МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ–ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

Кафедра №34

«УТВЕРЖДАЮ»
Руководитель направления
проф., д.т.н., доц.
(должность, уч. степень, звание)
С.В. Беззатеев
(подпись)
«24» мая 2020 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Криптографические методы защиты информации»
(Название дисциплины)

Код направления	10.05.03
Наименование направления/ специальности	Информационная безопасность автоматизированных систем
Наименование направленности	Обеспечение информационной безопасности распределенных информационных систем
Форма обучения	очная

Санкт-Петербург 2020 г.

Лист согласования рабочей программы дисциплины

Программу составил(а)

д.т.н.,доц.	24.05.2020	С.В. Беззатеев
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Программа одобрена на заседании кафедры № 34

«21» мая 2020 г, протокол № 10

Заведующий кафедрой № 34

д.т.н.,доц.	24.05.2020	С.В. Беззатеев
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Ответственный за ОП 10.05.03(07)

доц.,к.т.н.,доц.	24.05.2020	В.А. Мыльников
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Заместитель директора института (декана факультета) № 3 по методической работе

доц.,к.э.н.	24.05.2020	Г.С. Армашова-Тельник
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Аннотация

Дисциплина «Криптографические методы защиты информации» входит в базовую часть образовательной программы подготовки обучающихся по специальности «10.05.03 «Информационная безопасность автоматизированных систем» направленность «Обеспечение информационной безопасности распределенных информационных систем». Дисциплина реализуется кафедрой №34.

Дисциплина нацелена на формирование у выпускника

общекультурных компетенций:

ОК-7 «способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности»;

общепрофессиональных компетенций:

ОПК-3 «способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности»,

ОПК-5 «способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами».

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. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-7 «способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности»:

знать - основные задачи и понятия криптографии;

уметь - использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки;

владеть навыками - криптографической терминологией;

иметь опыт деятельности - применения методов и средств анализа и моделирования современных криптографических алгоритмов;

ОПК-3 «способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности»:

знать - требования к шифрам и основные характеристики шифров;

уметь - применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;

владеть навыками - навыками использования типовых криптографических алгоритмов;

иметь опыт деятельности - формирования требований по обеспечению криптографической защиты информации;

ОПК-5 «способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами»:

знать - принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах;

уметь - применять методы криптографии при решении задач защиты информации;

владеть навыками - навыками математического моделирования в криптографии;

иметь опыт деятельности - осуществлять программную реализацию криптографических алгоритмов.

2. Место дисциплины в структуре ОП

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

- Введение в специальность
- Информатика
- Основы программирования
- Основы программирования
- 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 дисциплины в ЗЕ/академ. час

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 1

Таблица 1 – 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
Аудиторные занятия, всего час., ***В том числе***	85	34	51
лекции (Л), (час)	34	17	17
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	95	38	57
Вид промежуточного контроля: зачет, дифф. зачет, экзамен **(Зачет, Дифф. зач, Экз.)**	Зачет, Экз.	Зачет	Экз.

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий

Разделы и темы дисциплины и их трудоемкость приведены в таблице 2.

Таблица 2. – Разделы, темы дисциплины и их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 5					
Раздел 1. Общие сведения. Введение	4		4		8
Раздел 2 Симметричная криптография	6		6		10

Раздел 3. Несимметричная криптография	7		7		10
Итого в семестре:	17		17		38
Семестр 6					
Раздел 4. Электронно-цифровая подпись	8		8		30
Раздел 5.Криптографические протоколы	9		9		27
Выполнение курсовой работы				17	
Итого в семестре:	17		17	17	57
Итого:	34	0	34	17	95

4.2. Содержание разделов и тем лекционных занятий

Содержание разделов и тем лекционных занятий приведено в таблице 3.

Таблица 3 - Содержание разделов и тем лекционных занятий

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	Раздел 1. Общие сведения. Введение Тема 1. Основные понятия и определения 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 - RC4 AES, ГОСТ 28147-89,»Кузнечик№ и др. Режимы использования и их сравнение (ECB,CBC, OFB, …). Тема 7 Криптографические свойства функций. Тема 8 Хзш 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, МакЭлайса, Меркля – Хеллмана. Тема 12. Некоторые методы быстрой модульной арифметики и их применение для ускорения криптографических алгоритмов
4	Раздел 4. Электронно-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 Р 34.10-94). 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 4.

Таблица 4 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	№ раздела дисцип-лины
Учебным планом не предусмотрено				
		Всего:		

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	№ раздела дисциплины
Семестр 5			
1	Нападения и угрозы безопасности в компьютерных системах	2	1
2	Модель нарушителя информационной безопасности	2	2
3	Криптография и криптоанализ	1	2
4	Методы криптографии	2	2
5	Методы криптоанализа	2	
6	Криптография и теория сложности	2	3
7	Криптография с секретным ключом	2	3
8	Протоколы симметричного шифрования	2	
9	Блочные и потоковые шифры.	2	3
Семестр 6			
8	Сложность теоретико-числовых алгоритмов. Однонаправленные функции.	2	4

9	Алгоритм RSA. Шифросистема Эль-Гамаля	3	4
10	Криптоанализ алгоритмов с открытым ключом	3	4
11	Хэш-функции. Аутентификация сообщений	3	5
12	Электронная цифровая подпись	3	5
13	Теоретико-информационная стойкость. Стойкость и надежность	3	5
	Всего:	34	

4.5. Курсовое проектирование (работа)

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 6.

