

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Грובה Татьяна Александровна

Должность: и.о. декана факультета математики и компьютерных наук имени

профессора Н.И. Червякова

Дата подписания: 19.06.2026 15:22:53

Уникальный программный ключ:

bd39d4208aa94cf4422feb787c81619a428c79a7

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
Грובה Т.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Криптоанализ с помощью программных средств

Направление подготовки
Направленность (профиль)

Форма обучения
Год начала обучения
Реализуется в 3 семестре

10.04.01 Информационная безопасность
Математическое и программное обеспечение
защиты информации
очная
2026

Введение

1. Назначение: обеспечение методической основы для организации и проведения текущего контроля по дисциплине «Криптоанализ с помощью программных средств». Текущий контроль по данной дисциплине – вид систематической проверки знаний, умений, навыков студентов. Задачами текущего контроля являются получение первичной информации о ходе и качестве освоения компетенций, а также стимулирование регулярной целенаправленной работы студентов. Для формирования определенного уровня компетенций.

2. ФОС является приложением к программе дисциплины «Криптоанализ с помощью программных средств»

3. Разработчик: Калмыков И.А., профессор кафедры вычислительной математики и кибернетики

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель: Петренко В.И., зав. кафедрой организации и технологии защиты информации.

Члены комиссии: Жук А.П., профессор кафедры организации и технологии защиты информации.

Рачков В.Е., доцент кафедры организации и технологии защиты информации.

Представитель организации-работодателя: Березницкий А.С., кандидат экономических наук, главный аналитик ФБУ «Северо-Кавказского регионального центра судебной экспертизы Министерства юстиции РФ» ФГБУ Кабардино-Балкарской лаборатории судебной экспертизы Министерства юстиции Российской Федерации.

Экспертное заключение: Представленный ФОС по дисциплине «Криптоанализ с помощью программных средств» соответствует требованиям ФГОС ВО. Предлагаемые преподавателем формы и средства текущего контроля адекватны целям и задачам реализации образовательной программы высшего образования по направлению 10.04.01 Информационная безопасность направленность (профиль) «Математическое и программное обеспечение защиты информации», а также целям и задачам рабочей программы реализуемой учебной дисциплины. Оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации представлены в полном объеме.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

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

Уровни сформированности компетенци(ий), индикатора (ов)	Дескрипторы			
	Минимальный уровень не достигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
ИД-3 УК-5 выбирает способы конструктивного взаимодействия с людьми с учетом их социокультурных особенностей в целях успешного выполнения профессиональных задач и усиления социальной интеграции	Делает грубые ошибки при выборе способов конструктивного взаимодействия с людьми с учетом их социокультурных особенностей в целях успешного выполнения профессиональных задач и усиления социальной интеграции	С помощью преподавателя выбирает способы конструктивного Взаимодействия людьми с учетом их социокультурных особенностей в целях успешного выполнения профессиональных задач и усиления социальной интеграции	выбирает способы конструктивного взаимодействия с людьми с учетом их социокультурных особенностей в целях успешного выполнения профессиональных задач и усиления социальной интеграции	Самостоятельно и творчески выбирает способы конструктивного взаимодействия с людьми с учетом их социокультурных особенностей в целях успешного выполнения профессиональных задач и усиления социальной интеграции
ИД-1 УК-6 Устанавливает личные и профессиональные цели в соответствии с уровнем своих ресурсов и приоритетов действий, для успешного развития в избранной сфере профессиональной деятельности	Делает грубые ошибки в личных и профессиональных целях в соответствии с уровнем своих ресурсов и приоритетов действий, для успешного развития в избранной сфере профессиональной деятельности	С помощью преподавателя устанавливает личные и профессиональные цели в соответствии с уровнем своих ресурсов и приоритетов действий, для успешного развития в избранной сфере профессиональной деятельности	Устанавливает личные и профессиональные цели в соответствии с уровнем своих ресурсов и приоритетов действий, для успешного развития в избранной сфере профессиональной деятельности	Самостоятельно и творчески устанавливает личные и профессиональные цели в соответствии с уровнем своих ресурсов и приоритетов действий, для успешного развития в избранной сфере профессиональной деятельности
ИД-2 УК-6 реализует и корректирует стратегию своего личностного и профессионального развития с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда	Делает грубые ошибки в реализации и корректировке стратегии своего личностного и профессионального развития с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы	С помощью преподавателя реализует и корректирует стратегию своего личностного и профессионального развития с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда	реализует и корректирует стратегию своего личностного и профессионального развития с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда	Самостоятельно и творчески реализует и корректирует стратегию своего личностного и профессионального развития с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда

ИД-3 УК-6 критически оценивает эффективность использования своего времени и других ресурсов при решении задач, поставленных в избранной сфере профессиональной деятельности	эффективности использования своего времени и других ресурсов при решении задач, поставленных в избранной сфере профессиональной деятельности	оценивает эффективность использования своего времени и других ресурсов при решении задач, поставленных в избранной сфере профессиональной деятельности	использования своего времени и других ресурсов при решении задач, поставленных в избранной сфере профессионально й деятельности	оценивает эффективность использования своего времени и других ресурсов при решении задач, поставленных в избранной сфере профессиональной деятельности
--	---	---	---	--

Оценочные средства для проверки уровня сформированности компетенций

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
1.		Принципы создания блочных шифров. Рассеивание и перемешивание.	УК-5
2.		Подстановки и перестановки. Сети Файстеля.	УК-5
3.		Архитектура «квадрат».	УК-5
4.		Алгоритмы разворачивания ключа.	УК-5
5.		Протокол Ко-Ли.	УК-5
6.		Протокол Ванга-Као.	УК-5
7.		Протокол Шпильрайна-Ушакова.	УК-5
8.		Конечные автоматы на полурешетках.	УК-5
9.		Алгебраическое шифрование.	УК-5
10.		Группы кос Артина.	УК-6
11.		Метод Аштель-Аштеля-Гольдфельда.	УК-6
12.		Дифференциальный криптоанализ.	УК-6
13.		Линейный криптоанализ.	УК-6
14.		Сильные и слабые S-блоки. Методы анализа S-блоков. Бент-функции.	УК-6
15.		Базис Грёбнера.	УК-6
16.		Принципы создания поточных шифров. Псевдослучайные последовательности.	УК-6
17.	алгоритмом	Впишите пропущенное слово в нужном падеже. _____ называется детерминированным, если после фиксированного числа шагов (операций над элементами конечного множества) результат работы данного алгоритма всегда является решением поставленной задачи.	УК-6
18.		Определение функции Мёбиуса. Доказать ее мультипликативность. Связь теоретико-числовой функции и функции Мёбиуса.	УК-6
19.		Понятие и свойства сравнения. Вычеты. Полная система вычетов. Полная система наименьших неотрицательных вычетов. Полная система абсолютно наименьших вычетов. Лемма о двух полных системах вычетов.	УК-6
20.		Определение функции Эйлера. Лемма и теорема о вычислении значения функции Эйлера. Доказать мультипликативность функции Эйлера	УК-6

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».

Рейтинговая система оценки не предусмотрено 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 студент показал глубокое, прочное и аргументированное знание программного учебного материала дисциплины, при этом поставленные вопросы раскрывает последовательно, четко и логически стройно, в полном исчерпывающем объеме; умеет правильно формулировать, и владеет основными категориями, понятиями и терминами по материалам дисциплины, не допускает при ответе ошибок, владеет инновационными приемами работы. Если он проявил самостоятельность, организованность, добросовестность творческий подход при подготовке доклада, выраженное стремление к приобретению и совершенствованию профессиональных знаний, умений и навыков.

Оценка «хорошо» выставляется студенту в случае, когда студент в основном знает программный учебный материал дисциплины, поставленные в докладе вопросы раскрывает последовательно, четко и логически стройно, но допускает незначительные неточности. Умеет правильно формулировать, и владеет основными категориями, понятиями и терминами по материалам доклада, однако допускает при ответе отдельные неточности или одну, две ошибки; не отличался инициативностью, высокой активностью, творческим подходом и самостоятельностью в выполнении доклада. В основном владеет инновационными приемами работы.

Оценка «удовлетворительно» выставляется студенту за: наличие поверхностных знаний, неустойчивых умений в области профессиональной деятельности; дает не полные ответы на поставленные в докладе вопросы, показал слабое владение инновационными приемами работы; отсутствие должностной инициативности, самостоятельности и творчества при подготовке доклада.

Оценка «неудовлетворительно» выставляется, если студент допускает грубые ошибки при ответе на вопросы по докладу, знает на недостаточно высоком уровне материал доклада и не в полной мере готов по подготовленному докладу