Компонент ОПОП 09.03.01 Информатика и вычислительная техника
(профиль «Программное обеспечение вычислительной техники и автоматизированных систем»)
наименование ОПОП

Б1.О.08.03
шифр дисциплины

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Дисциплины (модуля) **Защита информации**

Разработчик (и):
Богомолов Р.А.
ФИО
доцент
должность

к.ф.-м. н., доцент
ученая степень, звание

Утверждено на заседании кафедры информационных технологий
наименование кафедры

№ 6 от 01.02.2024
Заведующий кафедрой ИТ

_____ Ляш. О.И.
подпись ФИО

1. Критерии и средства оценивания компетенций и индикаторов их достижения, формируемых дисциплиной (модулем)

Код и наименование компетенции	Код и наименование индикатора(ов) достижения Компетенции	Результаты обучения по дисциплине (модулю)			Оценочные средства текущего контроля	Оценочные средства промежуточной аттестации
		Знать	*Уметь*	*Владеть*		
ОПК-2. Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности. .	ИД-1$_{ОПК-2}$ Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, которые могут быть использованы при решении задач профессиональной деятельности ИД-2$_{ОПК-2}$ Способен выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности ИД-3$_{ОПК-2}$ Способен применять современные информационные	принципы работы современных информационных технологий и программных средств; основы информационной и библиографической культуры.	использовать принципы работы современных информационных технологий и программных средств при решении задач профессиональной деятельности; решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникативных технологий.	принципами работы современных информационных технологий и программных средств; принципами информационной безопасности.	- тестовые задания; - типовые задания по вариантам для выполнения контрольной (расчетно-графической) работы	Результаты текущего контроля

	технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности					
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ИД-1$_{ОПК-3}$ Способен применять знания принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ИД-2$_{ОПК-3}$ Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом					

	основных требований информационной безопасности ИД-З$_{ОПК-3}$ Способен составлять обзоры, аннотации, рефераты, готовить доклады с учетом требований информационной безопасности					

2. Оценка уровня сформированности компетенций (индикаторов их достижения)

Показатели оценивания компетенций (индикаторов их достижения)	**Шкала и критерии оценки уровня сформированности компетенций (индикаторов их достижения)**			
	Ниже порогового *(«неудовлетворительно»)*	**Пороговый** *(«удовлетворительно»)*	**Продвинутый** *(«хорошо»)*	**Высокий** *(«отлично»)*
Полнота знаний	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущены не грубые ошибки.	Уровень знаний в объёме, соответствующем программе подготовки. Допущены некоторые погрешности.	Уровень знаний в объёме, соответствующем программе подготовки.
Наличие умений	При выполнении стандартных заданий не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Выполнены типовые задания с не грубыми ошибками. Выполнены все задания, но не в полном объеме (отсутствуют пояснения, неполные выводы)	Продемонстрированы все основные умения. Выполнены все основные задания с некоторыми погрешностями. Выполнены все задания в полном объёме, но некоторые с недочетами.	Продемонстрированы все основные умения. Выполнены все основные и дополнительные задания без ошибок и погрешностей. Задания выполнены в полном объеме без недочетов.
Наличие навыков (владение опытом)	При выполнении стандартных заданий не продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для выполнения стандартных заданий с некоторыми недочетами.	Продемонстрированы базовые навыки при выполнении стандартных заданий с некоторыми недочетами.	Продемонстрированы все основные умения. Выполнены все основные и дополнительные задания без ошибок и погрешностей. Продемонстрирован творческий подход к решению нестандартных задач.
Характеристика сформированности компетенции	Компетенции фактически не сформированы. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач. ИЛИ Зачетное количество баллов не набрано согласно установленному диапазону	Сформированность компетенций соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач. ИЛИ Набрано зачетное количество баллов согласно установленному диапазону	Сформированность компетенций в целом соответствует требованиям. Имеющихся знаний, умений, навыков достаточно для решения стандартных профессиональных задач. ИЛИ Набрано зачетное количество баллов согласно установленному диапазону	Сформированность компетенций полностью соответствует требованиям. Имеющихся знаний, умений, навыков в полной мере достаточно для решения сложных, в том числе нестандартных, профессиональных задач. ИЛИ Набрано зачетное количество баллов согласно установленному диапазону

3. Критерии и шкала оценивания заданий текущего контроля

3.1 Критерии и шкала оценивания лабораторных работ Перечень лабораторных/ работ, описание порядка выполнения и защиты работы, требования к результатам работы, структуре и содержанию отчета и т.п. представлены в методических материалах по освоению дисциплины (модуля) и в электронном курсе в ЭИОС МАУ.

