«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зав. кафедрой ИБСиТ
_____ В.Ф. Антонов
«____» _____ 202_ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущей и промежуточной аттестации

По дисциплине	Б1.В.ДВ.04.01 «Математические основы криптологии»
Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль)	Комплексная защита объектов информатизации
Квалификация выпускника	бакалавр
Форма обучения	очная
Год начала обучения	2020 г

	Астр. часов	Акад. часов	
Объем занятий: Итого	81,0 ч.	108 ч.	3 з.е.
В том числе аудиторных	48,0 ч.	64 ч.	
Из них:			
Лекций	24,0 ч.	32 ч.	
Лабораторных работ	12,0 ч.	16 ч.	
Практических занятий	12,0 ч.	16 ч.	
Самостоятельной работы	33,0 ч.	44 ч.	
Зачет с оценкой в 4 семестре	____ч.	__ ч..	

Дата разработки:

Предисловие

1. Фонд оценочных средств предназначен для проверки знаний, умений и навыков при проведении текущего и промежуточного контроля.

2. Фонд оценочных средств текущего контроля и промежуточной аттестации на основе рабочей программы дисциплины, составлен в соответствии с образовательной программой по направлению подготовки 10.03.01 Информационная безопасность, утвержденной на заседании учебно-методического совета ФГАОУ ВО «СКФУ» протокол № 1 от «29» сентября 2020 г.

3. Разработчик _____ Битюцкая Н.И.., доцент кафедры ИБСиТ

4. ФОС рассмотрен и утвержден на заседании кафедры информационной безопасности, систем и технологий Протокол № 2 от «4» сентября 2020г.

5. ФОС согласован с выпускающей кафедрой кафедры информационной безопасности, систем и технологий Протокол № 2 от «4» сентября 2020г.

6. Проведена экспертиза ФОС. Члены экспертной группы, проводившие внутреннюю экспертизу:
Председатель_____ Антонов В.Ф.
_____ Мишин В.В.
_____ Сорокин И.Д.

Экспертное заключение: данные оценочные средства соответствует требованиям федерального государственного образовательного стандарта высшего образования, рекомендуются для использования в учебном процессе.
«____»_____

_____(подпись)

7. Срок действия ФОС один год.

Паспорт фонда оценочных средств
для проведения текущей и промежуточной аттестации

По дисциплине	Б1.В.ДВ.04.01 «Математические основы криптологии»
Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль)	Комплексная защита объектов информатизации
Квалификация выпускника	бакалавр
Форма обучения	очная
Год начала обучения	2020

Код оцениваемой компетенции (или её части)	Модуль, раздел, тема (в соответствии с Программой)	Тип контроля	Вид контроля	Компонент фонда оценочных средств	Количество заданий для каждого уровня, шт.	
					Базовый	Повышенный
4 семестр						
ОПК-2, ОПК-4, ПСК-3 ПСК-5	Темы 1 - 8	текущий	устный	Вопросы для собеседования	42	17
	Темы 2, 3, 5 - 8	текущий	письменный	Темы индивидуальных заданий для лабораторных работ	11	4
	Темы 2 - 9, 11 - 12	текущий	письменный	Темы индивидуальных заданий для практических занятий	12	5

Составитель _____ Битюцкая Н.И.
(подпись)

«____»_____20 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зав. кафедрой ИБСиТ

_____ В.Ф. Антонов

«____» _____ 202_ г.

Вопросы для собеседования

по дисциплине «Математические основы криптологии»

4 семестр

Базовый уровень

Тема 1. Основные понятия и термины криптографии.
1. Методы защиты информации.
2. Криптография и криптоанализ.
3. Понятие шифра и ключа.
4. Симметричные и ассиметричные алгоритмы шифрования.

Тема 2. Основы теории делимости.
1. Основные понятия теории делимости целых чисел.
2. Алгоритм Евклида нахождения наибольшего общего делителя.
3. Расширенный алгоритм Евклида.

