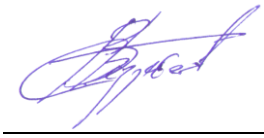
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра № 33

УТВЕРЖДАЮ
Руководитель направления

проф.,д.т.н.,доц.
(должность, уч. степень, звание)

С.В. Беззатеев
(инициалы, фамилия)



(подпись)
«27» мая 2022 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Математические основы постквантовой криптографии»
(Наименование дисциплины)

Код направления подготовки/ специальности	10.04.01
Наименование направления подготовки/ специальности	Информационная безопасность
Наименование направленности	Интеллектуальные средства обеспечения безопасности объектов
Форма обучения	очная

Санкт-Петербург– 2022

Лист согласования рабочей программы дисциплины

Программу составил (а)

д.т.н.,доц.	27.05.22	С.В. Беззатеев
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33

«27» мая 2022 г, протокол № 10

Заведующий кафедрой № 33

д.т.н.,доц.	27.05.22	С.В. Беззатеев
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Ответственный за ОП ВО 10.04.01(01)

доц.,к.т.н.,доц.	27.05.22	В.А. Мыльников
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель директора института №3 по методической работе

	27.05.22	Н.В. Решетникова
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Аннотация

Дисциплина «Математические основы постквантовой криптографии» входит в образовательную программу высшего образования – программу магистратуры по направлению подготовки/ специальности 10.04.01 «Информационная безопасность» направленности «Интеллектуальные средства обеспечения безопасности объектов». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-2 «Способен обосновывать перспективы проведения исследований в соответствующей области знаний»

Содержание дисциплины охватывает круг вопросов, связанных с основными принципами и методам, применяемыми при синтезе и анализе криптосистем.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа студента.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме дифференцированного зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа.

Язык обучения по дисциплине «русский »

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Цель курса - научить студентов основным принципам и методам, применяемым при синтезе и анализе криптосистем.

В курс включены основные методы криптографического анализа, применяемые в защите информации. Анализ криптографических алгоритмов органически связан с синтезом криптоалгоритмов и криптопротоколов. В результате изучения курса студенты должны овладеть основным криптографическим инструментарием, необходимым для построения защищенных ИКС.

1.2. Дисциплина входит в состав части, формируемой участниками образовательных отношений, образовательной программы высшего образования (далее – ОП ВО).

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП ВО.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Профессиональные компетенции	ПК-2 Способен обосновывать перспективы проведения исследований в соответствующей области знаний	ПК-2.З.1 знает методы, средства и практику планирования, организации, проведения и внедрения научных исследований и опытно-конструкторских разработок ПК-2.У.1 умеет анализировать новую научную проблематику соответствующей области знаний ПК-2.В.1 владеет навыками проведения анализа новых направлений исследований в соответствующей области знаний

2. Место дисциплины в структуре ОП

Дисциплина может базироваться на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

– «Теория информации»,
– «Методы моделирования и оптимизации».

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и могут использоваться при написании выпускной квалификационной работы магистра.

3. Объем и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены втаблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№2
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	2/ 72	2/ 72
Из них часов практической подготовки	34	34
Аудиторные занятия, всего час.	51	51
в том числе:		
лекции (Л), (час)	17	17

практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	34	34
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)		
Самостоятельная работа, всего (час)	21	21
***Вид промежуточной аттестации*:** зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Дифф. Зач.	Дифф. Зач.

Примечание: **кандидатский экзамен

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий.

Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 2					
Раздел 1. Введение	1				1
Раздел 2. Элементы теории NP-полныхзадач и задача анализа стойкости криптографических систем. Тема 2.1. – Основные понятия. Тема 2.2. - Класс задач NP.	4		8		4
Раздел 3. Принципы криптоанализа. Тема 3.1. – Анализ стойкости систем. Тема 3.2. – Криптоанализ ранцевыхсистем.	5		8		4
Раздел 4. Кодовые криптосистемы. Тема 4.1. – Основные понятия теориикодирования. Тема 4.2. – Традиционные кодовые криптосистемы.	7		18		12
Итого в семестре:	17		34		21
Итого	17	0	34	0	21

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	Раздел 1. Введение Классификация криптографических систем
2	Раздел 2. Элементы теории NP-полныхзадач и задача анализа
	стойкости криптографических систем. Тема 2.1. – Основные понятия. Детерминированные машины Тьюринга и класс задач P. Тема 2.2. - Класс задач NP. Недетерминированные алгоритмы и класс задач NP. Основные NP-полные задачи.

