МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Северо-Кавказский филиал

ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»

> Утверждаю Зам. директора по УВР А.Г. Жуковский 2022 г.

Методы и средства криптографической защиты информации Б1.О.25 рабочая программа дисциплины

Кафедра:

Инфокоммуникационные технологии и системы связи

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Безопасность компьютерных систем.

Формы обучения:

очная

Распределение часов дисциплины по семестрам (для очной формы обучения), курсам (для заочной формы обучения)

3Ф ОΦ Вид учебной работы 3E 3E часов часов Общая трудоемкость 180/5сем дисциплины, в том числе (по семестрам, курсам): Контактная работа, в том 90/5сем числе (по семестрам, курсам): Лекции 34/5сем Лабораторных работ 34/5сем Практических занятий 22/5 сем Семинаров Самостоятельная работа 54/5сем Контроль 36 Число контрольных работ (по курсам) Число КР (по семестрам, курсам) Число КП (по семестрам, курсам) Число зачетов с оценкой с разбивкой по семестрам (курсам) Число экзаменов с разбивкой 1/5сем по семестрам (курсам)

Программу составил:

Доцент кафедры ИТСС, к.т.н., доцент Шухардин А.Н.

Рецензент:

Ведущий сотрудник ФГУП «РНИИРС», д.т.н., доцент Елисеев А.В.

Рабочая программа дисциплины

«Методы и средства криптографической защиты информации»

разработана в соответствии с ФГОС ВО:

направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020г. N 1427.

Составлена на основании учебного плана

направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 25.04.2022 г., и утвержденного директором СКФ МТУСИ 25.04.2022 г.

Рассмотрена и одобрена на заседании кафедры «Инфокоммуникационные технологии и системы связи»

Протокол от «29» <u>08</u> 2022г. № <u>4</u>

Зав. кафедрой В.И. Юхнов

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР
«»20 г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»
Протокол от «» 20 г. №
Зав. кафедрой
Визирование для использования в 20/20 уч. году
Утверждаю
Зам. директора по УВР
<u></u>
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры «Инфокоммуникационные технологии и системы связи»
Протокол от «» 20 г. № Зав. кафедрой
Визирование для использования в 20/20 уч. году Утверждаю Зам. директора по УВР
«» 20 г. Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры «Инфокоммуникационные технологии и системы связи»
Протокол от «»20 г. № Зав. кафедрой
Визирование для использования в 20/20 уч. году
Утверждаю
Зам. директора по УВР
« <u> </u>
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»
Протокол от «» 20 г. № Зав. кафедрой

1. Цели изучения дисциплины

Целью освоения дисциплины является формирование у обучаемых знаний в области принципов криптографических преобразований, типовых программно-аппаратных средств криптографической защиты информации и инфокоммуникаций от несанкционированного доступа.

Задачи освоения дисциплины:

- формирование знаний, умений и навыков, позволяющих проводить самостоятельный криптографический анализ информационных процессов, как изучаемых в настоящей дисциплине, так и находящихся за ее рамками.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать профессиональные задачи в соответствии с *эксплуатационным* видом деятельности:

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)

ОПК-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности

Знать:

- основные математические методы и алгоритмы шифрования, расшифрования и дешифрования сообщений;
- классификацию методов криптографического преобразования информации;
- принципы функционирования программных средств криптографической защиты информации.;
- основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы;
- национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения;
- алгоритмы электронной (цифровой) подписи в телекоммуникационных системах.

Уметь:

- пользоваться методами теории чисел
- классифицировать и оценивать угрозы информационной безопасности;
- использовать СКЗИ в автоматизированных системах;
- использовать механизмы идентификации и аутентификации.

Владеть:

- навыками анализа и оценки угроз информационной безопасности объекта информатизации;
- навыками работы по основам защиты информации с использованием программно-аппаратных комплексов.

