

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

Кафедра № 25

УТВЕРЖДАЮ

Руководитель образовательной программы

доц., к.т.н., доц.

(должность, уч. степень, звание)

Н.В. Марковская

(инициалы, фамилия)

(подпись)

«24» июня 2024 г

Лист согласования рабочей программы дисциплины

Программу составил (а)

доц., к.т.н., доц.

(должность, уч. степень, звание)

24.06.2024

(подпись, дата)

А.А. Овчинников

(инициалы, фамилия)

Программа одобрена на заседании кафедры № 25

«24» июня 2024 г, протокол № 12/2023-24

Заведующий кафедрой № 25

д.т.н., проф.

(уч. степень, звание)

24.06.2024

(подпись, дата)

А.М. Тюрликов

(инициалы, фамилия)

Заместитель директора института №2 по методической работе

доц., к.т.н., доц.

(должность, уч. степень, звание)

24.06.2024

(подпись, дата)

Н.В. Марковская

(инициалы, фамилия)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Криптографические методы защиты информации»

(Наименование дисциплины)

Код направления подготовки/ специальности	11.03.02
Наименование направления подготовки/ специальности	Инфокоммуникационные технологии и системы связи
Наименование направленности	Программно-защищенные инфокоммуникации
Форма обучения	очная
Год приема	2024

## Аннотация

Дисциплина «Криптографические методы защиты информации» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 11.03.02 «Инфокоммуникационные технологии и системы связи» направленности «Программно-защищенные инфокоммуникации». Дисциплина реализуется кафедрой «№25».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-1 «Способен к развитию систем и сетей передачи данных»

ПК-3 «Способен применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств инфокоммуникаций, использованию и внедрению результатов исследований»

ПК-4 «Способен оценивать параметры безопасности и защищать программное обеспечение и сетевые устройства администрируемой сети с помощью специальных средств управления безопасностью»

Содержание дисциплины охватывает круг вопросов, связанных с защитой компьютерной информации, существующих методов и информационных технологий этой защиты и оценкой их стойкости в информационных системах.

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

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

Общая трудоемкость освоения дисциплины составляет 7 зачетных единиц, 252 часа.

Язык обучения по дисциплине «русский»

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Цель курса - научить студентов понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности.

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-1 Способен к развитию систем и сетей передачи данных	ПК-1.3.5 знать цели и задачи проводимых исследований и разработок ПК-1.У.3 уметь применять методы анализа научно-технической информации
Профессиональные компетенции	ПК-3 Способен применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств инфокоммуникаций, использованию и внедрению результатов исследований	ПК-3.3.1 знать методы и средства планирования и организации исследований и разработок ПК-3.В.1 владеть навыками организации сбора и изучения научно-технической информации по теме исследований и разработок
Профессиональные компетенции	ПК-4 Способен оценивать параметры безопасности и защищать программное обеспечение и сетевые устройства администрируемой сети с помощью специальных средств управления безопасностью	ПК-4.3.2 знать основные принципы, криптографические протоколы и программные средства обеспечения информационной безопасности сетевых устройств ПК-4.3.3 знать основы защиты информации и базовые угрозы ПК-4.У.1 уметь применять программные, аппаратные и программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа

## 2. Место дисциплины в структуре ОП

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

- Дискретная математика
- Алгоритмы и структуры данных

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и используются при изучении других дисциплин:

- Учебно-исследовательская работа студента

## 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	
		№5	№6
1	2	3	4
<b>Общая трудоемкость дисциплины, ЗЕ/ (час)</b>	6/ 216	2/ 72	4/ 144
<b>Из них часов практической подготовки</b>	51	17	34
<b>Аудиторные занятия, всего час.</b>	102	51	51
в том числе:			
лекции (Л), (час)	51	34	17
практические/семинарские занятия (ПЗ), (час)			
лабораторные работы (ЛР), (час)	34	17	17
курсовой проект (работа) (КП, КР), (час)	17		17
экзамен, (час)	54		54
<b>Самостоятельная работа, всего (час)</b>	60	21	39
<b>Вид промежуточной аттестации:</b> зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Зачет, Экз.	Зачет	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)
<b>Семестр 5</b>					
Раздел 1. Основные понятия криптографии	12		9		7
Текущий контроль	1				7
Раздел 2. Симметричные шифры	21		8		7
Итого в семестре:	34		17		21
<b>Семестр 6</b>					
Раздел 3. Криптография с открытым ключом	10		9		5
Текущий контроль	1				10
Раздел 4. Криптографические протоколы	6		8		5

Выполнение курсовой работы				17	19
Итого в семестре:	17		17	17	39
Итого	51	0	34	17	60

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	<p>Раздел 1. Основные понятия криптографии. Тема 1.1 – Основные определения Определение целей и принципов защиты информации; установление, факторов, влияющих на защиту информации; основные опасности и угрозы в области информационной безопасности. Классификации видов, методов и средств защиты информации. Организационная защита информации. Инженерно-техническая защита информации. Криптографическая защита информации. Представление информации в цифровом виде.</p> <p>Тема 1.2 – Задачи информационной безопасности Задача обеспечения конфиденциальности. Определение шифра. Задача обеспечения аутентификации, понятия об электронной цифровой подписи (ЭЦП). Основные задачи в области управления ключами. Криптопротоколы: обеспечение идентификации, разделение секрета, выработка ключа, цифровые деньги.</p>
2	<p>Раздел 2. Симметричные шифры Тема 2.1. Исторические шифры Подстановочные шифры и перестановочные шифры. Шифр Цезаря, аффинный шифр, шифр моноалфавитной замены. Шифр Виженера. Цилиндр Джефферсона. Полиалфавитные шифры. Роторные машины.</p> <p>Тема 2.2. Блочные шифры Понятие стойкости, предположения об исходных условиях криптоанализа, совершенная стойкость. Одноразовый блокнот. Шифр Вернама. Принципы построения блочных шифров. Свойства смешивания и рассеивания. Составные шифры, итеративные шифры. SP-сети, сети Файстеля. Современные системы шифрования: алгоритмы DES, ГОСТ 28147-89, AES. Режимы блочного шифрования: ECB, CBC, CFB, OFB. Режим счетчика. Многократное шифрование.</p> <p>Тема 2.3. Поточковые шифры Требования к поточным шифрам. Методы построения больших периодов в поточных шифрах. Регистры сдвига с линейной обратной связью (РСЛОС). m-последовательности.</p>

	Алгоритм Берлекэмп-Мессе. Построение потоковых шифров на основе РСЛОС. Нелинейное комбинирование РСЛОС: генератор Геффе, шифры с контролем тактов. Применение поточного шифрования.
3	<p>Раздел 3. Криптография с открытым ключом</p> <p>Тема 3.1 - Математические основы систем с открытым ключом</p> <p>Модульная арифметика. Алгоритм Евклида и его сложность. Расширенный алгоритм Евклида. Основные теоремы о вычетах. Функция Эйлера. Теоремы Эйлера, Ферма. Факторизация. Логарифмирование в конечных полях. Оценки сложности “трудных” проблем, на которых строятся системы с открытым ключом. Быстрое возведение в степень.</p> <p>Тема 3.2 - Основные алгоритмы с открытым ключом</p> <p>Система Меркли-Хеллмана. Схема RSA. Атаки на RSA. Схема шифрования Эль-Гамала. Система Мак-Элиса. Криптографические хэш-функции. Понятие о цифровой подписи. Подпись RSA. Подпись Эль-Гамала. Подпись DSA. ЭЦП ГОСТ Р 34.10-94 и ГОСТ Р 34.10-01.</p>
4	<p>Раздел 4. Криптографические протоколы</p> <p>Тема 4.1 - Основные протоколы с открытым ключом</p> <p>Выработка ключа. Протокол Диффи-Хеллмана. Гибридные системы шифрования: цифровой конверт. Доказательство с нулевым разглашением. Схема идентификации Фиата-Шамира. Схема идентификации Гиллу-Квискуотера. Инфраструктура открытых ключей. Сертификаты открытых ключей.</p> <p>Тема 4.2. – Специальные протоколы</p> <p>Слепая подпись. Протоколы разделения секрета и вручения бит. Протоколы цифровых денег и электронного голосования. Защищенные распределенные вычисления.</p>

#### 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,	№ раздела дисциплины

			(час)	лины
Семестр 5				
1	Вводное занятие	1	1	1
2	Задачи информационной безопасности ч.1	4	4	1
3	Задачи информационной безопасности ч.2	4	4	1
4	Исторические шифры	4	4	2
5	Блочные шифры	4	4	2
Семестр 6				
6	Вводное занятие	1	1	3
7	Математические основы систем с открытым ключом	4	4	3
8	Основные алгоритмы с открытым ключом	4	4	3
9	Основные протоколы с открытым ключом	4	4	4
10	Специальные протоколы	4	4	4
Всего:		34	34	

#### 4.5. Курсовое проектирование/ выполнение курсовой работы

Цель курсовой работы: Исследование структуры, свойств и криптографической стойкости потокового шифра (по заданию преподавателя)

Часов практической подготовки: 17

Примерные темы заданий на курсовую работу приведены в разделе 10 РПД.