3	Раздел 3. Принципы криптоанализа. Тема 3.1. – Анализ стойкости систем. Прямая и косвенная атаки на криптографические системы. Тема 3.2. – Криптоанализ ранцевых систем. Атака Шамира ранцевых систем. Криптоатака Лагариса-Одлыжко.
4	Раздел 4. Кодовые криптосистемы. Тема 4.1. – Основные понятия теории кодирования. NP-полные задачи кодирования. Тема 4.2. – Традиционные кодовые криптосистемы. Атака системы Мак-Элиса, основанная на анализе группы симметрии кода. Системы, основанные на задаче полного декодирования. Модификации кодовых криптосистем.

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено					
Всего					

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 2				
	Машина Тьюринга	4	4	2
	Задача о сумме подмножества	4	4	2
	Факторизация целых чисел	4	4	3
	Вычисление дискретного логарифма	4	4	3
	Декодирование линейного кода	6	6	4
	Оценка параметров кодовой криптосистемы	6	6	4
	Модификации кодовых криптосистем	6	6	4
	Всего	34	34	

4.5. Курсовое проектирование/ выполнение курсовой работы

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 2, час
1	2	3

Изучение теоретического материала дисциплины (ТО)	8	8
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	8	8
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	5	5
Всего:	21	21

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны вп.п. 7-11.

6. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 8.

Таблица 8– Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004 Р 98	Рябко, Б. Я. Криптографические методы защиты информации [Текст]: учебное пособие / Б. Я. Рябко, А. Н.Фионов. - 2-е изд., стер. - М. : Горячая линия - Телеком, 2014. - 229 с.	10
004 В 75	Основы защиты информации. Защита персонального компьютера от умышленных угроз [Текст]: учебное пособие / А. В. Воронов, Ю. В. Трифонова; С.- Петерб. гос. ун-т аэрокосм. приборостроения. - СПб.:Изд-во ГУАП, 2015. - 99 с.	57
004/М 87-604316-ED	Защищенные инфотелекоммуникации. Анализ и синтез: монография / Н. Н. Мошак; С.-Петерб. гос. ун-т аэрокосм.	40
	приборостроения. - Электрон. текстовые дан. - СПб. : Изд-во ГУАП, 2014. - 197 с.	
http://znanium.com/catalog.php?bookinfo=427831	Основы современной криптографии и стеганографии / Рябко Б.Я., Фионов А.Н., 2-е изд. - М.: Гор. линия-Телеком, 2013. - 232 с.	

7. Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно- телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

URL адрес	Наименование
https://www.pgpru.com/	Проект "OpenPGP в России"

8. Перечень информационных технологий

8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2. Перечень информационно-справочных систем,используемых при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной частиматериально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Компьютерный класс	

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Дифференцированный зачёт	Список вопросов.

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 –Критерии оценки уровня сформированности компетенций

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	

«отлично» «зачтено»	– обучающийся глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	– обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	– обучающийся не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений.

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

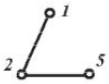
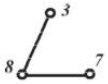
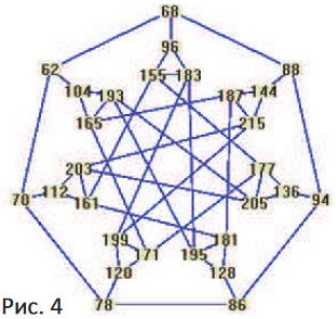
№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
	Учебным планом не предусмотрено	

