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

Кафедра № 33

УТВЕРЖДАЮ
Руководитель образовательной программы

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

С.В. Беззатеев
(инициалы, фамилия)

(подпись)

«20» февраля 2026 г

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/ специализации	Безопасность открытых информационных систем
Форма обучения	очная
Год приема	2026

Санкт-Петербург– 2026

Лист согласования рабочей программы дисциплины

Программу составил (а)

зав.кафедрой, д.т.н.,проф. (должность, уч. степень, звание) — 20.02.26 (подпись, дата) — С.В. Беззатеев (инициалы, фамилия)

Программа одобрена на заседании кафедры № 33
«20» февраля 2026 г, протокол № 7

Заведующий кафедрой № 33

д.т.н.,проф. (уч. степень, звание) — 20.02.26 (подпись, дата) — С.В. Беззатеев (инициалы, фамилия)

Заместитель директора института №3 по методической работе

доц.,к.т.н. (должность, уч. степень, звание) — 20.02.26 (подпись, дата) — Н.В. Решетникова (инициалы, фамилия)

Аннотация

Дисциплина «Методы и средства криптографической защиты информации» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 10.03.01 «Информационная безопасность» направленности «Безопасность компьютерных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ОПК-9 «Способен применять средства криптографической и технической защиты информации для решения 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 6 зачетных единиц, 216 часов.

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-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.З.3 знает основные понятия и задачи криптографии, математические модели криптографических систем ОПК-9.З.4 знает основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы ОПК-9.З.5 знает национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения ОПК-9.У.2 умеет применять математические модели для оценки стойкости СКЗИ ОПК-9.У.3 умеет использовать СКЗИ в автоматизированных системах

2. Место дисциплины в структуре ОП

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

- Информатика
- Дискретная математика
- 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-исследовательская работа
– Производственная преддипломная практика

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
Общая трудоемкость дисциплины, ЗЕ/ (час)	6/ 216	2/ 72	4/ 144
Из них часов практической подготовки			
Аудиторные занятия, всего час.	119	51	68
в том числе:			
лекции (Л), (час)	68	34	34
практические/семинарские занятия (ПЗ), (час)			
лабораторные работы (ЛР), (час)	34	17	17
курсовой проект (работа) (КП, КР), (час)	17		17
экзамен, (час)	36		36
Самостоятельная работа, всего (час)	61	21	40
***Вид промежуточной аттестации*:** 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)
Семестр 5					
Раздел 1. Общие сведения. Введение	4		2		2
Раздел 2 Симметричная криптография	8		4		5
Раздел 3. Несимметричная криптография	8		7		7
Раздел 4. Цифровая подпись	8		2		4
Раздел 5.Криптографические протоколы	8		2		3
Итого в семестре:	34		17		21
Семестр 6					
Раздел 4. Цифровая подпись			8		10
Раздел 5.Криптографические протоколы			9		10
Выполнение курсовой работы				17	
Итого в семестре:	34		17	17	40
Итого	68	0	34	17	61