3. Место дисциплины в структуре образовательной программы

Тре	Требования к предварительной подготовке обучающегося (предшествующие						
	дисциплины, модули, темы):						
1	1 Дисциплина «Методы и средства криптографической защиты информации» включена в обязательную часть (блок Б1.О) учебного плана по направлению «Информационная безопасность». Ей предшествует изучение дисциплины «Основы информационной безопасности».						
2	Успешное освоение дисциплины «Методы и средства криптографической защиты информации»» базируется также на знаниях, приобретенных из дисциплин: Б1.О.03 «Информатика», Б1.О.05 «Математический анализ», Б1.О.13 «Теория вероятности и математическая статистика».						
	Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:						
1	1 Дисциплина является базовой для успешного освоения дисциплин: Б1.О.33 «Программно-аппаратные средства защиты информации», Б1.О.36 «Криптографические протоколы», Б1.О.37 «Комплексное обеспечение защиты информации»						

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 180 часов, 90 аудиторных часов, 54 часов самостоятельной работы, 36 часов контроль)

Код з	• • • • • • • • • • • • • • • • • • • •	Вид зан.	Кол. часов	Компет енции	УМИО
	Курс 3, Семестр 5				
	Модуль 1. Методы модулярной арифметики и аналити	ческих	преобр	разовани	й.
	(40+26) часов				
1.1	Лекция 1.	Л1	2	ОПК-6	Л1.1
	ИНФОРМАЦИЯ КАК ГЛАВНЫЙ РЕСУРС НАУЧНО-			ОПК-9	Л1.2
	ТЕХНИЧЕСКОГО И СОЦИАЛЬНО-				Л1.3
	ЭКОНОМИЧЕСКОГО РАЗВИТИЯ ОБЩЕСТВА.				
	1. Задачи обеспечения информационной безопасности				
	телекоммуникационных систем.				
	2. Система передачи информации с шифрованием				
	сообщений.				
	3. Три исторических этапа развития КСЗИ.				
1.2	Лекция 2.	Л2	2	ОПК-6	Л1.1
	ОСНОВНЫЕ ТРЕБОВАНИЯ К КСЗИ.			ОПК-9	Л1.2
	Основные понятия криптографии: алфавит, открытый				Л1.3
	текст, закрытый текст (криптограмма), шифрование,				
	расшифрование, секретный ключ.				
	Криптоанализ и дешифрование.				
1.3	Лекция 3.	Л3	2	ОПК-9	Л1.1
	ТЕОРЕТИКО-ИНФОРМАЦИОННЫЕ ОСНОВЫ				Л1.2
	КРИПТОЗАЩИТЫ СООБЩЕНИЙ.				Л1.3
	1 Количественные меры информации.				
	2. Взаимная информация между криптограммой и				
	ключом (первая криптотеорема Шеннона).				
	3 Теоретическая стойкость КСЗИ.				
1.4	Лекция 4.	Л4	4	ОПК-9	Л1.1