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора

1	Классификация криптографических систем. Симметричные и несимметричные криптографические функции. Задачи криптоанализа. Элементы теории NP-полных задач и задача анализа стойкости криптографических систем. Задачи распознавания. Языки. Детерминированные машины Тьюринга и класс задач P. Недетерминированные алгоритмы и класс задач NP. Полиномиальная сводимость и NP-полные задачи. Теорема Кука. Основные NP-полные задачи. Прямая и косвенная атаки на криптографические системы. Система Хеллмана-Меркля. Теоретико-числовые криптосистемы и задача разложения чисел на простые множители. Атака Шамира ранцевых систем. Модификации ранцевых систем и криптоатака Лагариса-Одлыжко.	ПК-2.З.1
2	Линейные коды. Способы задания. Декодирование линейных кодов как «трудная» задача. Декодирование линейных кодов как «простая» задача. Системы Мак-Элиса и Нидеррайтера. Прямая атака кодовых криптосистем. Атака Сидельникова-Шестакова. Атака системы Мак-Элиса, основанная на анализе группы симметрии кода. Системы, основанные на задаче полного декодирования. Атака Зоргера. Модификации кодовых криптосистем.	ПК-2.У.1
3	Известно, что число $N = 203060593$ является произведением двух простых чисел p и q, а количество натуральных чисел, меньших и взаимно простых с N, равно 203030388. Найдите числа p и q. Известно, что три числа a_1, a_2, a_3 были получены следующим образом. Сначала выбрали натуральное число A и нашли числа $A_1 = [A]_{16}, A_2 = [A/2]_{16}, A_3 = [A/4]_{16}$, где $[X]_{16}$ – остаток от деления целой части числа X на 16 (например, $[53/2]_{16} = 10$). Затем было выбрано целое число B такое, что $0 \le B \le 15$. Числа A_1, A_2, A_3 и B записывают в двоичной системе счисления, т.е. представляют каждое из них в виде цепочки из 0 и 1 длины 4, приписывая слева необходимое число нулей. Такие цепочки условимся складывать посимвольно «в столбик» без переносов в следующий разряд согласно правилу: $1+1=0+0=0$ и $0+1=1+0=1$, а саму операцию посимвольного сложения обозначим символом $\oplus$. Например, $3 \oplus 14 = (0011) \oplus (1110) = (1101) = 13$. Положим $a_1 = A_1 \oplus B$, $a_2 = A_2 \oplus B$, $a_3 = A_3 \oplus B$. Найдите все возможные значения числа a_3, если известно, что $a_1 = 10, a_2 = 4$. Для зашифрования натурального числа m используется граф, представляющий собой множество вершин, некоторые из которых соединены друг с другом прямой линией. Вершины графа, соединенные друг с другом, называют соседними. Зашифрование состоит в	ПК-2.В.1

	выполнении следующих действий. В вершины графа записываются натуральные числа так, чтобы их сумма была равна m . Затем к числу в каждой вершине прибавляются числа в соседних вершинах. В результате получается граф, в котором «зашифровано» число m . Пример: для зашифрования числа 8 будем использовать граф на рис. 1. В его вершины поместим числа, сумма которых равна 8 (рис. 2). Затем к каждому числу прибавим числа в соседних вершинах. Результат зашифрования указан на рис. 3. На рис. 4 приведен результат зашифрования некоторого числа. Найдите его.  Рис. 1  Рис. 2  Рис. 3  Рис. 4	

Перечень тем для курсового проектирования/выполнения курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для курсового проектирования/выполнения курсовой работы

№ п/п	Примерный перечень тем для курсового проектирования/выполнения курсовой работы
	Учебным планом не предусмотрено

Вопросы для проведения промежуточной аттестации в виде тестированияпредставлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
1	1. Наука, занимающаяся проблемой защиты информации путем ее преобразования - это A. криптология B. криптография C. криптоанализ D. шифрование 2. Наука, занимающаяся исследованием возможности расшифровывания информации без знания ключей - это A. криптоанализ B. криптология C. криптография D. шифрование 3. Конечное множество используемых для кодирования информации знаков - это A. алфавит	ПК-2.У.1

B. текст
C. шифр
D. ключ

4. Преобразовательный процесс, при котором исходный текст заменяется шифрованным текстом - это

A. шифрование
B. дешифрование
C. декодирование
D. кодирование

5. Преобразовательный процесс, при котором шифрованный текст преобразуется в исходный - это

A. дешифрование
B. шифрование
C. кодирование
D. декодирование

6. Информация, необходимая для беспрепятственного шифрования и дешифрирования текстов - это

A. ключ
B. алфавит
C. шифр
D. код

7. Из перечисленных: 1) симметричные, 2) несимметричные, 3) с открытым ключом, 4) с закрытым ключом - различают криптосистемы

A. 1, 3
B. 1, 2
C. 3, 4
D. 1, 4

8. Криптосистемы, в которых для шифрования и для дешифрования используется один и тот же ключ называются криптосистемами

A. симметричными
B. несимметричными
C. с открытым ключом
D. с закрытым ключом

9. Криптосистемы, в которых ннформация шифруется с помощью одного ключа, а расшифровывается с помощью другого ключа, известного только получателю сообщения называются криптосистемами

