

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

проф. д.т.н., доц.

(должность, уч. степень, звание)

С.В. Беззатеев

(инициалы, фамилия)

(подпись)

«27» июня 2024 г

Лист согласования рабочей программы дисциплины

Программу составил (а)

д.т.н., доц.

(должность, уч. степень, звание)

27.06.2024

(подпись, дата)

С.В. Беззатеев

(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

«Методы и средства криптографической защиты информации»  
(Наименование дисциплины)

Код направления подготовки/ специальности	10.05.03
Наименование направления подготовки/ специальности	Информационная безопасность автоматизированных систем
Наименование направленности	Безопасность открытых информационных систем
Форма обучения	очная
Год приема	2024

## Аннотация

Дисциплина «Методы и средства криптографической защиты информации» входит в образовательную программу высшего образования – программу специалитета по направлению подготовки/ специальности 10.05.03 «Информационная безопасность автоматизированных систем» направленности «Безопасность открытых информационных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ОПК-10 «Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности»

Содержание дисциплины охватывает круг вопросов, связанных с основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

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

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

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа.

Язык обучения по дисциплине «русский»

## 1. Перечень планируемых результатов обучения по дисциплине

### 1.1. Цели преподавания дисциплины

Основной целью дисциплины «Криптографическая защита информации» является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Задачи дисциплины «Криптографическая защита информации» - дать основы:

- системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;
- принципов разработки шифров;
- математических методов, используемых в криптографии.

1.2. Дисциплина входит в состав обязательной части 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
Общепрофессиональные компетенции	ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.3.1 знать криптографические модели и алгоритмы ОПК-10.У.1 уметь оценивать эффективность применения отдельных средств криптографической защиты информации в автоматизированных информационных системах ОПК-10.В.1 владеть методами реализации систем защиты информации с помощью криптографических алгоритмов

## 2. Место дисциплины в структуре ОП

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

- Введение в специальность
- Информатика
- Технологии и методы программирования

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

- Производственная (конструкторская) практика
- Научно-технический семинар
- Научно-исследовательская работа
- Производственная преддипломная практика
- Методы и средства проектирования информационных систем

## 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
		№6
1	2	3
<b>Общая трудоемкость дисциплины, ЗЕ/ (час)</b>	4/ 144	4/ 144
<b>Из них часов практической подготовки</b>		
<b>Аудиторные занятия, всего час.</b>	85	85
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)	17	17
экзамен, (час)	36	36
<b>Самостоятельная работа, всего (час)</b>	23	23
<b>Вид промежуточной аттестации:</b> 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 6					
Раздел 1. Общие сведения. Введение	4		4		4
Раздел 2 Симметричная криптография	8		8		4
Раздел 3. Несимметричная криптография	8		8		4
Раздел 4. Электронно-цифровая подпись	8		8		4
Раздел 5.Криптографические протоколы	8		8		7
Выполнение курсовой работы				17	
Итого в семестре:	34		34	17	23
Итого	34	0	34	17	23

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. Общие сведения. Введение</p> <p>Тема 1. Основные понятия и определения криптографии.</p> <p>Тема 2. Этапы развития криптографии. Роль математики в развитии методов защиты информации. Новые направления в криптографии.</p> <p>Тема 3. Криптографические примитивы и криптографические протоколы по защите информации.</p> <p>Тема 4. Двухсторонние и многосторонние протоколы. Типы предполагаемых противников. Формальные методы оценки качества криптографических протоколов.</p> <p>Тема 5. Шифры. Примеры. Стойкость шифра. Классификация методов дешифрования</p>
2	<p>Раздел 2 Симметричная криптография</p> <p>Тема 6. Блочные и поточные криптосистемы и их классификация. Описание DES - RC4 AES, ГОСТ 28147-89, «Кузнечик» и др. Режимы использования и их сравнение (ECB, CBC, OFB, ...).</p> <p>Тема 7 Криптографические свойства функций.</p> <p>Тема 8 Хэш функции. Хэш цепочки. Дерево Меркле. Стандарты хэш функций</p>
3	<p>Раздел 3. Несимметричная криптография</p> <p>Тема 9 Основные понятия криптографии с открытым ключом. Сравнение криптосистем с открытым и секретным ключом.</p> <p>Тема 10. Однонаправленные (односторонние) функции по Нидхэму. Однонаправленные функции, основанные на сложности задачи дискретного логарифмирования. Применения в современных технологиях.</p> <p>Тема 11. Однонаправленные (односторонние) функции с секретом и их применение для цели шифрования информации. Схемы RSA, Рабина, Эль Гамала, МакЭлайса, Меркля – Хеллмана.</p> <p>Тема 12. Некоторые методы быстрой модульной арифметики и их применение для ускорения криптографических алгоритмов</p>
4	<p>Раздел 4. Электронно-цифровая подпись</p> <p>Тема 13. Понятия о цифровой подписи на основе однонаправленной функции с секретом. Классификация атак на схемы цифровой подписи.</p> <p>Тема 14. Сравнение стандартов цифровой подписи США (FIPS PUB 186) и России (ГОСТ Р 34.10-94). Стандарт цифровой подписи ГОСТ Р 34.10-2001, 2015 на основе эллиптических кривых.</p> <p>Тема 15. Схемы подписи Фиата-Шамира, Файге-Фиата-Шамира и др. Схема Шнорра.</p> <p>Тема 16. Подпись вслепую (blind signature) и ее применения.</p> <p>Тема 17. Схемы конфиденциальной подписи (undeniable signature) и их применение. Протоколы проверки и отвержения как примеры протоколов доказательств с нулевым разглашением. Схемы Шаума.</p> <p>Тема 18. Схемы подписи, в которых подделка подписи может быть доказана.</p> <p>Тема 19 Схемы мультиподписи (multisignature scheme).</p> <p>Тема 20. Групповая подпись (group signature scheme).</p> <p>Тема 21. Подпись по доверенности (proxy signature)</p>
5	<p>Раздел 5. Криптографические протоколы</p> <p>Тема 22. Управление ключами. Доказуемо безопасные генераторы ключей. Некоторые способы сокращения объемов хранимых</p>

	<p>ключей.</p> <p>Тема 23. Протоколы распределения криптографических ключей.</p> <p>Тема 24. Криптографическая инфраструктура на основе механизма открытых ключей(РКИ). Модели криптографической инфраструктуры.</p> <p>Тема 25. Протоколы, основанные на идентификационной информации (ID-based cryptosystems).</p> <p>Тема 26. Протоколы с разделением секрета. Пороговые схемы.</p> <p>Тема 27. Криптосистемы и протоколы на эллиптических кривых.</p> <p>Тема 28. Протоколы идентификации и аутентификации.</p> <p>Тема 29. Протоколы честного обмена секретами.</p> <p>Тема 30. Интерактивные схемы доказательств</p> <p>Тема 31. Протоколы электронного тайного голосования .</p> <p>Тема 32. Понятие о протоколах электронных платежей</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 6				
1	Нападения и угрозы безопасности в компьютерных системах	2		1
2	Модель нарушителя информационной безопасности	2		1
3	Криптография и криптоанализ	2		2
4	Методы криптографии	2		2
5	Методы криптоанализа	2		2
6	Криптография и теория сложности	2		2
7	Криптография с секретным ключом	2		3
8	Протоколы симметричного шифрования	2		3
9	Блочные и потоковые шифры.	2		3
8	Сложность теоретико-числовых алгоритмов. Однонаправленные функции.	2		3
9	Алгоритм RSA. Шифросистема Эль-Гамала	2		4
10	Криптоанализ алгоритмов с открытым ключом	4		4

11	Хэш-функции. Аутентификация сообщений	4		5
12	Электронная цифровая подпись	4		5
13	Теоретико-информационная стойкость. Стойкость и надежность	4		5
Всего		34		

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

Цель курсовой работы: изучение и реализация методов криптографической защиты информации в различных предметных областях.

Поставленная цель достигается путем решения следующих задач:

1. Обозначить сущность проблемы и рассмотреть задачи защиты информации в информационных и телекоммуникационных системах.
2. Установить угрозы информации и способы их воздействия на объекты защиты информации.
3. Рассмотреть методы и средства защиты информации.
4. Раскрыть концепцию информационной безопасности предприятия.
5. Реализовать алгоритмы криптографической защиты информации согласно выданному заданию.

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 6, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	13	13
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	5	5
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	5	5
Всего:	23	23

#### 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/	Библиографическая ссылка	Количество
-------	--------------------------	------------

URL адрес		экземпляров в библиотеке (кроме электронных экземпляров)
004.05В 75	Воронов, А. В. Основы защиты информации: учебное пособие/ А. В. Воронов, Н. В. Волошина. - СПб.: ГОУ ВПО "СПбГУАП", 2009. - 78 с.	(74)
004 Ш 22	Шаньгин, В. Ф. Информационная безопасность [Текст]: научно-популярная литература / В. Ф. Шаньгин. - М.: ДМК Пресс, 2014. - 702 с	(8)
Х Я 47	Яковец, Е. Н. Правовые основы обеспечения информационной безопасности Российской Федерации [Текст] : учебное пособие / Е. Н. Яковец. - М. : Юрлитинформ, 2010. - 336 с.	(9)
	<a href="http://e.lanbook.com/books/element.php?pl1_id=3032">http://e.lanbook.com/books/element.php?pl1_id=3032</a> Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : ДМК Пресс, 2012. — 592 с	
004 М 48	Мельников, В. П. Защита информации [Текст] : учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; ред. В. П. Мельников. - М. : Академия, 2014. - 304 с.	(5)
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)
	<a href="http://e.lanbook.com/books/element.php?pl1_id=4959">http://e.lanbook.com/books/element.php?pl1_id=4959</a> Титов, А.А. Инженерно-техническая защита информации [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2010. — 195 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="http://www.intuit.ru/studies/courses/10/10/info">http://www.intuit.ru/studies/courses/10/10/info</a>	Владимир Галатенко. Основы информационной безопасности (курс лекций, с дистанционным обучением)

## 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 таблице 12.

Таблица 12 – Состав материально-технической базы

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

## 10. Оценочные средства для проведения промежуточной аттестации

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

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Экзамен	Список вопросов к экзамену; Экзаменационные билеты; Задачи; Тесты.
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 привязывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий.

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
«хорошо» «зачтено»	<ul style="list-style-type: none"> <li>– обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы;</li> <li>– не допускает существенных неточностей;</li> <li>– увязывает усвоенные знания с практической деятельностью направления;</li> <li>– аргументирует научные положения;</li> <li>– делает выводы и обобщения;</li> <li>– владеет системой специализированных понятий.</li> </ul>
«удовлетворительно» «зачтено»	<ul style="list-style-type: none"> <li>– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы;</li> <li>– допускает несущественные ошибки и неточности;</li> <li>– испытывает затруднения в практическом применении знаний направления;</li> <li>– слабо аргументирует научные положения;</li> <li>– затрудняется в формулировании выводов и обобщений;</li> <li>– частично владеет системой специализированных понятий.</li> </ul>
«неудовлетворительно» «не зачтено»	<ul style="list-style-type: none"> <li>– обучающийся не усвоил значительной части программного материала;</li> <li>– допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении;</li> <li>– испытывает трудности в практическом применении знаний;</li> <li>– не может аргументировать научные положения;</li> <li>– не формулирует выводов и обобщений.</li> </ul>

### 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	<p>Основные понятия и определения криптографии.</p> <p>Виды криптосистем. Задачи, решаемые методами криптографии.</p> <p>Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений.</p> <p>История криптографии. Основные этапы становления науки криптографии.</p> <p>Классификация шифров замены. Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат. Шифр Хилла. Шифр Виженера. Частотный анализ. Тест Казиски.</p> <p>Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ.</p> <p>Шифры гаммирования. Шифр Вернама. Подходы к его криптоанализу.</p> <p>Композиции шифров. Enigma. Шифр Хейглина.</p> <p>Математическая модель шифра.</p> <p>Атаки и угрозы шифрам.</p> <p>Блочные шифры и их ключевая система. Замены и перестановки.</p> <p>Сеть Файстеля. Шифры DES, ГОСТ 28147-89.</p> <p>Шифр AES</p>	ОПК-10.3.1

	<p>Шифр IDEA.</p> <p>Подходы к криптоанализу блочных шифров.</p> <p>Дифференциальный криптоанализ. Линейный криптоанализ.</p> <p>Режимы шифрования.</p> <p>Многokратное шифрование. Композиция блочных шифров.</p> <p>Совершенные шифры. Пример совершенного шифра.</p> <p>Энтропийные характеристики шифров. Идеальные шифры.</p>	
2	<p>Избыточность языка.</p> <p>Оценка числа ложных ключей и расстояние единственности.</p> <p>Безусловно стойкие и вычислительно стойкие шифры.</p> <p>Псевдослучайные последовательности (ПСП).</p> <p>Характеристики генераторов ПСП (ПСГ). Требования к криптографическим ПСП. Примеры ПСГ и криптографических ПСГ.</p> <p>Поточные шифры. Общая схема поточного шифра.</p> <p>Синхронные и самосинхронизирующиеся шифры.</p> <p>Регистры сдвига с обратной линейной связью (РСЛОС).</p> <p>ПСГ на основе РСЛОС.</p> <p>Шифр A5.</p> <p>Нелинейные регистры сдвига.</p> <p>Шифр RC4.</p> <p>Теория имитостойкости Симмонса. Имитация и подмена сообщения. Характеристики имитостойкости.</p> <p>Совершенная имитостойкость.</p> <p>Коды аутентификации сообщений.</p> <p>Защитные контрольные суммы.</p> <p>Криптографические хэш-функции и требования к ним.</p> <p>Подходы к проектированию хэш-функций.</p> <p>Хэш-функции на основе блочного шифра.</p> <p>Ключевые хэш-функции.</p> <p>Понятие односторонней функции и односторонней функции с "лазейкой". Проблемы факторизации целых чисел и логарифмирования в конечных полях.</p>	ОПК-10.У.1
3	<p>Криптосистема Диффи-Хэллмана. Пример.</p> <p>Криптосистема RSA. Пример.</p> <p>Криптосистема Эль-Гамала. Пример.</p> <p>Криптосистема Рабина. Пример.</p> <p>Криптосистема Гольдвассер-Микали. Пример.</p> <p>Криптосистема Блюма-Гольдвассер. Пример.</p> <p>Рюкзачные шифры. Криптосистема Меркла-Хэллмана.</p> <p>Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП.</p> <p>Подпись RSA, Эль-Гамала.</p> <p>Подпись Фиата-Шамира.</p> <p>Подпись Онга-Шнорра-Шамира.</p> <p>Неотрицаемая подпись Шаума-ван-Антверпена.</p> <p>Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94.</p> <p>Эллиптическая кривая над конечным полем. Операции на эллиптической кривой. Сумма точек. Кратная точка.</p> <p>Проблема дискретного логарифмирования на эллиптической кривой. Переход от шифра (ЭЦП) в <math>Z_p</math> к шифру (ЭЦП) на эллиптической кривой.</p> <p>Шифр Эль-Гамала на эллиптической кривой.</p> <p>Стандарты ЭЦП на эллиптической кривой: ГОСТ Р 34.10-</p>	ОПК-10.В.1

2001, ECDSA.
--------------

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
	<ol style="list-style-type: none"> <li>1. Самостоятельный анализ исторического шифра. Шифры простой замены, Плейфера, Виженера, Полибия, Хилла, Вернама, «Решетка», Хейглина, Enigma и др.</li> <li>2. Режимы блочного шифрования ГОСТ 28147-89, DES.</li> <li>3. Алгоритм разворачивания ключа шифра AES.</li> <li>4. Исследование энтропийных свойств русского и английского языков.</li> <li>5. Генераторы ПСП и их свойства.</li> <li>6. Самосинхронизирующиеся поточные шифры.</li> <li>7. Построение чистого шифра. Оценка трудоемкости подбора ключа при известной паре «открытый – зашифрованный текст».</li> <li>8. Теория имитостойкости Симмонса. Оценка вероятности имитации ключевых хэш-функций.</li> <li>9. Построение защитных контрольных сумм на основе бесключевой хэш-функции.</li> <li>10. Построение криптографической хэш-функции на основе односторонней функции.</li> <li>11. Построение класса больших простых чисел.</li> <li>12. Вероятностные тесты на простоту. Построение доказуемо простых чисел.</li> <li>13. Построение ключевой информации для ЭЦП.</li> <li>14. Вычисления на эллиптической кривой.</li> <li>15. Инфраструктура открытых ключей.</li> </ol>

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
	<ul style="list-style-type: none"> <li>• В протоколе шифра Шамира сообщение пересылается               <ol style="list-style-type: none"> <li>а) два раза</li> <li>б) три раза</li> <li>в) один раз</li> <li>г) четыре раза.</li> </ol> </li> <li>• Надежность системы RSA базируется на том, что               <ol style="list-style-type: none"> <li>а) сложно определить по данному числу, является ли оно простым</li> <li>б) задача дискретного логарифмирования сложна</li> <li>в) задача разложения на множители числа, являющегося произведением двух простых, сложна.</li> </ol> </li> <li>• Укажите правильный порядок ответов в правом столбике:</li> </ul>	

RC4	шифр с открытым ключом	
AES	поточковый шифр	
RSA	совершенный шифр	
Шифр Вернама	блоковый шифр	

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.

## 1. Методические указания для обучающихся по освоению дисциплины

Основной целью дисциплины «Криптографическая защита информации» является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Задачи дисциплины «Криптографическая защита информации» - дать основы:

- системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;
- принципов разработки шифров;
- математических методов, используемых в криптографии.

### 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 обучающимся 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:

- Изложение лекционного материала;
- Представление теоретического материала преподавателем в виде слайдов;
- Освоение теоретического материала по практическим вопросам;
- Список вопросов по теме для самостоятельной работы студента (Табл.21).

### **Методические указания для обучающихся по прохождению 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 у 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**

Задание на лабораторные работы представлены по темам изучаемой дисциплины и представляют собой программную реализацию изучаемых алгоритмов криптографической защиты информации:

Тема 1: Введение в криптографию. Свойства информации. Ситуационные задачи на определение свойств информации, подлежащей криптографическому преобразованию.

Тема 2: История криптографии. Исторические шифры. Исторические шифры и их криптоанализ. Компьютерная реализация и вскрытие шифров замены. Компьютерная реализация и вскрытие шифров перестановки и гаммирования.

Тема 3: Математическая модель шифра. Теория секретности Шеннона. Построение моделей шифров. Вероятностные характеристики текстов. Определение избыточности текста, языка. Вероятностные характеристики простых шифров. Расчет параметров шифров. Расстояние единственности, определение количества ложных ключей.

Тема 4: Блочные шифры. Блочные шифры. ГОСТ 28147-89, IDEA и DES. Многочлены над  $Z_2$  и блочный шифр AES.

Тема 5: Псевдослучайные последовательности и поточные шифры. Псевдослучайные генераторы на основе РСЛОС. Оценка свойств гаммы шифра. Изучение современных поточных криптосистем.

Тема 6: Теория имитостойкости Симмонса и криптографические хэш-функции. Вычисление параметров имитостойкости, помехоустойчивости шифров. Построение криптографической хэш-функции на основе блочного шифра и исследование ее свойств методами математической статистики и теории информации.

Тема 12: Асимметричные (с открытым ключом) шифры. Вычисления в  $Z_n$ . Шифр с открытым ключом: RSA, Эль-Гамала, Шамира, Диффи-Хэллмана, Рабина, Гольдвассер-Микали, Блюма-Гольдвассер, Меркла-Хэллмана. Генерация больших простых чисел для асимметричных криптосистем.

Тема 13: Схемы цифровой подписи. Реализация схемы ЭЦП: RSA, Эль-Гамала и ее варианты, Фиата-Шамира, Онга-Шнорра-Шамира, Шнорра. Неотрицаемая подпись Шаума-ван-Антверпена.

Тема 14: Эллиптические кривые над конечным полем. Шифры и ЭЦП на их основе. Эллиптические кривые над конечным полем. Преобразование криптосистемы над  $Z_p$  в криптосистему на эллиптической кривой.

Тема 15: Введение в криптографические протоколы. Изучение примитивных протоколов. Изучение криптосистемы Kerberos.

### **Структура и форма отчета о лабораторной работе**

Отчёт по лабораторной работе оформляется индивидуально каждым студентом, выполнившим необходимые (независимо от того, выполнялся ли эксперимент индивидуально или в составе группы студентов). Страницы отчёта следует пронумеровать (титульный лист не нумеруется, далее идет страница 2 и т.д.). Титульный лист отчёта должен содержать фразу: «Отчёт

по лабораторной работе «Название работы», чуть ниже: Выполнил студент группы (номер группы) (Фамилия, инициалы)». Внизу листа следует указать текущий год. Например, Отчёт по лабораторной работе № (номер работы) «Введение в спектральный анализ», Выполнил студент группы 5221 Иванов И.И. Вторая страница текста, следующая за титульным листом, должна начинаться с пункта: Цель работы. Отчёт, как правило, должен содержать следующие основные разделы:

1. Цель работы;
2. Теоретическая часть;
3. Программное обеспечение, используемое в работе;
4. Результаты;
5. Выводы.

В случае необходимости в конце отчёта приводится перечень литературы.

### **Требования к оформлению отчета о лабораторной работе**

Теоретическая часть должна содержать минимум необходимых теоретических сведений о предметной области. Не следует копировать целиком или частично методическое пособие (описание) лабораторной работы или разделы учебника.

В разделе Программное обеспечение необходимо описать, с помощью каких инструментальных средств и каким образом были разработаны модели и получены результаты. Рисунки, блок-схемы, описание модели и её особенностей, необходимость отладки – все это должно быть представлено в указанном разделе.