Тема 3. Модульная арифметика.
1. Операции по модулю. Система вычетов.
2. Сравнение по модулю. Свойства оператора mod.
3. Аддитивная и мультипликативная инверсии чисел.

Тема 4. Матрицы вычетов.
1. Определение матрицы вычетов.
2. Операции над матрицами вычетов.

Тема 5. Проверка чисел на простоту.
1. Способы проверки на простое число.
2. Решето Эратосфена.
3. Phi-функция Эйлера.
4. Простые числа Мерсенны.
5. Простые числа Ферма.

Тема 6. Алгоритмы генерации простых чисел.
1. Генераторы псевдослучайных чисел.
2. Детерминированные алгоритмы проверки чисел на простоту.

Тема 7. Разложение чисел на простые множители.
1. Основная теорема арифметики.
2. Приложения разложения на множители.
3. Алгоритмы разложения на множители: метод проверки делением, метод Ферма.

Тема 8. Китайская теорема об остатках.
1. Китайская теорема об остатках.
2. Решение систем линейных уравнений с модулями. Примеры практических задач.

Тема 9. Алгебраические основы криптологии.
1. Группы, кольца, поля, их определения и виды.
Тема 10. Эллиптические кривые.
1. Эллиптические кривые в вещественных числах.
2. Эллиптические кривые в GF(p).
Тема 11. Классификация криптосистем.
1. Классификация классических шифров: шифры замены и перестановки.
2. Поточные и блочные шифры.
3. Моноалфавитные и многоалфавитные шифры.
Тема 12. Классические шифры замены.
1. Классические шифры с симметричным ключом.
2. Шифры замены: аддитивные, мультипликативные, аффинные.
Тема 13. Классические шифры перестановки.
1. Бесключевой шифр.
2. Ключевые шифры.
3. Шифры с двойной перестановкой.
Тема 14. Современные блочные шифры с симметричным ключом.
1. Различия между современными и традиционными шифрами с симметричным ключом.
2. Современные блочные шифры: шифры замены и шифры перестановки.
Тема 15. Современные шифры с асимметричным ключом.
1. Концепция криптографии с открытым ключом.
Тема 16. Сложность криптографических алгоритмов.
1. Понятие сложности алгоритма.
2. Линейная, полиномиальная и неполиномиальная сложность.
3. Класс NP – полных задач.
4. Способы определения сложности алгоритмов.

Повышенный уровень

Тема 1. Основные понятия и термины криптографии.
1. Симметричные и ассиметричные алгоритмы шифрования.
Тема 2. Основы теории делимости.
1. Решение линейных диофантовых уравнений.
Тема 3. Модульная арифметика.
1. Применение расширенного алгоритма Евклида для нахождения мультипликативной инверсии.
2. Решение уравнений с одним неизвестным, содержащих сравнение.
Тема 4. Матрицы вычетов.
1. Решение систем уравнений, содержащих сравнения.
Тема 5. Проверка чисел на простоту.
1. Теорема Ферма.
2. Теорема Эйлера.
Тема 6. Алгоритмы генерации простых чисел.
1. Вероятностные алгоритмы проверки чисел на простоту.
Тема 7. Разложение чисел на простые множители.
1. Алгоритмы разложения на множители: метод PO (Rho) Полларда.
Тема 8. Китайская теорема об остатках.
1. Примеры практических задач на применение китайской теоремы об остатках.
Тема 9. Алгебраические основы криптологии.
1. Полиномы над структурой.
Тема 10. Эллиптические кривые.
1. Эллиптические кривые в $GF(2^n)$.
Тема 11. Классификация криптосистем.
1. Современные шифры с закрытым и открытым ключом.

Тема 12. Классические шифры замены.
1.Криптоанализ шифров замены.
Тема 13. Классические шифры перестановки.
1. Криптоанализ шифров перестановки.
Тема 14. Современные блочные шифры с симметричным ключом.
1. Основные компоненты современного блочного шифра.
Тема 15. Современные шифры с асимметричным ключом.
1. Алгоритмы шифрования с открытыми ключами.
Тема 16. Сложность криптографических алгоритмов.
1. Сложность известных алгоритмов, используемых в криптографии и криптоанализе.

1. Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если он в ходе собеседования правильно ответил на вопрос по теме собеседования, сопровождая наглядными примерами.
Оценка «хорошо» выставляется студенту, если он в ходе собеседования ответил на вопрос по теме собеседования, при этом есть неуверенность с практическими примерами.
Оценка «удовлетворительно» выставляется студенту, если он ходе собеседования ответил неуверенно на вопросы по теме собеседования, не смог привести практические примеры.
Оценка «неудовлетворительно» выставляется студенту, если он не ответил на вопрос по теме собеседования.

2. Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура проведения данного оценочного мероприятия включает в себя устные ответы студентов на вопросы собеседования.

Предлагаемые студенту вопросы позволяют проверить компетенции ОПК-2, ОПК-4, ПСК-3, ПСК-5.

Каждому студенту предлагается ответить на два вопроса базового уровня и один вопрос повышенного уровня.

При подготовке к ответу студенту предоставляется право пользования лекциями, и методическими материалами к самостоятельной работе.

При оценивании ответов студента учитываются:
- точность и последовательность формулировок;
- умение приводить конкретные примеры по теме вопроса.

Составитель _____ Н.И. Битюцкая
(подпись)

«____»_____20 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зав. кафедрой ИБСиТ

_____ В.Ф. Антонов

«____» _____ 202_ г.

Темы индивидуальные заданий для лабораторных работ по дисциплине «Математические основы криптологии»

4 семестр

Индивидуальные задания:

Базовый уровень

1. Вычисление наибольшего общего делителя для двух чисел при помощи алгоритма Евклида.
2. Расширенный алгоритм Евклида.
3. Нахождение мультипликативной инверсии числа по заданному модулю с использованием расширенного алгоритма Евклида.
4. Решение линейного диофантового уравнения с использованием расширенного алгоритма Евклида.
5. Решение уравнения сравнения с использованием расширенного алгоритма Евклида.
6. Реализация детерменированного алгоритма проверки на простоту.
7. Реализация алгоритма решета Эратосфена проверки числа на простоту.
8. Реализация теста Ферма проверки числа на простоту.
9. Реализация алгоритма испытания квадратным корнем проверки числа на простоту.
10. Программная реализация алгоритма разложения числа на множители методом проверки делением.
11. Программная реализация алгоритма Ферма разложения числа на множители.

Повышенный уровень

1. Программная реализация алгоритма Миллера-Рабина проверки числа на простоту.
2. Программная реализация метода РО Полларда разложения числа на множители.
3. Вычисление Phi-функции Эйлера φ(n) для заданного числа n.
4. Решение системы трех уравнений сравнения с одной неизвестной и различными модулями с использованием китайской теоремы об остатках.

1. Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если отчет по работе выполнен в соответствии с требованиями, предъявляемыми методическими рекомендациями по выполнению лабораторных работ, а также раскрыты полностью все вопросы по заданию.

Оценка «хорошо» выставляется студенту, если отчет по работе выполнен в соответствии с требованиями, предъявляемыми методическими рекомендациями по выполнению лабораторных работ, а также частично раскрыты вопросы по заданию.

Оценка «удовлетворительно» выставляется студенту, если отчет по работе выполнен в соответствии с требованиями, предъявляемыми методическими

рекомендациями по выполнению лабораторных работ, а также раскрыт не полностью перечень необходимых вопросов по заданию.

Оценка «неудовлетворительно» выставляется студенту, если отчет по работе выполнен не в соответствии с требованиями, предъявляемыми методическими рекомендациями по выполнению лабораторных работ, а также не раскрыты вопросы по заданию.

2. Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура проведения данного оценочного мероприятия включает в себя: выполнение индивидуального задания и оформление отчета по лабораторным работам. Предлагаемые студенту задания позволяют проверить компетенции ОПК-2, ОПК-4, ПСК-3, ПСК-5.