A. с открытым ключом
B. с закрытым ключом
C. симметричными

D. несимметричными

10. В криптосистемах с открытым ключом

A. открытый ключ доступен всем желающим, закрытый ключ доступен только получателю сообщения
B. для шифрования и дешифрования используется один ключ
C. закрытый ключ доступен всем желающим, открытый ключ доступен только получателю сообщения
D. закрытый и открытый ключи доступны всем желающим

11. Присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения, называется

A. электронной подписью
B. идентификатором
C. ключом
D. шифром

12. Характеристика шифра, определяющая стойкость шифра к дешифрованию без знания ключа, называется

A. криптостойкостью
B. надежностью
C. эффективностью
D. уровнем безопасности

13. Из перечисленных: 1) количество всех возможных ключей, 2) размер алфавита, 3) размер открытого текста, 4) среднее время криптоанализа - к показателям криптостойкости шифра относятся

A. 1, 4
B. 1, 2, 3, 4
C. 2, 3
D. 1, 2, 3

14. Из перечисленных: 1) замена, 2) перестановка, 3) гаммирование, 4) смысловое кодирование, 5) рассечение и разнесение - к методам шифрования информации относятся

A. 1, 2, 3
B. 1, 2, 3, 4, 5
C. 4, 5
D. 1, 2, 3, 4

15. Из перечисленных: 1) одноалфавитная, 2) многоалфавитная, 3) смысловая, 4) механическая - к методам шифрования информации способом замены относятся

A. 1, 2
B. 1, 2, 3, 4
C. 3, 4

D. 1, 2, 3

16. Из перечисленных: 1) простая, 2) усложненная по таблице, 3) усложненная по маршрутам, 4) одноалфавитная, 5) многоалфавитная - к методам шифрования информации способом перестановки относятся

A. 1, 2, 3
B. 1, 2, 3, 4, 5
C. 4, 5
D. 2, 3, 4, 5

17. Шифрование - это вид криптографического закрытия,

A. при котором преобразованию подвергается каждый символ защищаемого сообщения
B. при котором преобразованию подвергается сообщение целиком, но не каждый его символ
C. при котором к каждому символу приписывается кодовая комбинация
D. который обеспечивает невозможность расшифровки

18. Кодирование - это вид криптографического закрытия,

A. при котором некоторые элементы защищаемых данных (это не обязательно отдельные символы) заменяются заранее выбранными кодами
B. при котором каждый символ защищаемых данных заменяется заранее выбранным кодом
C. при котором к каждому символу приписывается кодовая комбинация
D. который обеспечивает полную невозможность чтения сообщения

19. Шифр, который производит замену каждой буквы открытого текста на символ шифрованного текста, называется

A. подстановка
B. перестановка
C. гаммирование
D. блочный

20. Шифр, у которого буквы открытого текста не замещаются на другие, а меняется порядок их следования, называется

A. перестановка
B. подстановка
C. гаммирование
D. блочный

21. Шифр, который заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа, называется

A. гаммирование

	B. перестановка C. подстановка D. блочный 22. Шифр, который представляет собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к части шифруемого текста, называется A. блочный B. рассечение-разнесение C. подстановка D. гаммирование 23. Шифр, который заключается в том, что массив защищаемых данных делится на такие элементы, каждый из которых в отдельности не позволяет раскрыть содержание защищаемой информации, и которые хранятся по разным зонам ЗУ или располагаются на различных носителях, называется A. рассечение-разнесение B. блочный C. гаммирование D. перестановка 24. Из перечисленных: 1) смысловое, 2) символьное, 3) блочное, 4) гаммирование - к методам криптографического закрытия информации способом кодирования относятся A. 1, 2 B. 1, 2, 3, 4 C. 3, 4 D. 1, 2, 4 25. При символьном кодировании A. кодируется каждый символ защищаемого сообщения B. символы защищаемого сообщения меняются местами в соответствии с днем недели C. закодированное сообщение имеет вполне определенный смысл (слова, предложения, группы предложений) D. символы защищаемого сообщения меняются местами случайным образом 26. При смысловом кодировании A. кодируемые элементы имеют вполне определенный смысл (слова, предложения, группы предложений) B. кодируемые элементы меняются местами в соответствии с днем недели C. кодируемые элементы не имеют никакого смысла D. кодируемые элементы меняются местами случайным образом	

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

11. Методические указания для обучающихся по освоению дисциплины

11.1. Методические указания для обучающихся по освоению лекционного материала.