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. Общие сведения. Введение Тема 1. Основные понятия, определения и задачи криптографии. Тема 2. Этапы развития криптографии. Роль математики в развитии методов защиты информации. Новые направления в криптографии. Тема 3. Криптографические примитивы и криптографические протоколы по защите информации. Тема 4. Двухсторонние и многосторонние протоколы. Типы предполагаемых противников. Формальные методы оценки качества криптографических протоколов. Тема 5. Шифры. Примеры. Стойкость шифра. Классификация методов дешифрования
2	Раздел 2. Симметричная криптография Тема 6. Блочные и поточные криптосистемы и их классификация. Описание DES, AES, ГОСТ 28147-89, ГОСТ 34.12-2018, RC 4 и др. Режимы использования и их сравнение (ECB,CBC, OFB, …). Тема 7. Криптографические свойства функций. Тема 8 Хэш функции. Хэш цепочки. Дерево Меркле. Стандарты хэш функций
3	Раздел 3. Несимметричная криптография Тема 9 Основные понятия криптографии с открытым ключом. Сравнение криптосистем с открытым и секретным ключом. Тема 10. Однонаправленные (односторонние) функции по Нидхэму. Однонаправленные функции, основанные на сложности задачи дискретного логарифмирования. Применения в современных технологиях. Тема 11. Однонаправленные (односторонние) функции с секретом и их применение для цели шифрования информации. Схемы RSA, Рабина, Эль Гамаля, Мак-Элиса, Меркля – Хеллмана. Тема 12. Некоторые методы быстрой модульной арифметики и их применение для ускорения криптографических алгоритмов
4	Раздел 4. Цифровая подпись Тема 13. Понятия о цифровой подписи на основе однонаправленной функции с секретом. Классификация атак на схемы цифровой подписи. Тема 14. Сравнение стандартов цифровой подписи США (FIPS PUB 186) и России (ГОСТ 34.10-2018). Стандарт цифровой подписи ГОСТ Р 34.10-2001, 2015 на основе эллиптических кривых. Тема 15. Схемы подписи Фиата-Шамира, Файге-Фиата-Шамира и др. Схема Шнорра. Тема 16. Подпись вслепую (blind signature) и ее применения. Тема 17. Схемы конфиденциальной подписи (undeniable signature) и их применение. Протоколы проверки и отвержения как примеры протоколов доказательств с нулевым разглашением. Схемы Шаума. Тема 18. Схемы подписи, в которых подделка подписи может

	быть доказана. Тема 19 Схемы мультиподписи (multisignature scheme). Тема 20. Групповая подпись (group signature scheme). Тема 21. Подпись по доверенности (proxy signature)
5	Раздел 5.Криптографические протоколы Тема 22. Управление ключами. Доказуемо безопасные генераторы ключей. Некоторые способы сокращения объемов хранимых ключей. Тема 23. Протоколы распределения криптографических ключей. Тема 24. Криптографическая инфраструктура на основе механизма открытых ключей(PKI). Модели криптографической инфраструктуры. Тема 25. Протоколы, основанные на идентификационной информации (ID-based cryptosystems). Тема 26. Протоколы с разделением секрета. Пороговые схемы. Тема 27. Криптосистемы и протоколы на эллиптических кривых. Тема 28. Протоколы идентификации и аутентификации. Тема 29. Протоколы честного обмена секретами. Тема 30. Интерактивные схемы доказательств Тема 31. Протоколы электронного тайного голосования . Тема 32. Понятие о протоколах электронных платежей

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	Исторические шифры и их криптоанализ	3		1
2	Симметричная криптография: уязвимости и атаки	7		2
3	Хэш-функции и криптосистемы с открытым ключом	7		2,3
Семестр 6				
4	Криптосистемы с открытым ключом: цифровая подпись	4		4
5	Криптографические методы защиты информации, основанные на эллиптических	6		4,5

	кривых			
6	Криптографические протоколы: доказательство с нулевым разглашением, схема разделения секрета, обмен ключами,	7		5
	Всего	34		

4.5. Курсовое проектирование/ выполнение курсовой работы

Цель курсовой работы: изучение и программная 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.

Требования к содержанию, оформлению и сдаче курсовой работы

- Курсовая работа (проект) (далее - КР) выполняется в группах до 3-х студентов
- Основной результат КР – программная реализация актуального криптографического алгоритма/протокола (запрещается дублирование тем)
- Пояснительная записка оформляется согласно ГОСТ 7.32
- Пояснительная записка должна содержать теоретическую часть, где описан выбранный алгоритм/протокол
- Пояснительная записка должна содержать практическую часть, которая включает в себя инструкцию для пользователя по программной реализации протокола/алгоритма с результатами работы программы (какой функционал программы, для каждой функции отдельный сценарий и т.д.)
- При написании пояснительной записки запрещается использование Искусственного Интеллекта
- Пояснительная записка должна содержать количественные показатели программной реализации (см. **Требования к программной реализации**)
- Пояснительная записка сдается в электронном виде – загружается в ответ на задание по КР в личном кабинете студента в формате pdf
- Объем пояснительной записки должен составлять не менее 25 страниц и не более 40 страниц

Обязательными структурными элементами пояснительной записки являются:

- **титульный лист**
- **задание на курсовую работу (проект)**
- **содержание**
- **введение** (включает в себя актуальность работы, проработанность выбранной темы, цель и задачи)
- **основная часть** (включает в себя 2–3 главы, подразделяемые на подглавы)
- **заключение**
- **список использованных источников**
- список сокращений (если есть)
- **приложение** (программный код)

Требования к программной реализации

- Язык программирования выбирается студентом самостоятельно
- Необходимо реализовать графический интерфейс пользователя
- Программа должна оценивать время выполнения каждого алгоритма/протокола в секундах/миллисекундах (например, при рассмотрении подписи необходимо оценить время генерации ключа, время подписи сообщения, время проверки подписи)
- Программа должна оценивать полученные выходные и входные данные в байтах
- Любые другие дополнительные метрики/функционал и тд, предложенные студентами, приветствуются (например: программная реализация алгоритма/протокола является constant-time)

Этапы сдачи КР

- Выбор темы КР и согласование с преподавателем
- Показ промежуточных результатов, к этому моменту должно быть выполнено около 50% поставленных задач
- Финальная сдача КР, после финальной сдачи работы не принимаются

Каждый этап сдачи КР имеет свои сроки выполнения, которые оглашаются преподавателем в начале семестра.

Оценивание КР

Ниже представлено приблизительное оценивание КР, оно может меняться.
Студент получает «**отлично**»:

- алгоритм/протокол разобран студентом самостоятельно (т.е. его не затрагивали в рамках дисциплины)
- студент презентовал КР (см. условия ниже)
- студент ответил на все дополнительные вопросы
- соблюдены все сроки дедлайнов
- выполнены все требования по КР
- за две недели до начала финальной сдачи КР студент должен уведомить преподавателя о желании презентовать КР
- пояснительная записка добавлена в ЛК за три дня до назначенной защиты

Защита проходит только в назначенную преподавателем дату, без повторных защит.
Представление КР в виде презентации, презентация оформляется в фирменном стиле университета, шаблон находится на сайте https://guap.ru/, следующее должно быть включено:

- актуальность работы
- цель и задачи
- математическое описание алгоритма/протокола
- скрины работы программы, показатели программной реализации
- количественные показатели программной реализации
- личный вклад каждого из участников.

Время выступления: до 7 минут.
Сдача КР включает в себя защиту – ответы на теоретические вопросы, демонстрацию программной реализации.

Студент получает «**хорошо**»:

- алгоритм/протокол частично разобран в рамках дисциплины и/или полностью рассмотрен его математический аппарат
- соблюдены/частично соблюдены сроки дедлайнов
- требования по КР выполнены частично

Студент получает «**удовлетворительно**»:

- алгоритм/протокол разобран в рамках дисциплины или включен в список: RSA, ElGamal, криптосистема Рабина, ECDSA, DSA, Протокол Диффи - Хеллмана, схема разделения секрета Шамира и Блома, AES, DES, Кузнечик, Магма, хэш-функции семейства MD|SHA, ГОСТ 34.10
- не соблюдены сроки дедлайнов, КР сдана с задержкой в неделю
- требования по КР выполнены частично

Выбор и оформление темы КР

- Тема КР выбирается студентом самостоятельно, ниже приведены рекомендации
- Тема КР не меняется после согласования с преподавателем
- Если в КР реализуется алгоритм/протокол, разобранный студентом самостоятельно, то название формулируется как: «Исследование и разработка программной реализации… »
- Если в КР реализуется алгоритм/протокол, разобранный в рамках дисциплины, то название формулируется как: «Разработка программной реализации …»
- При выборе направления КР можно выбирать современные технологии, системы,…, где применяются криптографические алгоритмы/протоколы. В рамках такой работы можно провести анализ области применения, определить требования к алгоритму/протоколу, определить преимущества и недостатки алгоритма/протокола, как можно покрыть выявленные недостатки (если они имеются). Возможные направления: Интеллектуальные Транспортные Системы (ITS), Интернет Вещей (IoT), мессенджеры, искусственный интеллект.