Таблица 6 Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 5, час	Семестр 6, час
1	2	3	4
Самостоятельная работа, всего	95	38	57
изучение теоретического материала дисциплины (ТО)	70	30	40
курсовое проектирование (КП, КР)			
расчетно-графические задания (РГЗ)			
выполнение реферата (Р)			
Подготовка к текущему контролю (ТК)	25	8	17
домашнее задание (ДЗ)			
контрольные работы заочников (КРЗ)			

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 8-10.

6. Перечень основной и дополнительной литературы

6.1. Основная литература

Перечень основной литературы приведен в таблице 7.

Таблица 7 – Перечень основной литературы

Шифр	Библиографическая ссылка / URL адрес	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	

6.2. Дополнительная литература

Перечень дополнительной литературы приведен в таблице 8.

Таблица 8 – Перечень дополнительной литературы

Шифр	Библиографическая ссылка/ URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
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 ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

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, используемых при осуществлении образовательного процесса по дисциплине

8.1. Перечень программного обеспечения

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10 – Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2. Перечень информационно-справочных систем

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11 – Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Состав материально-технической базы 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. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

10.1. Состав фонда оценочных средств приведен в таблице 13

Таблица 13 - Состав фонда оценочных средств для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных средств
Экзамен	Список вопросов к экзамену; Задачи; Тесты.
Зачет	Список вопросов; Тесты.
Выполнение курсовой работы	Экспертная оценка на основе требований к содержанию курсовой работы по дисциплине.

1.1. Перечень компетенций, относящихся к дисциплине, и этапы их формирования в процессе освоения образовательной программы приведены в таблице 14.

Таблица 14 – Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Номер семестра	Этапы формирования компетенций по дисциплинам/практикам в процессе освоения ОП
ОК-7 «способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности»	
1	Экология
1	Экономика
1	Иностранный язык
1	Введение в специальность
1	Промышленная экология
2	Иностранный язык
2	Культурология
2	Учебная (ознакомительная) практика
3	Социальная психология
3	Психология и педагогика
3	Иностранный язык
4	Правоведение
4	Учебная практика
4	Иностранный язык
5	Криптографические методы защиты информации
6	Криптографические методы защиты информации
6	Мировая экономика
6	Производственная (эксплуатационная) практика
6	Международный бизнес
8	Производственная (конструкторская) практика
9	Научно-технический семинар
9	Экономика проектов в информационных технологиях
9	Научно-исследовательская работа
9	Научно-исследовательская работа
9	Прикладная экономика
10	Научно-исследовательская работа

10	Научно-исследовательская работа
10	Научно-технический семинар
10	Производственная преддипломная практика
ОПК-3 «способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности»	
1	Информатика
2	Основы программирования
3	Основы программирования
4	Технологии и методы программирования
5	Криптографические методы защиты информации
6	Программно-аппаратные средства обеспечения информационной безопасности
6	Криптографические методы защиты информации
6	Производственная (эксплуатационная) практика
7	Методы и средства проектирования информационных систем
8	Методы и средства проектирования информационных систем
8	Языки программирования
8	Производственная (конструкторская) практика
9	Научно-исследовательская работа
9	Научно-исследовательская работа
10	Научно-исследовательская работа
10	Научно-исследовательская работа
10	Производственная преддипломная практика
ОПК-5 «способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами»	
3	Инженерная графика
5	Криптографические методы защиты информации
6	Криптографические методы защиты информации
9	Научно-исследовательская работа
9	Научно-технический семинар
9	Научно-исследовательская работа
10	Научно-исследовательская работа
10	Научно-исследовательская работа
10	Научно-технический семинар

1.2. В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала модульно–рейтинговой системы университета. В таблице 15 представлена 100–балльная и 4-балльная шкалы для оценки сформированности компетенций.

Таблица 15 –Критерии оценки уровня сформированности компетенций

Оценка компетенции		Характеристика сформированных компетенций
100-балльная	4-балльная шкала	

шкала		
$85 \le К \le 100$	«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.
$70 \le К \le 84$	«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.
$55 \le К \le 69$	«удовлетво-рительно» «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.
$К \le 54$	«неудовлетво рительно» «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.

1.3. Типовые контрольные задания или иные материалы:

1. Вопросы (задачи) для экзамена (таблица 16)

Таблица 16 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена
	1. Основные понятия и определения криптографии. 2. Виды криптосистем. Задачи, решаемые методами криптографии. 3. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений. 4. История криптографии. Основные этапы становления науки криптографии. 5. Классификация шифров замены. Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат. Шифр Хилла. Шифр Виженера. Частотный анализ. Тест Казиски. 6. Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ. 7. Шифры гаммирования. Шифр Вернама. Подходы к его криптоанализу. 8. Композиции шифров. Enigma. Шифр Хейглина. 9. Математическая модель шифра. 10. Атаки и угрозы шифрам. 11. Блочные шифры и их ключевая система. Замены и перестановки.