1. Вытеты по могулю то. Теорема Эвклида 2. Свойство коммутативности . Функция Эйдера. 3. Свойства (колочисленных операций тиоф N. 4. Вытисление обратных величин 1.5. Практическое занятие №2 Обпие формулы вычисления больших степепей 1.6. Практическое занятие №2 Обпие формулы вычисления больших степепей 1.7. Лежция №5 КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ. Методы перестановки. Методы подстановки и замены. Методы на магитическое занятие № 3 Методы магитическое занятие № 3 Практическое занятие № 4 Методы подстановки и замены. Методы замилических преобразований 1.8. Практическое занятие № 4 Метод полиномов. 1.9. Практическое занятие № 4 Метод полиномов. 1.10. Лабораторная работа №2. Пифры замены. 1.11. Лабораторная работа №2. Пифры перестановки. 1.12. Лежция №6. Гаммирование. Основные понятия. Методы тестирования песендослучайных последовательностей. Комбинированные методы шифрования 1.13. Практическое занятие № 5 Графические тесты. Проверка на монотопность. Опеночные тесты 1.14. Лабораторная работа № 3. Генерация дискретных случайных последовательностей. Комбинированные методы шифрования 1.13. Практическое занятие № 5 Графические тесты. Проверка на монотопность. Опеночные тесты 1.14. Лабораторная работа № 3. Генерация дискретных случайных последовательностей. Комбинирования ПСП. 1.9. История появления шифров. Локтрина информации. Обеспечение сохранения коммерческой тайны предпратия. Каталог обобисенных меропратий по защите конфиденциальной информации. Појходы к оценке стойкости апторитмов пифрования. Электронные ресурсы молулярной арифметнки. Калькуляторы. Пескрослучайные последовательности. Свойства, разновидности. Мосуль 2 Криптографические системы защиты информации. Појходы к оценке стойкости апторитмов пифрования. Электронные ресурсы молулярной арифметнки. Калькуляторы. Пескрослучайные последовательности. Свойства, разновия. Лосков Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES 3. Сталдарт пифрования. Алгоритм AES 3. Сталдарт пифрования. Алгоритм AES 3. Сталдарт пиф		МОДУЛЯРНАЯ АРИФМЕТИКА				Л1.2
2. Свойство коммутативности . Функция Эйлера. 3. Свойства целочисленных операций mod N. 4. Выгивление обратных величин ПЗ1 4 ОПК-9 ЛЗ.1 1.5 Практическое занятие № 1. ПЗ2 2 ОПК-9 ЛЗ.1 1.6 Практическое занятие № 2. ПЗ2 2 ОПК-9 ЛЗ.1 1.7 Лекция №5 ПЗ Декция №5 ПЗ 2 ОПК-9 ЛП.1 1.8 Практическое занятие № 3 ПЗ 3 2 ОПК-9 ЛП.2 1.9 Практическое занятие № 3 ПЗ 3 2 ОПК-9 ЛЗ.1 1.9 Практическое занятие № 4 Метод полиномов. ПЗ 4 2 ОПК-9 ЛЗ.1 1.10 Лабораторияя работа № 1. ЛР 4 ОПК-9 ЛЗ.2 1.11 Лабораторияя работа № 2. ЛР 4 ОПК-9 ЛЗ.2 1.12 Лекция №6. Ле 4 ОПК-9 ЛЗ.2 1.12 Лекция №6. Ле 4 ОПК-9 ЛЗ.1 1.13 Практическое занятие № 5 Графические тесты. Проверка на монотонность. Опсночные порязин						
3. Свойства целочисленных операций mod N. 4. Вычисление обратных величин 1.5 Практическое занятие № 1.6 Практическое занятие № 1.7 Лекция №5 1.7 Лекция №5 1.8 Практическое занятие № 1.9 Лекция №5 1.1 Лекция №5 1.1 Лекция №5 1.2 ОПК-9 1.3 Лекция №5 1.3 Практическое занятие № 1.4 Методы персетановки Методы подетановки и замены. Методы аналитических преобразований 1.8 Практическое занятие № 3 Методы умножения матриц, «укладки ранца». 1.9 Практическое занятие № 4 Метод полиномов. 1.10 Лабораторная работа №1. Пифры замены. 1.11 Лабораторная работа №2. Пифры персетановки. 1.12 Лекция №6. Гаммирование. Основные понятия. Методы тестирования псевдослучайных последовательностей. Комбинированные методы информация. 1.13 Практическое занятие № 5 Графические тесты. Проверка на монотопность. Опеночные тесты. Опеночные тесты. 