  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)	20	10	10
Курсовое проектирование (КП, КР)	10		10
Расчетно-графические задания (РГЗ)			
Выполнение реферата (Р)			
Подготовка к текущему контролю успеваемости (ТКУ)	15	5	10
Домашнее задание (ДЗ)			
Контрольные работы заочников (КРЗ)			
Подготовка к промежуточной	16	6	10

аттестации (ПА)			
Всего:	61	21	40

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)
004.05В 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)
	http://e.lanbook.com/books/element.php?pl1_id=3032 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)
	http://e.lanbook.com/books/element.php?pl1_id=4959 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

http://www.intuit.ru/studies/courses/10/10/info	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 таблице12.

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

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
1	Основные понятия и определения криптографии. Виды криптосистем. Задачи, решаемые методами криптографии. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений.	ОПК-9.3.3

	История криптографии. Основные этапы становления науки криптографии.	
2	Коды аутентификации сообщений. Защитные контрольные суммы. Криптографические хэш-функции и требования к ним. Подходы к проектированию хэш-функций. Хэш-функции на основе блочного шифра. Ключевые хэш-функции. Понятие односторонней функции и односторонней функции с "лазейкой". Проблемы факторизации целых чисел и логарифмирования в конечных полях.	ОПК-9.З.4
3	Криптосистема Диффи-Хэллмана. Пример. Криптосистема RSA. Пример. Криптосистема Эль-Гамаля. Пример. Криптосистема Рабина. Пример. Криптосистема Гольдвассер-Микали. Пример. Криптосистема Блюма-Гольдвассер. Пример.	ОПК-9.З.5
4	Рюкзачные шифры. Криптосистема Меркла-Хэллмана. Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП. Подпись RSA, Эль-Гамаля. Подпись Фиата-Шамира. Подпись Онга-Шнорра-Шамира. Неотрицаемая подпись Шаума-ван-Антверпена. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94. Эллиптическая кривая над конечным полем. Операции на эллиптической кривой. Сумма точек. Кратная точка.	ОПК-9.У.2
5	Проблема дискретного логарифмирования на эллиптической кривой. Переход от шифра (ЭЦП) в Zp к шифру (ЭЦП) на эллиптической кривой. Шифр Эль-Гамаля на эллиптической кривой. Стандарты ЭЦП на эллиптической кривой: ГОСТ Р 34.10-2001, ECDSA.	ОПК-9.У.3

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	Избыточность языка. Оценка числа ложных ключей и расстояние единственности. Безусловно стойкие и вычислительно стойкие шифры. Псевдослучайные последовательности (ПСП). Характеристики генераторов ПСП (ПСГ). Требования к криптографическим ПСП. Примеры ПСГ и криптографических ПСГ. Поточные шифры. Общая схема поточного шифра. Синхронные и самосинхронизирующиеся шифры.	ОПК-9.З.3
2	Регистры сдвига с обратной линейной связью (РСЛОС). ПСГ на основе РСЛОС. Шифр A5. Нелинейные регистры сдвига. Шифр RC4. Теория имитостойкости Симмонса. Имитация и подмена сообщения. Характеристики имитостойкости. Совершенная имитостойкость.	ОПК-9.З.4

3	Классификация шифров замены. Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат. Шифр Хилла. Шифр Виженера. Частотный анализ. Тест Казиски. Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ. Шифры гаммирования. Шифр Вернама. Подходы к его криптоанализу. Композиции шифров. Enigma. Шифр Хейглина. Математическая модель шифра.	ОПК-9.З.5
4	Атаки и угрозы шифрам. Блочные шифры и их ключевая система. Замены и перестановки. Сеть Файстеля. Шифры DES, ГОСТ 28147-89. Шифр AES Шифр IDEA. Подходы к криптоанализу блочных шифров. Дифференциальный криптоанализ. Линейный криптоанализ.	ОПК-9.У.2
5	Режимы шифрования. Многократное шифрование. Композиция блочных шифров. Совершенные шифры. Пример совершенного шифра. Энтропийные характеристики шифров. Идеальные шифры.	ОПК-9.У.3