Раздел Результаты включает в себя скриншоты программного приложения, полученные при выполнении лабораторной работы. Рисунки, графики и таблицы нумеруются и подписываются заголовками.

Выводы не должны быть простым перечислением того, что сделано. Здесь важно отметить, какие новые знания о предмете исследования были получены при выполнении работы, к чему привело обсуждение результатов, насколько выполнена заявленная цель работы. Выводы по работе каждый студент делает самостоятельно. В случае необходимости в конце отчёта приводится Список литературы, использованной при подготовке к работе. В тексте отчёта делаются краткие ссылки на литературу (учебники, справочники, иные источники...) номером в квадратных скобках, напр., [1]. Литературные источники нумеруются по мере их появления в тексте отчёта. В конце отчёта даётся их подробный список. На все источники списка литературы должны быть ссылки в тексте отчёта, там, где это необходимо.

При сдаче отчёта преподаватель может сделать устные и письменные замечания, задать дополнительные вопросы. Все ответы на дополнительные вопросы, обсуждения выполняются студентом на отдельных листах, включаемых в отчёт (при этом в тексте основного отчёта делается сноска или другой значок, которому будет соответствовать новый материал). При этом



письменные замечания преподавателя должны остаться в тексте для ясности динамики работы над отчётом.

Объём отчёта должен быть оптимальным для понимания того, что и как сделал студент, выполняя работу. Обязательные требования к отчёту включают общую и специальную грамотность изложения, а также аккуратность оформления.

После приёма преподавателем отчёт хранится на кафедре.

### **Методические указания для обучающихся по прохождению курсового проектирования/ 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 профессиональным учебным дисциплинам и модулям в соответствии с требованиями к уровню подготовки, установленными программой учебной дисциплины, программой подготовки специалиста соответствующего уровня, квалификации;

- применить полученные знания, умения и практический опыт при решении комплексных задач, в соответствии с основными видами профессиональной деятельности по направлению/ специальности/ программе;

- 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 / проекта**

Изучение курса «Управление данными» заканчивается выполнением курсовой работы по проектированию баз данных различного назначения.

Содержание курсового проекта излагается в программе курса для соответствующих специальностей и должно соответствовать приведенному в приложении заданию на курсовое проектирование. Бланк задания на курсовое проектирование должен быть подшит в пояснительную записку перед введением.

Отчёт по курсовой работе оформляется каждым студентом индивидуально и содержит описание лично выполненной работы, которая включает:

- титульный лист;
- индивидуальное задание;
- пояснительную записку;
- программы и спецификации на электронном носителе;

Пояснительная записка содержит разделы:

- содержание с указанием страниц и разделов;
- введение;
- основную часть;
- список литературы;
- приложения.

В содержании должна быть отражена структура пояснительной записки. Введение должно характеризовать ту сферу человеческой деятельности, для которой будет проектироваться приложение.

Список литературы, помимо книг, использованных при работе над курсовой работой, должен включать ссылки на все электронные материалы, использованные при проектировании.

Листинги программ с подробными комментариями должны быть приведены в приложениях.

### **Требования к оформлению пояснительной записки курсовой работы / проекта**

В виду принадлежности курсового проекта к дисциплинам связанным с информационными технологиями и электронно-вычислительными машинами пояснительная записка должна быть оформлена при помощи любого программного инструмента и распечатана на листах формата А4 (210×297 мм), листы должны быть пронумерованы и сшиты. Поля листа должны составлять левое 25 мм, верхнее и нижнее 20 мм, правое 15 мм. Текст записки должен быть набран удобочитаемым шрифтом по размеру и начертанию соответствующий «Times New Roman» в 14 пт. Межстрочный интервал должен соответствовать полуторному. В записке также должен быть предусмотрен карман для помещения в него диска с работоспособным приложением и всеми исходными текстами программ. Допускается помещать на дискету архив в формате zip или rar.

Полный листинг программы должен включать в себя распечатку всех файлов программ, из которых состоит проект. Формы проекта должны быть распечатаны в двух видах: в виде формы и в виде тестового файла. Все файлы форм должны быть сгруппированы в следующей последовательности:

сначала форма в процессе разработки, затем форма в текстовом виде и в завершении текст модуля связанный с формой. В записке фрагменты текстов программы, а также тексты распечаток модуля и формы должны быть выполнены шрифтом «Courier New» размером 10 пт., через одинарный интервал.

### **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;
- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

### **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 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