1.14 Лабораторная работа № 3 Генерация дискретных случайных величин (событий) с помощью датчика ПСП. 1.9 История появления шифров. Доктрина информационной безопасности Российской Федерации. Обеспечение сохратения коммерческой тайны предприятия. Каталог обобщенных мероприятий позащите конфиденциальной информации. Подходы к оценке стоты моммерческой тайны предприятия. Каталог обобщенных мероприятий позащите конфиденциальной информации. Подходы к оценке стоты моммерческой тайны предприятия. Каталог обобщенных мероприятий позащите конфиденциальной информации. Подходы к оценке стотием вифромации. Подходы к оценке стотием вифромации. Подходы к оценке стотием авторитмов шифровация. Занктронные весурь модулярной арифметики. Калькуляторы. Певупостучийные АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Скема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Лигоритм DES. Режим шифровация. Алгоритм АЕS						
4. Вычисление обратных величин Практическое занятие 1. ПЗ1 4 ОПК-9 ЛЗ.1 1.6 Практическое занятие №2 Общие формулы вычисления больших степеней ПЗ2 2 ОПК-9 ЛЗ.1 1.7 Лекция №5 КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ. Методы перестановки. Методы подстановки и замены. Методы аналитических преобразований ЛІ 2 ОПК-9 ЛЗ.1 1.8 Практическое запятие № 3 Методы умножения матрип, «укладки ранца». 133 2 ОПК-9 ЛЗ.1 1.9 Практическое запятие № 4 Метод полипомов. ПЗ4 2 ОПК-9 ЛЗ.1 1.10 Лабораторная работа №1. Шифры замены. ЛР1 4 ОПК-9 ЛЗ.2 1.11 Лабораторная работа №2. Шифры замены. ЛР2 4 ОПК-9 ЛЗ.2 1.12 Лекция №6. Гаммирование. Основные понятия. Методы тестрирование. Основные понятия. Методы тестрирования псевдослучайных последовательностей. Комбинированные методы пифрования. ЛВ 2 ОПК-9 ЛЗ.1 1.13 Практическое занятие № 5 Графические тесты. Проверка на монотопность. Опсночные тесты. Проверка на монотопность. Опсночные тесты. Проверка на монотопность. Опсночные ресурена модуаний событий с помощью датчика ПСП. ПРЗ 4 ОПК-9 ЛЗ.1 1.9 История появления шфоровации. Обсепечение сохранения вомнерческой тайны предпрактия. Каталог обобщеных мероприятий позащите конфидентий подосл						
1.5 Практическое занятие 1. Вычисления по модулю п. ПЗ 0 1 4 0ПК-9 ЛЗ.1 1.6 Практическое занятие № 2 Общие формулы вычисления больших степеней ПЗ 2 2 0ПК-9 ЛЗ.1 1.7 Лскция №5 КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ. Методы перестановки. Методы подстановки и замены. Методы парастановки и торы умножения матрип, «укладки ранца». ПЗ 3 2 0ПК-9 ЛЗ.1 1.8 Практическое занятие № 3 Методы умножения матрип, «укладки ранца». ПЗ 4 2 0ПК-9 ЛЗ.1 1.9 Практическое занятие № 4 Метод полипомов. ПЗ 4 2 0ПК-9 ЛЗ.2 1.10 Лабораторная работа №1. Шифры замсны. ЛР 4 0ПК-9 ЛЗ.2 1.11 Лабораторная работа №2. Шифры перестановки. ЛР 4 0ПК-9 ЛЗ.2 1.12 Лекция №6. Гаммирование. Основные понятия. Методы тестерования псекдослучайных последовательностей . Комбинированые методы инфромация Л6 4 0ПК-9 ЛЗ.1 1.13 Практическое запятие № 5 Графические тесты. Проверка на монотонность. Опеночные песты помощью датчика ПСП. ДРЗ 4 0ПК-9 ЛЗ.1 1.14 Лабораторная работа № 3 Генерация дискретных случайных величин (событий) с помощью датчика ПСП. СРС 28 0ПК-9 ЛЗ.1 1.9 История появления шифромации. ПОлходы к оцеке стойкости алгоритмов шифрования. Электромучайныь последовятельности. Свойства, разновини (50-28)		<u>-</u>				
Вычисления по модулю п. 1.6 Практическое занятие №2 Общие формулы вычисления больших степеней	1.5		П31	4	ОПК-9	Л3.1
1.6 Практическое занятие №2 Общие формулы вычисления больших степеней ПЗ2 2 ОПК-9 ЛЗ.1 1.7 Лекция №5 КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ. Методы перестановки. Методы подстановки и замены. Методы перестановки. Методы подстановки и замены. Методы запитических преобразований ЛБ 2 ОПК-9 ЛЗ.1 1.8 Практическое занятие № 3 Методы умножения матриц, «укладки ранца». ПЗ3 2 ОПК-9 ЛЗ.1 1.9 Практическое занятие № 4 Метод полипомов. ПЗ4 2 ОПК-9 ЛЗ.1 1.10 Лабораторная работа №1. Шифры замены. ПР1 4 ОПК-9 ЛЗ.2 1.11 Лабораторная работа №2. ПИфры перестановки. ЛР2 4 ОПК-9 ЛЗ.2 1.12 Лекция №6. Гаммирование. Осповные полятия. Методы тестирования псевдослучайных последовательностей. Комбинированные методы шифрования Л6 4 ОПК-9 ЛЗ.1 1.13 Практическое занятие № 5 Графические тесты. Проверка на монотонность. Опеночные тесты. Проверка на монотонность. Опеночные тесты ПЗ5 2 ОПК-9 ЛЗ.1 1.14 Лабораторная работа № 3 Генерация дискретных случайных величин (событий) с помощью датчика ПСП. ЛР3 4 ОПК-9 ЛЗ.1 1.9 История появления шифров. Доктрина информационной безопасности Российской Федерации. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Подходы к оценке стойкости апгоритмов шифрования. Электроные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Л7 4 ОПК-6 Л1.						