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
	1. Самостоятельный анализ исторического шифра. Шифры простой замены, Плейфера, Виженера, Полибия, Хилла, Вернама, «Решетка», Хейглина, Enigma и др. 2. Режимы блочного шифрования ГОСТ 28147-89, DES. 3. Алгоритм разворачивания ключа шифра AES. 4. Исследование энтропийных свойств русского и английского языков. 5. Генераторы ПСП и их свойства. 6. Самосинхронизирующиеся поточные шифры. 7. Построение чистого шифра. Оценка трудоемкости подбора ключа при известной паре «открытый – шифрованный текст». 8. Теория имитостойкости Симмонса. Оценка вероятности имитации ключевых хэш-функций. 9. Построение защитных контрольных сумм на основе бесключевой хэш-функции. 10. Построение криптографической хэш-функции на основе односторонней функции. 11. Построение класса больших простых чисел. 12. Вероятностные тесты на простоту. Построение доказуемо простых чисел. 13. Построение ключевой информации для ЭЦП. 14. Вычисления на эллиптической кривой. 15. Инфраструктура открытых ключей. 16. Исследование и разработка программной реализации протокола конфиденциальных вычислений (протокол Ben-Or – Goldwasser – Wigderson/ протокол Goldreich – Micali – Wigderson) 17. Исследование и разработка программной реализации протокола забывчивой передачи данных

	18. Исследование и разработка программной реализации слепой/групповой/пороговой/кольцевой/забывчивой схемы подписи 19. Исследование и разработка программной реализации гомоморфного шифрования 20. Исследование и разработка программной реализации атаки Castryck-Decru на SIKE

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
	• В протоколе шифра Шамира сообщение пересылается а) два раза б) три раза в) один раз г) четыре раза. • Надежность системы RSA базируется на том, что а) сложно определить по данному числу, является ли оно простым б) задача дискретного логарифмирования сложна в) задача разложения на множители числа, являющегося произведением двух простых, сложна. • Укажите правильный порядок ответов в правом столбике: RC4 шифр с открытым ключом AES потоковый шифр RSA совершенный шифр Шифр Вернама блоковый шифр • Найдите x, распишите ход решения: $x^2 \equiv 55 \pmod{79}$. • Решите уравнение, распишите ход решения: $53x \equiv 31 \pmod{72}$	

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

Основной целью дисциплины «Методы и средства криптографической защиты 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, ее 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;

– научится 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: Исторические шифры и их криптоанализ.

Тема 2: Симметричная криптография: уязвимости и атаки.

Тема 3: Хэш-функции и криптосистемы с открытым ключом.

Тема 4: Криптосистемы с открытым ключом: цифровая подпись

Тема 5: Криптографические методы защиты информации, основанные на эллиптических кривых.

Тема 6: Криптографические протоколы: доказательство с нулевым разглашением, схема разделения секрета, обмен ключами.

Порядок выполнения и сдачи лабораторных работ

Для успешного прохождения каждой лабораторной работы студент обязан выполнить следующие этапы в указанной последовательности:

1. Самостоятельная подготовка. До начала выполнения лабораторной работы студент обязан изучить соответствующий лекционный материал, указанный в перечне (Таблица 4 РПД), а также рекомендованную учебно-методическую литературу.

2. Выполнение практической части. В ходе лабораторного занятия или в отведенное для самостоятельной работы время студент реализует задания лабораторной работы: осуществляет программную реализацию криптографических алгоритмов, проводит вычисления, анализирует результаты, выявляет уязвимости – в соответствии с условиями конкретного задания. Язык программирования выбирается студентом самостоятельно, если иное не указано в задании.

3. Оформление отчета. Студент оформляет отчет по лабораторной работе в соответствии с требованиями настоящего документа и загружает его в личный кабинет (далее – ЛК) в установленный срок.

4. Защита лабораторной работы. После загрузки отчета студент обязан пройти процедуру защиты лабораторной работы в срок, установленный преподавателем для данной работы. Каждое задание имеет индивидуально установленные предельные сроки загрузки отчета и проведения защиты. Актуальные сроки доводятся преподавателем на первом занятии по дисциплине и публикуются в личном кабинете студента.

Выполнение каждого из указанных этапов является обязательным условием сдачи лабораторной работы. Отчет, не прошедший защиту, не считается сданным.