Оценка/баллы	Критерии оценивания
Отлично	Задание выполнено полностью и правильно. Отчет по лабораторной работе подготовлен качественно в соответствии с требованиями. Полнота ответов на вопросы преподавателя при защите работы.
Хорошо	Задание выполнено полностью, но нет достаточного обоснования или при верном решении допущена незначительная ошибка, не влияющая на правильную последовательность рассуждений. Все требования, предъявляемые к работе, выполнены.
Удовлетворительно	Задания выполнены частично с ошибками. Демонстрирует средний уровень выполнения задания на лабораторную работу. Большинство требований, предъявляемых к заданию, выполнены.
Неудовлетворительно	Задание выполнено со значительным количеством ошибок на низком уровне. Многие требования, предъявляемые к заданию, не выполнены. ИЛИ Задание не выполнено.

3.2. Критерии и шкала оценивания выполнения заданий РГР

Перечень контрольных заданий расчетно-графической работы, рекомендации по их выполнению представлены в методических материалах по освоению дисциплины и в электронном курсе в ЭИОС МАУ.

В ФОС включен типовой вариант РГР.

В РГР должны быть представлены многочлены второй степени, коэффициентами которых являются ASCII – коды инициалов студента, некоторые простейшие криптопреобразования этих многочленов и оценена степени сходства и различия между исходным и преобразованными многочленами по различным критериям.

Перечень заданий, предъявляемых студентам

1. Используя стандартную ASCII – кодировку представить каждую букву собственных инициалов в виде шестнадцатеричной и двоичной последовательностей. Массиву $\{a_0, a_1, a_2\}$ присвоить значения этих кодов в порядке {Ф.,И.,О.}.
2. Построить многочлен $f(x) = a_0 + a_1 x + a_2 x^2$. Используя всевозможные перестановки трех элементов, из многочлена $f(x)$ построить еще пять многочленов отличающихся перестановкой $P^{(k)}$ коэффициентов. Для перечисления перестановок и многочленов пользоваться единой нумерацией согласно таблице 1.

Таблица 1

№п/п	0	1	2	3	4	5
$P^{(k)}$	(0 1 2)	(1 0 2)	(2 0 1)	(0 2 1)	(1 2 0)	(2 1 0)
$f_k(x)$	$a_0 + a_1x + a_2x^2$	$a_1 + a_0x + a_2x^2$	$a_2 + a_0x + a_1x^2$	$a_0 + a_2x + a_1x^2$	$a_1 + a_2x + a_9x^2$	$a_2 + a_1x + a_0x^2$

3. Считая отрезок [a,b] (a и b далее в таблице вариантов) областью определения всех указанных многочленов, вычислить аналитически расстояния $\rho(f, f_k) = \sqrt{\int_a^b (f(x) - f_k(x))^2 dx}$, скалярные произведения $(f, f_k) = \int_a^b f(x) f_k(x) dx$ и угловые характеристики $\cos\Psi_k = (f, f_k) / \|f\| / \|f_k\|$. Здесь $\|f\| = \|f_k\| = \sqrt{\int_a^b f^2(x) dx}$.

   Записать полученные аналитические формулы и, с помощью программы на языке высокого уровня, получить численные значения этих формул. Результаты представить в таблице 2 следующего вида.

