с использован ием цифровых средств	хорошо знает методы рецензирования научных статей, авторефератов и диссертаций, составления научных обзоров, рефератов и библиографии с использованием цифровых средств	отлично знает методы рецензирования научных статей, авторефератов и диссертаций, составления научных обзоров, рефератов и библиографии с использованием цифровых средств
<i>Индикатор ИД-2:</i> Решает задачи профессиональной деятельности с использованием цифровых средств и алгоритмов обработки данных	не умеет решать задачи профессиональн ой деятельности с использованием цифровых средств и алгоритмов обработки данных	удовлетвори тельно умеет решать задачи профессиона льной деятельност и с использован ием цифровых средств и алгоритмов обработки данных	хорошо умеет решать задачи профессиональн ой деятельности с использованием цифровых средств и алгоритмов обработки данных	отлично умеет решать задачи профессиональн ой деятельности с использованием цифровых средств и алгоритмов обработки данных
<i>Индикатор ИД-3:</i> Занимается подготовкой научных и научно-	Не умеет заниматься подготовкой научных и научно-	Удовлетвори тельно умеет заниматься подготовкой научных и	Хорошо умеет заниматься подготовкой научных и научно-	Отлично умеет заниматься подготовкой научных и научно-

технических публикаций по тематике проводимых исследований	технических публикаций по тематике проводимых исследований	научно-технических публикаций по тематике проводимых исследований	технических публикаций по тематике проводимых исследований	технических публикаций по тематике проводимых исследований
--	--	---	--	--

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 - очная, Семестр - 2	
1.	a	Современные проблемы информационной безопасности a: актуальны b: не актуальны c: таких проблем не существует	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
2.	создания шифров	Основные понятия криптографии нацелены на решение задач «раскрытия шифров» «создания шифров» _____ (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
3.	раскрытия шифров	Основные понятия криптологии нацелены на решение задач «раскрытия шифров» «создания шифров» _____ (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
4.	Высшей алгебры	Модулярная арифметика – это раздел «Математического анализа» «Аналитической геометрии» «Высшей алгебры» _____ (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
5.	Создания новых шифров	Криптографические алгоритмы применяются для «Создания новых шифров» «Создания теорем математической логики» «Распознавания графических образов» _____ (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
6.	одинаковый ключ для шифрования и дешифрования	симметричные шифры используют «одинаковый ключ для шифрования и дешифрования» «разные ключи для шифрования и дешифрования» _____ (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
7.	DES	симметричный шифр «RSA»	ИД-2 ПК7 ИД-1 ПК7

		«DES» «DSA» (впечатать правильный вариант без кавычек)	ИД-3 ПК7
8.	разные ключи для шифрования и дешифрования	Асимметричные шифры используют «одинаковый ключ для шифрования и дешифрования» «разные ключи для шифрования и дешифрования» (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
9.	RSA	асимметричный шифр «RSA» «DES» «шифр Шеннона» (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
10.	обладают абсолютной стойкостью к взлому	Сильные симметричные шифры «обладают абсолютной стойкостью к взлому» «никак не защищены от взлома» «абсолютная стойкость к взлому симметричных шифров не доказана» (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
11.	открытую часть ключа	Алгоритм RSA использует для шифрования «открытую часть ключа» «закрытую часть ключа» (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
12.	закрытую часть ключа	Алгоритм RSA использует для дешифрования «открытую часть ключа» «закрытую часть ключа» (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
13.	абсолютная стойкость к взлому асимметричных алгоритмов не доказана	Сильные асимметричные алгоритмы шифрования «обладают абсолютной стойкостью к взлому» «никак не защищены от взлома» «абсолютная стойкость к взлому асимметричных алгоритмов не доказана» (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
14.	закрытую часть ключа	электронная цифровая подпись использует для шифрования «открытую часть ключа» «закрытую часть ключа»	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7

		(впечатать правильный вариант без кавычек)	
15.	открытую часть ключа	электронная цифровая подпись использует для дешифрования «открытую часть ключа» «закрытую часть ключа» (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
16.	извлечения корня в конечных полях	криптографический алгоритм Рабина основан на сложности решения задачи «извлечения корня в конечных полях» «сложения чисел в конечных полях» «поиска обратного мультипликативного элемента в конечных полях» (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
17.	полиномиальное время	Квантовые криптографические алгоритмы позволяют решить задачу факторизации числа за «полиномиальное время» «факториальное время» «экспоненциальное время» (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
18.	на квантовых ЭВМ и на обычных ЭВМ	Постквантовые криптографические алгоритмы позволяют создавать шифры, сложные для взлома «исключительно на квантовых ЭВМ» «исключительно на обычных ЭВМ» «на квантовых ЭВМ и на обычных ЭВМ» (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
19.	доказательствах с нулевым разглашением	протокол Фиата-Шамира основан на «симметричном шифровании» «асимметричном шифровании» «доказательствах с нулевым разглашением» (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
20.	хорошо распараллеливается	Операция сложения в модулярной арифметике «хорошо распараллеливается» «является немодульной» (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
21.	хорошо распараллеливается	Операция вычитания в модулярной арифметике «хорошо распараллеливается»	ИД-2 ПК7 ИД-1 ПК7

		«является немодульной» (впечатать правильный вариант без кавычек)	ИД-3 ПК7
22.	хорошо распараллеливается	Операция умножения в модулярной арифметике «хорошо распараллеливается» «является немодульной» (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
23.	является немодульной	Операция деления в модулярной арифметике «хорошо распараллеливается» «является немодульной» (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
24.	является немодульной	Операция сравнения чисел в модулярной арифметике «хорошо распараллеливается» «является немодульной» (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
25.	расширенный алгоритм Евклида	Для поиска обратного мультипликативного элемента можно использовать «алгоритм Евклида» «расширенный алгоритм Евклида» «алгоритм Кузнецик» (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
26.	ГОСТ	Российский алгоритм шифрования данных называется «DES» «RSA» «ГОСТ» (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
27.	DES	Американский алгоритм шифрования данных называется «DES» «RSA» «ГОСТ» (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
28.	асимметричным шифрам	Шифрование на эллиптических кривых относится к «симметричным шифрам» «асимметричным шифрам» (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7

29.	постквантовым методам шифрования	Криптография на решетках относится к «постквантовым методам шифрования» «классическим методам шифрования» _____ (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
30.	за факториальное время	Вычислительно сложной считается задача, решаемая за «полиномиальное время» «линейное время» «факториальное время» _____ (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
31.	экспоненциальное время	Вычислительно сложной считается задача, решаемая за «полиномиальное время» «линейное время» «экспоненциальное время» _____ (впечатать правильный вариант без кавычек)	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7
32.	а	Популярной свободно распространяемой программой создания и проверки электронной цифровой подписи является а) GNU GPG б) Microsoft Word в) Adobe Photoshop	ИД-2 ПК7 ИД-1 ПК7 ИД-3 ПК7

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 требованиях, описанных в Положении об организации образовательного процесса на основе рейтинговой системы оценки знаний студентов в ФГАОУ ВО «СКФУ».

3. Критерии оценивания компетенций*

Оценка **«отлично»** выставляется студенту, если он показывает глубокие и всесторонние знания предмета, аргументировано и логически стройно излагает материал; *умеет* безошибочно и логически обосновать точку зрения; уверенно *владеет* методическими понятиями и принятой символикой.

Оценка **«хорошо»** выставляется студенту, если он показывает твердые знания предмета, аргументировано излагает материал;

умеет применять знания для анализа конкретных ситуаций, но при этом незначительно нарушает последовательность изложения материала, дает недостаточно полное, хотя и верное определение понятий;

владеет основными методическими понятиями и символикой.

Оценка **«удовлетворительно»** выставляется студенту, если он в основном *знает* предмет, но программный материал излагает фрагментарно и непоследовательно;

умеет практически применять свои знания, допускает отдельные ошибки и погрешности при решении задач;

неуверенно *владеет* основными математическими понятиями и применением математической символики.

Оценка **«неудовлетворительно»** выставляется студенту, если он не достаточно усвоил основного содержания предмета и обнаруживает *незнание* большей части учебного материала, допускает грубые ошибки при формулировании определений и понятий;

не достаточно умеет логически обоснованно анализировать и решать практические задачи;

не достаточно владеет математической символикой и ее грамотным применением.