


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)  
«11» февраля 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

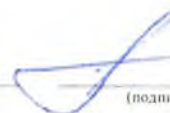
«Криптографические методы защиты информации»  
(Наименование дисциплины)

Код направления подготовки/ специальности	11.03.02
Наименование направления подготовки/ специальности	Инфокоммуникационные технологии и системы связи
Наименование направленности/ специализации	Программно-защищенные инфокоммуникации
Форма обучения	очная
Год приема	2026

Лист согласования рабочей программы дисциплины

Программу составил (а)

доц. к.т.н. доц. \_\_\_\_\_  
(должность, уч. степень, звание)



11.02.2026  
(подпись, дата)

А.А. Овчинников \_\_\_\_\_  
(инициалы, фамилия)

Программа одобрена на заседании кафедры № 25

«11» февраля 2026 г. протокол № 7/2025-26

Заведующий кафедрой № 25

д.т.н., проф. \_\_\_\_\_  
(уч. степень, звание)



11.02.2026  
(подпись, дата)

А.М. Тюрликов \_\_\_\_\_  
(инициалы, фамилия)

Заместитель директора института №2 по методической работе

доц. к.т.н. доц. \_\_\_\_\_  
(должность, уч. степень, звание)



11.02.2026  
(подпись, дата)

Н.В. Марковская \_\_\_\_\_  
(инициалы, фамилия)

## 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/специализации «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 зачета (5 семестр), экзамена (6 семестр).

Общая трудоемкость освоения дисциплины составляет 6 зачетных единиц, 216 часов.

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 знает цели и задачи проводимых исследований и разработок ПК-1.У.3 умеет 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 знает методы и средства планирования и организации исследований и разработок ПК-3.В.1 владеет 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 знает основные принципы, криптографические протоколы и программные средства обеспечения информационной безопасности сетевых устройств ПК-4.3.3 знает основы защиты информации и базовые угрозы ПК-4.У.1 умеет 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., Курс. Раб.	Зачет,	Экз., Курс. Раб.

## 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 5					
Раздел 1. Основные понятия криптографии	12		9		7
Тема 1.1 – Основные определения					
Тема 1.2 – Задачи информационной безопасности					
Текущий контроль	1				7
Раздел 2. Симметричные шифры	21		8		7
Тема 2.1. Исторические шифры					
Тема 2.2. Блочные шифры					
Тема 2.3. Поточковые шифры					
Итого в семестре:	34		17		21

Семестр 6					
Раздел 3. Криптография с открытым ключом Тема 3.1 - Математические основы систем с открытым ключом Тема 3.2 - Основные алгоритмы с открытым ключом	10		9		5
Текущий контроль	1				10
Раздел 4. Криптографические протоколы Тема 4.1 - Основные протоколы с открытым ключом Тема 4.2. – Специальные 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	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. 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.
2	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. Тема 2.2. Блочные шифры Понятие стойкости, предположения об исходных условиях криптоанализа, совершенная стойкость. Одноразовый

	<p>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</p> <p>Требования к поточным шифрам. Методы построения больших периодов в поточных шифрах. Регистры сдвига с линейной обратной связью (РСЛОС). m-последовательности. Алгоритм Берлекэмпа-Мессии. Построение поточковых шифров на основе РСЛОС. Нелинейное комбинирование РСЛОС: генератор Геффе, шифры с контролем тактов. Применение поточного шифрования.</p>
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-Хелмана. 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, (час)	№ раздела дисциплины
Семестр 5				
1	Задачи информационной безопасности	5	5	1
2	Исторические шифры	6	6	2
3	Блочные шифры	6	6	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. Выполнение курсового проекта/ курсовой работы

Цель курсовой работы: закрепление знаний, развитие умений и навыков, полученных на лекционных занятиях и лабораторных работах.

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. разделов 6-11.

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)
<a href="https://lib.guap.ru/jirbis2/index.php?option=com_irbis&amp;view=irbis&amp;Itemid=108">https://lib.guap.ru/jirbis2/index.php?option=com_irbis&amp;view=irbis&amp;Itemid=108</a> Режим доступа: для авторизованных пользователей.	Криптографические методы защиты информации : [ Электронный ресурс ] : учебное пособие / А. А. Овчинников ; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - 133 с. - Систем. требования: ACROBAT READER 5.X.	
[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/index.php?option=com_irbis&amp;view=irbis&amp;Itemid=108">https://lib.guap.ru/jirbis2/index.php?option=com_irbis&amp;view=irbis&amp;Itemid=108</a>	Мошак, Николай Николаевич	

Режим доступа: для авторизованных пользователей.	(проф.). Защищенные инфотелекоммуни кации. Анализ и синтез [Электронный ресурс] : монография / Н. Н. Мошак ; С.- Петерб. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - СПб. : Изд-во ГУАП, 2014. - 197 с.- Систем. требования: ACROBAT READER 5.X.	
--	---	--

#### 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://pro.guap.ru/">https://pro.guap.ru/</a>	Элементы электронного курса по дисциплине размещены <u>внутри ЭИОС ГУАП «Интегрированная среда обучения»</u>

#### 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.	Электронная информационно-образовательная среда ГУАП «Интегрированная среда обучения» ( <a href="https://pro.guap.ru/">https://pro.guap.ru/</a> ) разработана сотрудниками ГУАП (введена в эксплуатацию приказом ГУАП от 06.06.2017 № 05-215/17), перечень модулей и их функциональное назначение изложены по ссылке <a href="https://guap.ru/it/system/iso">https://guap.ru/it/system/iso</a>
2.	Официальный сайт образовательной организации в сети «Интернет» ( <a href="https://guap.ru/">https://guap.ru/</a> ), разработан сотрудниками ГУАП (введен в эксплуатацию Приказом ГУАП от 23.03.2023 № 05-145/23)
3.	LibreOffice 5 (Лицензия LGPLv3)
4.	Microsoft Office 2019 (договор ГУАП, информация о лицензии представлена по ссылке <a href="https://guap.ru/it/system/iso/po">https://guap.ru/it/system/iso/po</a> )
5.	MozillaFirefox(лицензии GPL/LGPL/MPL)

6.	MathWorks MATLAB (договор ГУАП, информация о лицензии представлена по ссылке <a href="https://guap.ru/it/system/iso/po">https://guap.ru/it/system/iso/po</a> )
----	--

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
1	Электронный каталог библиотеки ГУАП с доступом к базе полнотекстовых изданий ( <a href="https://lib.guap.ru">https://lib.guap.ru</a> ), доступ через личный кабинет читателя библиотеки ГУАП
2	Научная электронная библиотека «eLIBRARY» ( <a href="https://elibrary.ru/">https://elibrary.ru/</a> ), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП
3	ЭБС «Лань» ( <a href="https://e.lanbook.com/">https://e.lanbook.com/</a> ), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП
5	ЭБС Znanium ( <a href="https://znanium.ru/">https://znanium.ru/</a> ), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП
6	Образовательная платформа «Юрайт» ( <a href="https://urait.ru/">https://urait.ru/</a> ), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП

#### 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	Учебная аудитория для занятий лекционного типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации - Мультимедийная лекционная аудитория: Специализированная мебель; технические средства обучения, служащие для представления учебной информации большой аудитории; переносной набор демонстрационного оборудования; Обеспечен доступ в электронную информационно-образовательную среду ГУАП по точке доступа WiFi	
3	Учебная аудитория для лабораторных работ, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Специализированная мебель; технические средства обучения, служащие для представления учебной информации большой аудитории; лабораторное оборудование (ПЭВМ - 12 шт., объединенных в локальную вычислительную сеть; обеспечен доступ в электронную информационно-образовательную среду ГУАП по локальной вычислительной сети и точке доступа WiFi)	
4	Помещение для самостоятельной работы, Интернет-класс. Специализированная мебель, возможность подключения к	12-16 (ул. Большая Морская, д.67, лит. А)

	сети «Интернет» и доступ в электронную информационно-образовательную среду организации. 10 ПК, Принтер лазерный HPLJP4515n, Принтер HP LaserJetEnterprise 600 M602dn.	
5	Помещение для самостоятельной работы обучающихся - Читальный зал библиотеки ГУАП: специализированная мебель; персональные компьютеры – 10 шт., обеспечен доступ в электронную информационно-образовательную среду ГУАП по локальной вычислительной сети и точке доступа WiFi, а также к электронно-библиотечным системам, реферативной базе данных Scopus; копировальный аппарат Kyocera KM2035.	22-19 (ул. Большая Морская, д.67, лит. А)

#### 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»	Обучающийся: – глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно связывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий. – правильно выполнил от 90% до 100% тестовых заданий**.
«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.

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
	– правильно выполнил от 70% до 89% тестовых заданий <sup>**</sup> .
«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. – правильно выполнил от 51% до 69% тестовых заданий <sup>**</sup> .
«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. – правильно выполнил менее 51% тестовых заданий <sup>**</sup> .

### 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.	Задача обеспечения секретности.	ПК-1.3.5
2.	Шифры подстановок. Примеры.	ПК-1.У.3
3.	Шифры перестановок. Примеры.	ПК-3.3.1
4.	Стойкость шифров. Модели атакующего	ПК-3.В.1
5.	Симметричные блочные шифры. Свойства, принципы построения.	ПК-4.3.2 ПК-4.3.3
6.	Итеративные блочные шифры. Сети Файстеля. Примеры.	ПК-4.У.1
7.	Шифр DES.	
8.	Шифр ГОСТ 28147-89.	
9.	Шифр FEAL	
10.	Шифр IDEA.	
11.	Шифр AES.	
12.	Режимы блочного шифрования.	
13.	Регистры сдвига с линейной обратной связью. Алгоритм Берлекэмпа-Мэсси.	
14.	Потоковые шифры. Свойства, принципы построения.	
15.	Хэш-функции, свойства, принципы построения. MD5, MAC	
16.	Задача идентификации. Парольная идентификация	
17.	Асимметричные шифры. Свойства, принципы построения.	
18.	Система RSA.	
19.	Система Эль-Гамала	

20.	Система Меркли-Хеллмана	
21.	Система Мак-Элиса	
22.	Задача обеспечения аутентификации. Цифровая подпись.	
23.	Подпись RSA.	
24.	Подпись DSA	
25.	Подпись Эль-Гамала.	
26.	Подпись ГОСТ Р 34.10-94	
27.	Распределение ключей. Протокол Диффи-Хеллмана.	
28.	Цифровой конверт	
29.	Распределение ключей. Сертификаты.	

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

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

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

№ п/п	Примерный перечень тем для выполнения курсового проекта/ 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
	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:

- постановка задачи;
- основные сведения по теме лекции;
- результаты и выводы.

Лекционный материал изложен в пособии:

Криптографические методы защиты информации : [ Электронный ресурс] : учебное пособие / А. А. Овчинников ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - 133 с. - Систем. требования: ACROBAT READER 5.X. доступно после авторизации в библиотеке ГУАП <https://lib.guap.ru/>

11.2. Методические указания для обучающихся по участию в семинарах  
*Учебным планом не предусмотрено*

11.3. Методические указания для обучающихся по прохождению практических занятий  
*Учебным планом не предусмотрено*

#### 11.4. 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. В соответствии с заданием обучающийся должен подготовить необходимые данные, произвести необходимые расчеты, выполнить указанную последовательность действий, получить требуемые результаты, защитить полученные результаты.

##### 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:

Основы информационной безопасности. Исторические шифры : [ Электронный ресурс ] : учебно-методическое пособие / А. А. Овчинников ; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - СПб. : Изд-во ГУАП, 2018. - 40 с. - Систем. требования: ACROBAT READER 5.X., доступно после авторизации в библиотеке ГУАП <https://lib.guap.ru/>

Основы информационной безопасности. Симметричные шифры : [ Электронный ресурс ] : учебно-методическое пособие / А. А. Овчинников ; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - Санкт-Петербург : Изд-во ГУАП, 2019. - 28 с. - Систем. требования: ACROBAT READER 5.X. доступно после авторизации в библиотеке ГУАП <https://lib.guap.ru/>

#### 11.5. Методические указания для обучающихся по выполнению курсового проекта/ 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;
- 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>).

11.6. 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.

В процессе выполнения самостоятельной работы у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет ему развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Основными методическими материалами, направляющими самостоятельную работу обучающихся, являются источники из перечня печатных и электронных учебных изданий, указанных в таблице 8. Кроме этого, обучающийся может пользоваться электронными ресурсами, указанными в таблицах 9 и 11.

11.7. 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 включает в себя:

- контроль посещаемости;
- письменное выполнение заданий лабораторных работ с защитой отчетов;

Результаты текущего контроля учитываются при проведении промежуточной аттестации в соответствии с требованиями РДО ГУАП. СМК 3.76 «Положение о текущем контроле успеваемости и промежуточной аттестации обучающихся ГУАП, осваивающих образовательные программы высшего образования».

11.8. 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».

– 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 РДО ГУАП. СМК 3.76 «Положение о текущем контроле успеваемости и промежуточной аттестации обучающихся ГУАП, осваивающих образовательные программы высшего образования».

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