#### 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 5, час	Семестр 6, час
1	2	3	4
Изучение теоретического материала дисциплины (ТО)	16	11	5
Курсовое проектирование (КП, КР)	19		19
Подготовка к текущему контролю успеваемости (ТКУ)	15	5	10
Подготовка к промежуточной аттестации (ПА)	10	5	5
Всего:	60	21	39

#### 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)
[004.056.55 Е 78]	Ерош, И. Л. Криптография. Первое знакомство: учебное пособие/ СПб.:ГОУ ВПО "СПбГУАП", 2008. - 84 с.	ФО(3), СО(295), ЛС(4), ЛСЧЗ(1), ИГ(20)
[004.05 В 75]	Воронов, А. В., Волошина Н.В. Основы защиты информации: учебное пособие.СПб.: ГОУ ВПО "СПбГУАП", 2009. - 78 с. -	ФО(4), СО(70)
	<a href="https://lib.guap.ru/jirbis2/components/com_irbis/pdf_view/?545655">https://lib.guap.ru/jirbis2/components/com_irbis/pdf_view/?545655</a> Мошак, Николай Николаевич (проф.). Защищенные инфотелекоммуникации. Анализ и синтез [Электронный ресурс] : монография / Н. Н. Мошак ; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - СПб. : Изд-во ГУАП, 2014. - 197 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
<a href="https://e.lanbook.com/">https://e.lanbook.com/</a>	Электронная библиотечная система
<a href="https://znanium.com/">https://znanium.com/</a>	Электронная библиотечная система
<a href="https://lib.guap.ru/jirbis2/">https://lib.guap.ru/jirbis2/</a>	Библиотека ГУАП

#### 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
1	Программный комплекс PGP
2	Менеджер паролей KeePass

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 таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Фонд аудиторий ГУАП для проведения занятий лекционного и семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Специализированная мебель; технические средства обучения, служащие для представления учебной информации большой аудитории; переносной набор демонстрационного оборудования	
2	Вычислительная лаборатория Специализированная мебель; технические средства обучения, служащие для представления учебной информации большой аудитории; лабораторное оборудование (ПЭВМ - 12 шт., объединенных в локальную вычислительную сеть с выходом в вычислительную сеть ГУАП и Интернет)	

## 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
Экзамен	Список вопросов к экзамену
Зачет	Список вопросов
Выполнение курсовой работы	Экспертная оценка на основе требований к содержанию курсовой работы по дисциплине.

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»	<ul style="list-style-type: none"> <li>– обучающийся глубоко и всесторонне усвоил программный материал;</li> <li>– уверенно, логично, последовательно и грамотно его излагает;</li> <li>– опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления;</li> <li>– умело обосновывает и аргументирует выдвигаемые им идеи;</li> <li>– делает выводы и обобщения;</li> </ul>

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
	– 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
	<ol style="list-style-type: none"> <li>1. Задача обеспечения секретности.</li> <li>2. Шифры подстановок. Примеры.</li> <li>3. Шифры перестановок. Примеры.</li> <li>4. Стойкость шифров. Модели атакующего</li> <li>5. Симметричные блочные шифры. Свойства, принципы построения.</li> <li>6. Итеративные блочные шифры. Сети Файстеля. Примеры.</li> <li>7. Шифр DES.</li> <li>8. Шифр ГОСТ 28147-89.</li> <li>9. Шифр FEAL</li> <li>10. Шифр IDEA.</li> <li>11. Шифр AES.</li> <li>12. Режимы блочного шифрования.</li> <li>13. Регистры сдвига с линейной обратной связью. Алгоритм Берлекэмпа-Мэсси.</li> <li>14. Поточные шифры. Свойства, принципы построения.</li> <li>15. Хэш-функции, свойства, принципы построения. MD5,</li> </ol>	<p>ПК-1.3.5  ПК-1.У.3  ПК-3.3.1  ПК-3.В.1  ПК-4.3.2  ПК-4.3.3  ПК-4.У.1</p>