Для подготовки к данному оценочному мероприятию необходимо к концу текущей лабораторной работы предоставить отчет по выполнению лабораторной работы.

При подготовке к ответу студенту предоставляется право пользования справочными материалами.

При проверке задания, оцениваются:

- последовательность и рациональность выполнения;
- знания технологий, использованных при выполнении задания,
- оформление отчета по лабораторной работе.

Составитель _____ Н.И. Битюцкая

«____»_____2020 г.

Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зав. кафедрой ИБСиТ

_____ В.Ф. Антонов

«____» _____ 202_ г.

Темы индивидуальные заданий для практических занятий по дисциплине «Математические основы криптологии»

4 семестр

Индивидуальные задания:

Базовый уровень

1. Вычисление наибольшего общего делителя для двух чисел при помощи алгоритма Евклида.
2. Расширенный алгоритм Евклида.
3. Нахождение мультипликативной инверсии числа по заданному модулю с использованием расширенного алгоритма Евклида.
4. Решение линейного диофантового уравнения с использованием расширенного алгоритма Евклида.
5. Решение уравнения сравнения с использованием расширенного алгоритма Евклида.
6. Операции над матрицами вычетов.
7. Проверка числа на простоту методом проверки делением.
8. Проверка числа на простоту с помощью решета Эратосфена.
9. Проверка числа на простоту с помощью теста Ферма.
10. Проверка числа на простоту с помощью испытания квадратным
11. Разложения числа на множители с помощью деления.
12. Разложения числа на множители с использованием алгоритма Ферма.

Повышенный уровень

1. Нахождение матрицы вычетов, инверсной данной.
2. Проверка числа на простоту по алгоритму Миллера-Рабина.
3. Разложения числа на множители с помощью метода РО Полларда.
4. Вычисление Phi-функции Эйлера φ(n) для заданного числа n.
5. Решение системы трех уравнений сравнения с одной неизвестной и различными модулями с использованием китайской теоремы об остатках.

4. Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если отчет по работе выполнен в соответствии с предъявляемыми требованиями, а также раскрыты полностью все вопросы по заданию.

Оценка «хорошо» выставляется студенту, если отчет по работе выполнен в соответствии с с предъявляемыми требованиями, а также частично раскрыты вопросы по заданию.

Оценка «удовлетворительно» выставляется студенту, если отчет по работе выполнен в соответствии с с предъявляемыми требованиями, а также раскрыт не полностью перечень необходимых вопросов по заданию.

Оценка «неудовлетворительно» выставляется студенту, если отчет по работе выполнен не в соответствии с предъявляемыми требованиями, а также не раскрыты вопросы по заданию.

5. Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**

6. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура проведения данного оценочного мероприятия включает в себя: выполнение индивидуального задания и оформление отчета. Предлагаемые студенту задания позволяют проверить компетенции ОПК-2, ОПК-4, ПСК-3, ПСК-5.

Для прохождения данного оценочного мероприятия необходимо самостоятельно выполнить индивидуальное задание, выданное преподавателем и подготовить письменный отчет по его выполнению.

При проверке задания, оцениваются:

- последовательность и рациональность выполнения;
- знание теории, использованной при выполнении задания,
- правильность оформления отчета.

Составитель _____ Н.И. Битюцкая

«____»_____2020 г.

Оценочный лист

№ п/п	Ф.И.О. студента	Параметры состояния образованности									Итоговый балл
		Предметно-информационная составляющая образованности				Деятельностно-коммуникативная составляющая образованности			Ценностно-ориентационная составляющая образованности		
		Контрольно-методический срез	Общеучебные умения и навыки			Уровень развития устной речи	Умение работать с информацией	Грамотность	Умение использовать получен-ные знания в повседневной жизни	Уровень адекватности самооценки	
			Умение анализировать	Умение доказывать	Умение делать выводы						
1.											
2.											
3.											
4.											
5.											
6.											
7.											
8.											
9.											
10.											
11.											
12.											
13.											
14.											
15.											
16.											
17.											