

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

Кафедра № 33

УТВЕРЖДАЮ

Ответственный за образовательную программу

доц., к.э.н., доц.

(должность, уч. степень, звание)

Т.Н. Елина

(инициалы, фамилия)

(подпись)

«27» июня 2024 г

Лист согласования рабочей программы дисциплины

Программу составил (а)

доц., к.э.н., доц.

(должность, уч. степень, звание)

27.06.2024

(подпись, дата)

Т.Н. Елина

(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33

«27» июня 2024 г, протокол № 11

Заведующий кафедрой № 33

д.т.н., доц.

(уч. степень, звание)

27.06.2024

(подпись, дата)

С.В. Беззатеев

(инициалы, фамилия)

Заместитель директора института №3 по методической работе

(должность, уч. степень, звание)

27.06.2024

(подпись, дата)

Н.В. Решетникова

(инициалы, фамилия)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Криптология»
(Наименование дисциплины)

Код направления подготовки/ специальности	10.04.01
Наименование направления подготовки/ специальности	Информационная безопасность
Наименование направленности	Технологии искусственного интеллекта в информационной безопасности
Форма обучения	очная
Год приема	2024

Санкт-Петербург – 2024

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

Кафедра № 33

УТВЕРЖДАЮ

Ответственный за образовательную
программу

доц., к.э.н., доц.

(должность, уч. степень, звание)

Т.Н. Елина

(инициалы, фамилия)

(подпись)

«27» июня 2024 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Криптология»
(Наименование дисциплины)

Код направления подготовки/ специальности	10.04.01
Наименование направления подготовки/ специальности	Информационная безопасность
Наименование направленности	Технологии искусственного интеллекта в информационной безопасности
Форма обучения	очная
Год приема	2024

Санкт-Петербург– 2024

Лист согласования рабочей программы дисциплины

Программу составил (а)

доц.,к.э.н.,доц.
(должность, уч. степень, звание)

27.06.2024
(подпись, дата)

Т.Н. Елина
(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33

«27» июня 2024 г, протокол № 11

Заведующий кафедрой № 33

д.т.н.,доц.
(уч. степень, звание)

27.06.2024
(подпись, дата)

С.В. Беззатеев
(инициалы, фамилия)

Заместитель директора института №3 по методической работе

(должность, уч. степень, звание)

27.06.2024
(подпись, дата)

Н.В. Решетникова
(инициалы, фамилия)

Аннотация

Дисциплина «Криптология» 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-7 «Способен проводить анализ угроз информационной безопасности в сетях электросвязи»

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

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

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

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-7 Способен проводить анализ угроз информационной безопасности в сетях электросвязи	ПК-7.3.1 знает организационно-технические мероприятия по обеспечению защиты сетей электросвязи от НСД и их эффективность ПК-7.У.1 умеет проводить проверку работоспособности и эффективности применяемых программно-аппаратных (в том числе криптографических) и технических средств защиты сетей электросвязи от НСД

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 в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№3
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	3/ 108	3/ 108
Из них часов практической подготовки	34	34

Аудиторные занятия , всего час.	68	68
в том числе:		
лекции (Л), (час)	34	34
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	34	34
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)	26	26
Самостоятельная работа , всего (час)	14	14
Вид промежуточной аттестации: зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Экз.	Экз.

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 3					
Раздел 1 . Введение	4				2
Раздел 2. Элементы теории NP-полных задач и задача анализа стойкости криптографических систем. Тема 2.1. – Основные понятия. Тема 2.2. - Класс задач NP.	10		10		4
Раздел 3. Принципы криптоанализа. Тема 3.1. – Анализ стойкости систем. Тема 3.2. – Криптоанализ ранцевых систем.	10		12		4
Раздел 4. Кодовые криптосистемы. Тема 4.1. – Основные понятия теории кодирования. Тема 4.2. – Традиционные кодовые криптосистемы.	10		12		4
Итого в семестре:	34		34		14
Итого	34	0	34	0	14

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
2	Раздел 2. Элементы теории NP-полных задач и задача анализа стойкости криптографических систем. Тема 2.1. – Основные понятия. Тема 2.2. – Класс задач NP.

3	Раздел 3. Принципы криптоанализа. Тема 3.1. – Анализ стойкостисистем. Тема 3.2. – Криптоанализ ранцевых систем.
4	Раздел 4. Кодовые криптосистемы. Тема 4.1. – Основные понятия теории кодирования. Тема 4.2. – Традиционные кодовые криптосистемы.

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 3				
1	Машина Тьюринга	4	4	2
2	Задача о сумме подмножества	4	4	2
3	Факторизация целых чисел	4	4	3
4	Вычисление дискретного логарифма	4	4	3
5	Декодирование линейного кода	6	6	4
6	Оценка параметров кодовой криптосистемы	6	6	4
7	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 3, час
----------------------------	------------	----------------

1	2	3
Изучение теоретического материала дисциплины (ТО)	14	
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)		
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)		
Всего:	14	14

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)
Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.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.-Петербург. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - СПб. : Изд-во ГУАП, 2014. - 197 с.	40
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 средствдля 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
Экзамен	Список вопросов к экзамену; Экзаменационные билеты.

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 5-балльная шкала	Характеристика сформированных компетенций
«отлично» «зачтено»	<ul style="list-style-type: none"> – 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»	<ul style="list-style-type: none"> – 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»	<ul style="list-style-type: none"> – 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»	<ul style="list-style-type: none"> – 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
1	Классификация криптографических систем.	ПК-7.3.1
2	Симметричные и несимметричные криптографические функции.	ПК-7.У.1
3	Задачи криптоанализа.	
4	Элементы теории NP-полных задач и задача анализа стойкости криптографических систем.	
5	Задачи распознавания. Языки.	
6	Детерминированные машины Тьюринга и класс задач P.	
7	Недетерминированные алгоритмы и класс задач NP.	
8	Полиномиальная сводимость и NP-полные задачи.	

9	Теорема Кука.	
10	Основные NP-полные задачи.	
11	Прямая и косвенная атаки на криптографические системы.	
12	Система Хеллмана-Меркля.	
13	Теоретико-числовые криптосистемы и задача разложения чисел на простые множители.	
14	Атака Шамира ранцевых систем.	
15	Модификации ранцевых систем и криптоатака Лагариса-Одлыжко.	
16	Линейные коды. Способы задания.	
17	Декодирование линейных кодов как «трудная» задача.	
18	Декодирование линейных кодов как «простая» задача.	
19	Системы Мак-Элиса и Нидеррайтера.	
20	Прямая атака кодовых криптосистем.	
21	Атака Сидельникова-Шестакова.	
22	Атака системы Мак-Элиса, основанная на анализе группы симметрии кода.	
23	Системы, основанные на задаче полного декодирования.	
24	Атака Зоргера.	
25	Модификации кодовых криптосистем.	

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
	Учебным планом не предусмотрено	

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 тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	Не предусмотрено	

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 экзамен.

Экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается 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