	<p>MAC</p> <p>16. Задача идентификации. Парольная идентификация</p> <p>17. Асимметричные шифры. Свойства, принципы построения.</p> <p>18. Система RSA.</p> <p>19. Система Эль-Гамала</p> <p>20. Система Меркли-Хеллмана</p> <p>21. Система Мак-Элиса</p> <p>22. Задача обеспечения аутентификации. Цифровая подпись.</p> <p>23. Подпись RSA.</p> <p>24. Подпись DSA</p> <p>25. Подпись Эль-Гамала.</p> <p>26. Подпись ГОСТ Р 34.10-94</p> <p>27. Распределение ключей. Протокол Диффи-Хеллмана.</p> <p>28. Цифровой конверт</p> <p>29. Распределение ключей. Сертификаты.</p>	
--	---	--

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
	<p>1. Задача обеспечения секретности.</p> <p>2. Шифры подстановок. Примеры.</p> <p>3. Шифры перестановок. Примеры.</p> <p>4. Стойкость шифров. Модели атакующего</p> <p>5. Симметричные блочные шифры. Свойства, принципы построения.</p> <p>6. Итеративные блочные шифры. Сети Файстеля. Примеры.</p> <p>7. Шифр DES.</p> <p>8. Шифр ГОСТ 28147-89.</p> <p>9. Шифр FEAL</p> <p>10. Шифр IDEA.</p> <p>11. Шифр AES.</p> <p>12. Режимы блочного шифрования.</p>	<p>ПК-1.3.5</p> <p>ПК-1.У.3</p> <p>ПК-3.3.1</p> <p>ПК-3.В.1</p> <p>ПК-4.3.2</p> <p>ПК-4.3.3</p> <p>ПК-4.У.1</p>

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
	Исследование структуры, свойств и криптографической стойкости потокового шифра (по заданию преподавателя)

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
1	Задание 1. Основы модульной арифметики (50 вариантов) Пример задания: Вариант 1. Вычислить: $-17 \bmod 44$ $-31 \bmod 17$ $-49 \bmod 16$ $-76 \bmod 11$ $23 \bmod 50$
2	Задание 2. Нахождение мультипликативных обратных с помощью алгоритма Евклида (50 вариантов) Пример задания:
3	Вариант 1. Вычислить: $8011^{-1} \bmod 16732$
4	Задание 3. Быстрое возведение в степень (50 вариантов) Пример задания: Вариант 1. Вычислить: $19^{220} \bmod 73$
5	Задание 4. Системы с открытым ключом: системы RSA, Мак-Элиса, Эль-Гамала (индивидуальные варианты) Пример задания: Построить открытый и секретный ключи, зашифровать и расшифровать сообщение с помощью системы Мак-Элиса, для сообщения $m = 100101$ . Параметр $M$ определяется индивидуальным номером студента, остальные параметры системы выбрать самостоятельно.
	Задание 5. Системы ЭЦП: системы RSA, Эль-Гамала (индивидуальные варианты) Пример задания: Построить открытый и секретный ключи, подписать и проверить подпись сообщения с помощью системы Эль-Гамала. Сообщение $M$ определяется индивидуальным номером студента, размер открытого модуля $p > 19$ , остальные параметры ЭЦП выбрать самостоятельно.

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. Основные понятия криптографии

Раздел 2. Симметричные шифры

Раздел 3. Криптография с открытым ключом

Раздел 4. Криптографические протоколы

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 по журналу группы. Перед проведением лабораторной работы обучающемуся следует внимательно ознакомиться с методическими указаниями по ее выполнению. В соответствии с заданием обучающийся должен подготовить

необходимые данные, получить от преподавателя допуск к выполнению лабораторной работы, выполнить указанную последовательность действий, 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 лабораторным работам выполняется отчет. Титульный лист оформляется в соответствии с шаблоном (образцом), приведенным на сайте ГУАП (<https://new.guap.ru/>) в разделе «Нормативная документация» (<https://guap.ru/standart/doc>). Текстовые и графические материалы оформляются в соответствии с действующими ГОСТами и требованиями, приведенными на сайте ГУАП в разделе «Нормативная документация» (<https://guap.ru/standart/doc>).

#### Методические указания по прохождению лабораторных работ:

Методические указания к выполнению лабораторных работ по дисциплине «Криптографические методы защиты информации». Электронный ресурс кафедры №25.

11.3. Методические указания для обучающихся по прохождению курсового проектирования/выполнения курсовой работы

Курсовой проект/ работа проводится с целью формирования у обучающихся опыта комплексного решения конкретных задач профессиональной деятельности.

Курсовой проект/ работа позволяет обучающемуся:

- систематизировать и закрепить полученные теоретические знания и практические умения по дисциплине «Основы построения инфокоммуникационных систем и сетей» в соответствии с требованиями к уровню подготовки, установленными программой учебной дисциплины, программой подготовки бакалавра по направлению 11.03.02 «Инфокоммуникационные технологии и системы связи»;
- применить полученные знания, умения и практический опыт при решении комплексных задач, в соответствии с основными видами профессиональной деятельности по направлению 11.03.02 «Инфокоммуникационные технологии и системы связи»;
- углубить теоретические знания в соответствии с заданной темой;
- сформировать умения применять теоретические знания при решении нестандартных задач;
- приобрести опыт аналитической, расчётной, конструкторской работы и сформировать соответствующие умения;
- сформировать умения работы со специальной литературой, справочной, нормативной и правовой документацией и иными информационными источниками;
- сформировать умения формулировать логически обоснованные выводы, предложения и рекомендации по результатам выполнения работы;
- развить профессиональную письменную и устную речь обучающегося;
- развить системное мышление, творческую инициативу, самостоятельность, организованность и ответственность за принимаемые решения;
- сформировать навыки планомерной регулярной работы над решением поставленных задач.

#### Структура пояснительной записки курсовой работы

Курсовая работа в общем случае должна содержать:

- текстовый документ, объемом до 15 – 20 страниц печатного текста;
- графический материал, не менее 2 листов;
- возможно наличие электронной версии в форме презентации.

Текстовый документ может включать в указанной ниже последовательности:

- 1) задание на курсовую работу;
- 2) содержание;
- 3) введение, в котором раскрываются актуальность и значение темы, выполняется краткий аналитический обзор, формулируется цель;
- 4) основную часть, структура и содержание которой зависит от характера работы;
- 5) заключение, в котором содержатся выводы и рекомендации относительно возможностей использования материалов работы;
- 6) список использованных источников;
- 7) приложения, содержащие материалы иллюстративного и вспомогательного характера и/или листинги разработанных программ.

#### Способы реализации курсовых работ

Все курсовые работы по данной дисциплине связаны с разработкой программного обеспечения. Данные работы реализуются на языке программирования C/C++ или в среде Matlab.

#### Требования к оформлению пояснительной записки курсовой работы

Титульный лист оформляется в соответствии с шаблоном (образцом), приведенным на сайте ГУАП (<https://new.guap.ru/>) в разделе «Нормативная документация» (<https://guap.ru/standart/doc>). Текстовые и графические материалы оформляются в соответствии с действующими ГОСТами и требованиями, приведенными на сайте ГУАП в разделе «Нормативная документация» (<https://guap.ru/standart/doc>).

#### Методические указания по курсовому проектированию:

Для выполнения курсовой работы используется электронный ресурс каф.25:

Методические указания по курсовой работе по дисциплине «Криптографические методы защиты информации».

11.4. 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 обучающихся являются:

- учебно-методический материал по дисциплине.

11.5. 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.

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».

11.6. 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 – 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».

– зачет – это форма оценки знаний, полученных обучающимся в ходе изучения учебной дисциплины в целом или промежуточная (по окончании семестра) оценка знаний обучающимся по отдельным разделам дисциплины с аттестационной оценкой «зачтено» или «не зачтено».

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». Экзамен/зачет проводится в устной форме. При явке на экзамен/зачет обучающийся обязан иметь при себе зачетную книжку, которую он предъявляет преподавателю. Прием экзамена/зачета без зачетной книжки не допускается. Если со стороны обучающегося во время экзамена/зачета допущены нарушения учебной дисциплины (списывание, несанкционированное использование средств мобильной связи, аудио–плееров и других технических устройств), нарушения правил внутреннего распорядка ГУАП, предпринята попытка подлога документов, преподаватель вправе удалить обучающегося с экзамена/зачета с занесением в ведомость оценки «неудовлетворительно»/«не зачтено». По результатам экзамена/зачета положительная оценка/зачтено заносится преподавателем в ведомость и зачетную книжку. Отрицательная оценка/не зачтено заносится только в ведомость. неявка обучающегося на экзамен/зачет отмечается в ведомости словами «не явился», либо «н/я». Директор института на основе ведомости выясняет причину отсутствия обучающегося на экзамене/зачете и принимает решение о порядке последующей сдачи.



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