Таблица 2

№п/п	0	1	2	3	4	5
$\rho(f, f_k)$						
(f, f_k)						
$\cos\Psi_k$						

4. По результатам п.п. 1-3 сделать выводы о достоинствах и недостатках криптоалгоритма, основанного на перестановках коэффициентов многочлена.
5. Разбивая отрезок [a, b] на n=256 частей построить массив значений функции $f(x)$, $F(s) = f(a + s\Delta x), s = 0,..., n-1; \Delta x = (b-a)/n$.
6. Для $m = 1,..., n$ раэбить массив $F(s)$ на последовательные подмассивы содержащие по m элементов. Так как в общем случае $n = dm + r$, то получится ровно d подмассивов из m элементов, а при r, отличном от нуля, еще и подмассив из r элементов. В каждом подмассиве из m элементов осуществляется циклическая перестановка из конца в начало на t элементов, $t = [m/2]$, [*] обозначает целую часть числа. В подмассиве из r элементов перестановка не осуществляется. Преобразуя таким образом массив $F(s)$ для фиксированного m необходимо получить массив $Fm(s)$. m=1 соответствует исходному массиву. В цикле по m вычислить расстояния $\rho(F, Fm) = \sum_{s=0}^{n-1} (F(s) - Fm(s))^2$,

скалярные произведения $(F, Fm) = \sum_{s=0}^{n-1} F(s) Fm(s)$ и угловые характеристики $\cos \Psi_m = (F, Fm) / \|F\| / \|Fm\|$, $\|F\| = \|Fm\| = \sum_{s=0}^{n-1} F^2(s)$. Полученные результаты представить в виде графиков зависимости расстояний, скалярных произведений и угловых характеристик от m.

7. Объяснить полученные зависимости и сделать выводы о зависимости действия рассмотренного криптоалгоритма от m.
8. Разбивая отрезок [a, b] на n=64 части построить массив значений функции $f(x)$, $F(s) = f(a + s\Delta x), s = 0,..., n-1; \Delta x = (b-a)/n$.
9. Для m=1,2,4,8,16,32,64 реализовать перестановку массива аналогичную п.6.
10. Для массивов полученных в п.9 построить точечные графики зависимости $F(s)$ от s=0,…,63.
11. Для массивов полученных в п.9 осуществить дискретное преобразование Фурье и построить дискретные графики амплитудного и фазового спектров.
12. Сделать выводы о том, как влияет примененный криптоалгоритм на изменение временной формы сигналов и формы амплитудного и фазового спектров.

Замечание 1.

Если два из трех инициалов совпадают, то один из совпадающих инициалов заменяется его номером в русском алфавите представленным в виде двоичной восьмибитовой комбинации. Если все три инициала совпадают, то в качестве исходных данных для выполнения РГЗ берется инициал, его номер в русском алфавите представленный в виде двоичной восьмибитовой комбинации и инвертированная двоичная восьмибитовая комбинация $0 \to 1, 1 \to 0$.

Замечание 2.

Значения a и b выбираются студентом из Таблицы 3 согласно формуле Nтаб=Nсп+(Nгр-1)*15. Nгр – последняя цифра номера группы.

№ п/п	a	b
1	1	2
2	2	3
3	3	4
4	4	5

5	5	6
6	0.1	0.2
7	0.2	0.3
8	0.3	0.4
9	0.4	0.5
10	0.5	0.6
11	1	3
12	2	4
13	3	5
14	4	6
15	5	7
16	0.1	1.1
17	0.2	1.2
18	0.3	1.3
19	0.4	1.4
20	0.5	1.5
21	.1	1.1
22	.2	1.1
23	.3	1.1
24	.4	1.1
25	.5	1.1
26	0.1	1
27	0.2	1
28	0.3	1
29	0.4	1
30	0.5	1

Баллы РГР	Критерии оценивания
40	Работа выполнена полностью, без ошибок (возможна одна неточность, описка, не являющаяся следствием непонимания материала).
35	Работа выполнена полностью, но обоснования шагов решения недостаточны, допущена одна негрубая ошибка или два-три недочета, не влияющих на правильную последовательность рассуждений.
30	В работе допущено более одной грубой ошибки или более двух-трех недочетов, но обучающийся владеет обязательными умениями по проверяемой теме.
0-29	В работе есть грубые ошибки и недочеты ИЛИ Контрольная работа не выполнена.

4. Критерии и шкала оценивания результатов обучения по дисциплине (модулю) при проведении промежуточной аттестации

Форма аттестации – зачет с оценкой.

Если обучающийся набрал зачетное количество баллов согласно установленному диапазону по дисциплине (модулю), то он считается аттестованным с оценкой согласно шкале баллов для определения итоговой оценки:

Оценка	Баллы	Критерии оценивания
Отлично	91 - 100	Набрано зачетное количество баллов согласно установленному диапазону
Хорошо	81 - 90	Набрано зачетное количество баллов согласно установленному диапазону
Удовлетворительно	60 - 80	Набрано зачетное количество баллов согласно установленному диапазону
Неудовлетворительно	менее 60	Зачетное количество согласно установленному диапазону баллов не набрано

5. Задания диагностической работы для оценки результатов обучения по дисциплине (модулю) в рамках внутренней и внешней независимой оценки качества образования

ФОС содержит задания для оценивания знаний, умений и навыков, демонстрирующих уровень сформированности компетенций и индикаторов их достижения в процессе освоения дисциплины (модуля).

Комплект заданий разработан таким образом, чтобы осуществить процедуру оценки каждой компетенции, формируемых дисциплиной (модулем), у обучающегося в письменной форме.

Содержание комплекта заданий включает: *тестовые задания.*

Комплект заданий диагностической работы

ОПК-2.
Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности

Задание № 1. *Наибольший общий делитель чисел 12 и 15 равен:*

а) 5;
б) 3;
в) 12;
г) 60.

Задание № 2. *Разность чисел 3 и 17 по модулю 7 равна:*

а) 2;
б) 0;
в) 5;
г) 8.

Задание № 3. *Произведение чисел 4 и 5 по модулю 12 равно:*

а) 9;
б) 3;
в) 8;
г) 10.

Задание № 4. *Порядок элемента 2 в кольце классов вычетов по модулю 15 равен:*

а) 2;
б) 6;
в) 4;
г) 3.

Задание № 5. *Элемент, обратный элементу 20 в кольце классов вычетов по модулю 21, равен:*

а) 7
б) 11
в) 2
г) 4.

Задание № 6. *Сколько элементов содержит расширение степени 5 двухэлементного поля?*

а) 5;
б)10;
в) 32;
г) 25.

Задание № 7. *Сколько над двухэлементным полем существует неприводимых многочленов степени 2?*

а) 1;
б) 2;
в) 3;
г) 4.

Задание № 8. *Первообразный корень по модулю 11 равен:*

а) 10;
б) 1;
в) 11;
г) 2.

Задание № 9. *Наименьшее общее кратное чисел 12 и 45 равно:*

а) 180;
б) 3;
в) 360;
г) 60.

Задание № 10. *Значение функции Эйлера от числа 75 равно:*

а) 15;
б) 20;
в) 30;
г) 40.

ОПК-3.

Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Задание № 1. *Одним из авторов системы шифрования RSA является:*

а) Шеппард;
б) Шамир;
в) Синклер;
а) Сантояна.

Задание № 2. *Сколько простых чисел используется в качестве начальных параметров в системе шифрования RSA?*

а) 2;
б) 3;

а) 0;
б) 1,

Задание № 3. *Сколько простых чисел используется в качестве начальных параметров в системе шифрования Эль-Гамаля?*

а) 2;
б) 0;
в) 3;
г) 1.

Задание № 4. *Вторым автором протокола обмена ключами DH является:*

а) Хиллман;
б) Холлман;
в) Хитман;
г) Хеллман.

Задание № 5. *Разложение натурального числа на простые множители называется:*

а) формализацией;
б) факторизацией;
в) мультипликацией;
г) примаризацией.

Задание №6. *Кто автор шифра со сдвигом на 3 позиции, применявшегося в древнеримской армии?*

а) Красс;
б) Антоний;
в) Октавиан Август;
г) Цезарь.

Задание № 7. *Второе название систем шифрования с открытым ключом:*

а) симметричные;
б) асимметричные;
в) антисимметричные;
г) кососимметричные.

Задание № 8. *Какая из приведенных ниже функций является однонаправленной при достаточно большом простом модуле?*

а) дискретный логарифм;
б) дискретное умножение на 2;
в) дискретное возведение в квадрат;
г) взятие обратного по данному модулю.

Задание № 9. *Как в системе шифрования RSA называется общедоступный ключ для шифрования?*

а) общий;

б) всеобщий;

в) открытый;

г) всемирный.

Задание № 10. *Как в системе шифрования RSA называется ключ получателя сообщения, предназначенный для дешифрования?*

а) неизвестный;

б) спрятанный;

в) потаенный;

г) секретный.