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимися лекционного материала:

- получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;
- получение опыта творческой работы совместно с преподавателем;
- развитие профессионально-деловых качеств, любви к предмету и самостоятельного творческого мышления.
- появление необходимого интереса, необходимого для самостоятельной работы;
- получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;
- научиться методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);
- получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

Раздел 1 . Введение

Раздел 2. Элементы теории NP-полных задач и задача анализа стойкости криптографических систем.

Тема 2.1. – Основные понятия.Тема 2.2.

– Класс задач NP.

Раздел 3. Принципы криптоанализа. Тема 3.1. –

Анализ стойкости систем.

Тема 3.2. – Криптоанализ ранцевых систем.Раздел 4.

Кодовые криптосистемы.

Тема 4.1. – Основные понятия теории кодирования.

Тема 4.2. – Традиционные кодовые криптосистемы.

11.2. Методические указания для обучающихся по выполнению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и

закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.
Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач обучающегося:

- приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;
- закрепление, развитие и детализация теоретических знаний, полученных на лекциях;
- получение новой информации по изучаемой дисциплине;
- приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ
Вариант задания по каждой лабораторной работе обучающийся получает в соответствии с номером в списке группы. Перед проведением лабораторной работы обучающемуся следует внимательно ознакомиться с методическими указаниями по ее выполнению, а также с содержанием соответствующего лекционного курса, при необходимости – изучить самостоятельно дополнительную литературу. В соответствии с заданием обучающийся должен подготовить необходимые данные, выполнить задание лабораторной работы, получить требуемые результаты, оформить и защитить отчет по лабораторной работе.

Структура и форма отчета о лабораторной работе
Отчет о лабораторной работе должен включать в себя: титульный лист, формулировку задания, теоретические положения, используемые при выполнении лабораторной работы, описание процесса выполнения лабораторной работы, полученные результаты и выводы.

Требования к оформлению отчета о лабораторной работе
По каждой лабораторной работе выполняется отдельный отчет. Титульный лист оформляется в соответствии с шаблоном (образцом) приведенным на сайте ГУАП (www.guap.ru) в разделе «Сектор нормативной документации». Текстовые и графические материалы оформляются в соответствии с действующими ГОСТами и требованиями, приведенными на сайте ГУАП (www.guap.ru) в разделе «Сектор нормативной документации».

11.3. Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.
Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.
Методическими материалами, направляющими самостоятельную работу Методическими материалами, направляющими самостоятельную работу обучающихся являются учебно-методические материалы по дисциплине.
Для развития у студентов навыков самостоятельного овладения теоретическим материалом ряд тем дисциплины на лекционных занятиях дается обзорно, что предполагает их самостоятельное детальное изучение.
Примерные темы для самостоятельного изучения:

- Задачи распознавания. Языки.

– Недетерминированные алгоритмы и класс задач NP.
– Полиномиальная сводимость и NP-полные задачи.
– Теорема Кука.
– NP-полные задачи и однонаправленные функции.
– Псевдослучайные генераторы.
– Доказательства с нулевым разглашением.
– Прямая и косвенная атаки на криптографические системы.
– Теоретико-числовые криптосистемы и задача разложения чисел на простые множители.
– Теоретико-числовые криптосистемы и задача вычисления дискретного логарифма.
– Эллиптические кривые
– Модификации ранцевых систем и криптоатака Лагариса-Одлыжко.
– Коды, основанные на спектральных свойствах.
– NP-полные задачи кодирования.
– Атака Сидельникова-Шестакова.
– Атака системы Мак-Элиса, основанная на анализе группы симметрии кода.
– Атака Зоргера.

11.4. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины. Форма проведения текущего контроля – защита отчетов по лабораторным работам. Результаты текущего контроля учитываются при проведении промежуточной аттестации в соответствии с требованиями СТО ГУАП. СМК 3.76 «Положение о текущем контроле успеваемости и промежуточной аттестации студентов и аспирантов ГУАП, обучающихся по образовательным программам высшего образования».

11.5. Методические указания для обучающихся по прохождению промежуточной аттестации.

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя дифференцированный зачет.

Дифференцированный зачет – это форма оценки знаний, полученных обучающимся при изучении дисциплины, при выполнении курсовых проектов, курсовых работ, научно-исследовательских работ и прохождении практик с аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой