

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 15:45:29

Уникальный программный ключ:

bd39d4208aa94cf4422feb787c81619d42de79a7

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

УТВЕРЖДАЮ

И.о. декана факультета математики
и компьютерных наук имени
профессора Н.И. Червякова
_____ Грובה Т.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Методы и средства криптографической защиты информации

Специальность	<u>10.05.01 Компьютерная безопасность</u>
Специализация	<u>Информационно-аналитическая и техническая экспертиза компьютерных систем</u>
Год начала обучения	<u>2026</u>
Форма обучения	<u>очная</u>
Реализуется в семестре	<u>5, 6</u>

Введение

1. Назначение: обеспечение методической основы для организации и проведения текущего контроля по дисциплине «Методы и средства криптографической защиты информации». 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 (модуля) «Методы и средства криптографической защиты информации»

Разработчик: Петросян С.М., старший преподаватель кафедры вычислительной математики и кибернетики

3. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель Тебуева Ф.Б., профессор кафедры вычислительной математики и кибернетики

Члены комиссии: Осипов Д.Л., доцент кафедры вычислительной математики и кибернетики
Гусева Л.Л., кафедры вычислительной математики и кибернетики

Представитель организации-работодателя: Березницкий А.С., заместитель директора ФБУ «Северо-Кавказский региональный центр судебной экспертизы Министерства юстиции РФ».

Экспертное заключение: Представленный ФОС по дисциплине «Методы и средства криптографической защиты информации» соответствует требованиям ФГОС ВО. Предлагаемые преподавателем формы и средства текущего контроля адекватны целям и задачам реализации образовательной программы высшего образования по специальности 10.05.01 Компьютерная безопасность, 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 и компетенции(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
<i>Компетенция: ОПК-10</i>				
Результаты обучения по дисциплине (модулю): <i>Индикатор: ИД-1 ОПК-10</i>	С грубыми ошибками решает задачи проектирования защищенных компьютерных систем с использованием криптографических методов	На минимальном уровне решает задачи проектирования защищенных компьютерных систем с использованием криптографических методов	На среднем уровне решает задачи проектирования защищенных компьютерных систем с использованием криптографических методов	На высоком уровне решает задачи проектирования защищенных компьютерных систем с использованием криптографических методов

Оценочные средства для проверки уровня сформированности компетенций 5 семестр

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
1	перестановочным	Впишите пропущенное слово в нужном падеже. Шифр называется _____, если все связанные с ним криптограммы получаются из соответствующих открытых текстов перестановкой букв.	ОПК-3
2	шифров замены	Впишите пропущенное слово в нужном падеже. Класс _____ выделяется тем свойством, что для получения криптограммы отдельные символы или группы символов исходного алфавита заменяются символами или группами символов шифроалфавита.	ОПК-3
3	открытый текст	Впишите пропущенное слово в нужном падеже. Информация считается представленной в виде некоторого текста (сообщения). Это – _____	ОПК-3
4		Шифросистема Эль-Гамала. Стойкость.	ОПК-3
5		Алгоритм симметричного шифрования DES.	ОПК-3
6		Алгоритм симметричного шифрования ГОСТ 28147-99.	ОПК-3
7		Алгоритм симметричного шифрования Rijndael.	ОПК-3
8		Алгоритмы симметричного шифрования IDEA и Blowfish.	ОПК-3
9		Режимы выполнения алгоритмов симметричного шифрования.	ОПК-3
10		Поточные криптосистемы. Принципы построения. Классификация. Проблема синхронизации.	ОПК-3
11		Линейные конгруэнтные генераторы. Линейные регистры сдвига.	ОПК-3

12		Поточные шифры. Отличия от блочных. Стойкость. Методы анализа.	ОПК-3
13		Виды атак на криптографические алгоритмы. Понятие стойкости.	ОПК-3
14		Классификация алгоритмов шифрования. Примеры простейших шифров.	ОПК-3
15		Шифры замены. Математическая модель. Примеры.	ОПК-3

Оценочные средства для проверки уровня сформированности компетенций 6 семестр

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
1		Атаки на функции хэширования.	ОПК-3
2		Функция хеширования MD5.	ОПК-3
3		Функция хеширования SHA-1.	ОПК-3
4		Функция хеширования ГОСТ 3411-94.	ОПК-3
5		Ключевая информация: сеансовый, секретный, мастер-ключ, открытый и закрытый ключ. Требования к качеству ключевой информации и источнику ключей.	ОПК-3
6		Распределение секретных ключей. Обмен ключами по Диффи-Хельмана.	ОПК-3
7		Криптосистемы RSA и Эль-Гамала.	ОПК-3
8		Криптографические функции аутентификации.	ОПК-3
9		Сертификаты открытых ключей. Распределение сертификатов открытых ключей.	ОПК-3
10		Электронная подпись: требования предъявляемые к электронной подписи, непосредственная и арбитражная цифровая подпись, групповая электронная подпись.	ОПК-3
11		Ключевая информация: сеансовый, секретный, мастер-ключ, открытый и закрытый ключ. Требования к качеству ключевой информации и источнику ключей.	ОПК-3
12		Распределение секретных ключей. Обмен ключами по Диффи-Хельмана.	ОПК-3
13		Криптосистемы RSA и Эль-Гамала.	ОПК-3
14	Шифром шифрованием,	Впишите пропущенное слово в нужном падеже. Способ преобразования слова в защищенную форму называется _____, процесс применения шифра _____	ОПК-3
15	криптограммой	Впишите пропущенное слово в нужном падеже. Полученный в результате шифрования измененный текст называется _____	ОПК-3

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, если студент на высоком уровне использует математические методы для решения типовых прикладных задач; разрабатывает, обосновывает и реализовывает решения задач профессиональной деятельности на основании математических методов и моделей

Оценка «хорошо» выставляется, если студент на среднем уровне использует математические методы для решения типовых прикладных задач; разрабатывает, обосновывает и реализовывает решения задач профессиональной деятельности на основании математических методов и моделей

Оценка «удовлетворительно» выставляется, если студент на минимальном уровне использует математические методы для решения типовых прикладных задач; разрабатывает, обосновывает и реализовывает решения задач профессиональной деятельности на основании математических методов и моделей

Оценка «удовлетворительно» выставляется, если студент с грубыми ошибками использует математические методы для решения типовых прикладных задач; разрабатывает, обосновывает и реализовывает решения задач профессиональной деятельности на основании математических методов и моделей