	12. Сеть Файстеля. Шифры DES, ГОСТ 28147-89. 13. Шифр AES 14. Шифр IDEA. 15. Подходы к криптоанализу блочных шифров. Дифференциальный криптоанализ. Линейный криптоанализ. 16. Режимы шифрования. 17. Многократное шифрование. Композиция блочных шифров. 18. Совершенные шифры. Пример совершенного шифра. 19. Энтропийные характеристики шифров. Идеальные шифры. 20. Избыточность языка. 21. Оценка числа ложных ключей и расстояние единственности. 22. Безусловно стойкие и вычислительно стойкие шифры. 23. Псевдослучайные последовательности (ПСП). Характеристики генераторов ПСП (ПСГ). Требования к криптографическим ПСП. Примеры ПСГ и криптографических ПСГ. 24. Поточные шифры. Общая схема поточного шифра. Синхронные и самосинхронизирующиеся шифры. 25. Регистры сдвига с обратной линейной связью (РСЛОС). 26. ПСГ на основе РСЛОС. 27. Шифр A5. 28. Нелинейные регистры сдвига. 29. Шифр RC4. 30. Теория имитостойкости Симмонса. Имитация и подмена сообщения. Характеристики имитостойкости. Совершенная имитостойкость. 31. Коды аутентификации сообщений. 32. Защитные контрольные суммы. 33. Криптографические хэш-функции и требования к ним. 34. Подходы к проектированию хэш-функций. 35. Хэш-функции на основе блочного шифра. 36. Ключевые хэш-функции. 37. Понятие односторонней функции и односторонней функции с "лазейкой". Проблемы факторизации целых чисел и логарифмирования в конечных полях. 38. Криптосистема Диффи-Хэллмана. Пример. 39. Криптосистема RSA. Пример. 40. Криптосистема Эль-Гамаля. Пример. 41. Криптосистема Рабина. Пример. 42. Криптосистема Гольдвассер-Микали. Пример. 43. Криптосистема Блюма-Гольдвассер. Пример. 44. Рюкзачные шифры. Криптосистема Меркла-Хэллмана. 45. Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП. 46. Подпись RSA, Эль-Гамаля. 47. Подпись Фиата-Шамира. 48. Подпись Онга-Шнорра-Шамира. 49. Неотрицаемая подпись Шаума-ван-Антверпена. 50. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94. 51. Эллиптическая кривая над конечным полем. Операции на эллиптической кривой. Сумма точек. Кратная точка. 52. Проблема дискретного логарифмирования на эллиптической кривой. Переход от шифра (ЭЦП) в Zp к шифру (ЭЦП) на эллиптической кривой. 53. Шифр Эль-Гамаля на эллиптической кривой. 54. Стандарты ЭЦП на эллиптической кривой: ГОСТ Р 34.10-2001, ECDSA.

55. Вопросы (задачи) для зачета / дифференцированного зачета (таблица 17)

Таблица 17 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	1. Основные понятия и определения криптографии. 2. Виды криптосистем. Задачи, решаемые методами криптографии. 3. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений. 4. История криптографии. Основные этапы становления науки криптографии. 5. Классификация шифров замены. Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат. Шифр Хилла. Шифр Виженера. Частотный анализ. Тест Казиски. 6. Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ. 7. Шифры гаммирования. Шифр Вернама. Подходы к его криптоанализу. 8. Композиции шифров. Enigma. Шифр Хейглина. 9. Математическая модель шифра. 10. Атаки и угрозы шифрам. 11. Блочные шифры и их ключевая система. Замены и перестановки. 12. Сеть Файстеля. Шифры DES, ГОСТ 28147-89. 13. Шифр AES 14. Шифр IDEA. 15. Подходы к криптоанализу блочных шифров. Дифференциальный криптоанализ. Линейный криптоанализ.

16. Темы и задание для выполнения курсовой работы / выполнения курсового проекта (таблица 18)

Таблица 18 – Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта

№ п/п	Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта
	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. Вопросы для проведения промежуточной аттестации при тестировании (таблица 19)

Таблица 19 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
	• 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

17. Контрольные и практические задачи / задания по дисциплине (таблица 20)

Таблица 20 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	Примерные темы расчетных заданий, требующие написание компьютерных программ в режиме самостоятельной (внеаудиторной) работы: • Система Диффи-Хеллмана в простом поле (в циклической подгруппе простого порядка). • Шифр Эль-Гамаля в простом поле (подгруппе). • Шифр RSA. • Шифр Рабина. • Цифровая подпись типа DSA • Цифровая подпись RSA • Оптимальный омофонный код. • Шифр на основе нумерации сочетаний. • Шифр на основе универсального омофонного кода.

10.2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и / или опыта деятельности, характеризующих этапы формирования компетенций, содержатся в Положениях «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».

11. 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;

– 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:

Тема1: 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 Z2 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 Zn. Шифр с открытым ключом: RSA, Эль-Гамаля, 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-Гамаля 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 Zp 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