Порядок защиты лабораторной работы

Защита лабораторной работы проводится по выбору преподавателя в одной из следующих форм.

Форма 1 – Устная защита. Студент демонстрирует корректную работу программной реализации, отвечает на теоретические и практические вопросы по тематике лабораторной работы, а также решает или комментирует практические задачи, предложенные преподавателем в ходе защиты. Преподаватель вправе задавать уточняющие вопросы по любому аспекту выполненной работы.

Форма 2 – Письменная защита. Студент выполняет письменный контрольный опрос, включающий тестовые вопросы с выбором ответа, развернутые теоретические

вопросы по теме лабораторной работы, а также расчетно-практические задания, требующие решения с подробным обоснованием.

Конкретная форма защиты определяется преподавателем для каждой лабораторной работы или для группы в целом. Преподаватель вправе комбинировать элементы обеих форм.

Структура и форма отчета о лабораторной работе

Отчёт по лабораторной работе оформляется каждым студентом индивидуально вне зависимости от того, выполнялась ли работа самостоятельно или в составе группы. Отчёт должен содержать следующие обязательные разделы в указанной последовательности:

1. **Титульный лист** – наименование университета и кафедры; наименование дисциплины; наименование и номер лабораторной работы; ФИО студента; номер учебной группы; год выполнения работы.
2. **Введение** – цель работы и перечень задач, решаемых в ходе её выполнения.
3. **Теоретическая часть** – минимально необходимые теоретические сведения, относящиеся к предмету исследования. Дословное копирование методических указаний или разделов учебника не допускается.
4. **Ход выполнения работы** – описание выполнения лабораторного задания: изложение примененной методики, последовательности действий студента, параметров эксперимента и промежуточных расчётов, демонстрирующее путь к решению поставленной задачи; скриншоты результатов программной реализации, полученные в ходе выполнения работы; таблицы и графики с соответствующими заголовками и нумерацией; демонстрация корректности работы программной реализации.
5. **Выводы** – анализ полученных результатов, новые знания, приобретённые в ходе работы; оценка степени достижения поставленной цели. Выводы не должны представлять собой простое перечисление выполненных действий.
6. Список литературы (при необходимости) – оформляется в соответствии с ГОСТ 7.0.5. Все источники из списка должны иметь ссылки в тексте отчета.

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 ее 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 отчета приводится Список литературы, использованной при подготовке к работе. В тексте отчета делаются краткие ссылки на литературу (учебники, справочники, иные источники…) номером в квадратных скобках, напр., [1]. Литературные источники нумеруются по мере их появления в тексте отчета. В конце отчета дается их подробный список. На все источники списка литературы должны быть ссылки в тексте отчета, там, где это необходимо.

Отчет оформляется в текстовом редакторе и распечатывается на листах формата А4 либо представляется в электронном виде в ЛК в соответствии с требованиями ГОСТ 7.32.

Технические требования к оформлению:

• Поля: левое – 25 мм, верхнее и нижнее – 20 мм, правое – 15 мм.

• Шрифт основного текста: Times New Roman (или аналогичный), 14 пт.

• Межстрочный интервал: полуторный.

• Нумерация страниц: сквозная; титульный лист не нумеруется, последующие страницы нумеруются начиная с цифры 2.

• Рисунки, таблицы, графики: нумеруются последовательно в пределах раздела или документа; подписываются заголовками.

• Фрагменты программного кода в тексте отчета набираются шрифтом Courier New, 10 пт, через одинарный интервал.

• Ссылки на литературу в тексте оформляются номером в квадратных скобках, например. Литературные источники нумеруются в порядке первого упоминания в тексте.

При сдаче отчета преподаватель может сделать устные и письменные замечания, задать дополнительные вопросы. Все ответы на дополнительные вопросы, обсуждения выполняются студентом на отдельных листах, включаемых в отчет (при этом в тексте основного отчета делается сноска или другой значок, которому будет соответствовать новый материал). При этом письменные замечания преподавателя должны остаться в тексте для ясности динамики работы над отчетом.

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

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, расчетной, 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.

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