1.7 Лекция №5 ЛБ 2 ОПК-9 Л1.1 Л1.2 Л1.3 Методы перестановки. Методы подстановки и замены. Методы аналитических преобразований ПЗЗ 2 ОПК-9 Л3.1 1.8 Практическое занятие № 3 ПЗЗ 2 ОПК-9 Л3.1 1.9 Практическое занятие № 4 Метод полиномов. ПЗ4 2 ОПК-9 Л3.1 1.10 Лабораторная работа №1. Шифры замены. ЛР1 4 ОПК-9 Л3.2 1.11 Лабораторная работа №2. Пифры перестановки. ЛР2 4 ОПК-9 Л3.2 1.12 Лекция №6. Гаммирование. Основные понятия. Методы песеторания псевдослучайных последовательностей. Комбинированиы методы пифрования Л6 4 ОПК-9 Л1.1 1.13 Практическое занятие № 5 Практическое занятие № 5 ПЗ5 2 ОПК-9 Л3.1 1.13 Практическое занятие № 5 Практическое занятие № 5 ПЗ5 2 ОПК-9 Л3.1 1.14 Лабораторная работа № 3 Генерация дискретных случайных величин (событий) с помощью датчика ПСП. ПР ОПК-9 Л3.1 1.9 История появления пифром СРС 28 ОПК-6 </td <td>1.6</td> <td>Практическое занятие №2</td> <td>П32</td> <td>2</td> <td>ОПК-9</td> <td>Л3.1</td>	1.6	Практическое занятие №2	П32	2	ОПК-9	Л3.1
1.7 Лекция №5 ЛБ 2 ОПК-9 Л1.1 Л1.2 Л1.3 Методы перестановки. Методы подстановки и замены. Методы аналитических преобразований ПЗЗ 2 ОПК-9 Л3.1 1.8 Практическое занятие № 3 ПЗЗ 2 ОПК-9 Л3.1 1.9 Практическое занятие № 4 Метод полиномов. ПЗ4 2 ОПК-9 Л3.1 1.10 Лабораторная работа №1. Шифры замены. ЛР1 4 ОПК-9 Л3.2 1.11 Лабораторная работа №2. Пифры перестановки. ЛР2 4 ОПК-9 Л3.2 1.12 Лекция №6. Гаммирование. Основные понятия. Методы песеторания псевдослучайных последовательностей. Комбинированиы методы пифрования Л6 4 ОПК-9 Л1.1 1.13 Практическое занятие № 5 Практическое занятие № 5 ПЗ5 2 ОПК-9 Л3.1 1.13 Практическое занятие № 5 Практическое занятие № 5 ПЗ5 2 ОПК-9 Л3.1 1.14 Лабораторная работа № 3 Генерация дискретных случайных величин (событий) с помощью датчика ПСП. ПР ОПК-9 Л3.1 1.9 История появления пифром СРС 28 ОПК-6 </td <td></td> <td>Общие формулы вычисления больших степеней</td> <td></td> <td></td> <td></td> <td></td>		Общие формулы вычисления больших степеней				
КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ. Л1.2 Методы перестановки. Методы подстановки и замены. Л1.3 1.8 Практическое занятие № 3 П33 2 ОПК-9 Л3.1 1.9 Практическое занятие № 4 Метод полиномов. П34 2 ОПК-9 Л3.1 1.10 Лабораторная работа №1. ЛР1 4 ОПК-9 Л3.2 1.11 Лабораторная работа №2. ЛР2 4 ОПК-9 Л3.2 1.11 Лабораторная работа №2. ЛР2 4 ОПК-9 Л3.2 1.12 Лекция №6. Л6 4 ОПК-9 Л3.2 1.12 Лекция №6. Л6 4 ОПК-9 Л3.1 1.12 Лекция №6. Л6 4 ОПК-9 Л1.1 1.12 Лекция №6. Л6 4 ОПК-9 Л1.1 1.13 Практическое занятие № 5 Прафические тесты. Проверка на монотонность. Прафические тесты Прафические тесты. Проверка на монотонность. 1.14 Лабораторная работа № 3 Генерация дискретных случайных тесты пифров. Доктрина пифров. СРС 28 ОПК-9 Л3.1 1.9	1.7		Л5	2	ОПК-9	Л1.1
Методы перестановки. Методы подстаповки и замены. Л1.3 Методы аналитических преобразований ПЗЗ 2 ОПК-9 ЛЗ.1 1.8 Практическое занятие № 3 Методы умножения матриц, «укладки ранца». ПЗЗ 2 ОПК-9 ЛЗ.1 1.9 Практическое занятие № 4 Метод полиномов. ПЗ4 2 ОПК-9 ЛЗ.2 1.10 Лабораторная работа №1. Пифры замены. ЛР1 4 ОПК-9 ЛЗ.2 1.11 Лабораторная работа №2. Пифры перестановки. ЛР2 4 ОПК-9 ЛЗ.2 1.12 Лекция №6. Гаммирование. Основные понятия. Методы тестирования псевдослучайных последовательностей . Комбинированияы пифрования Л6 4 ОПК-9 ЛЗ.1 1.13 Практическое занятие № 5 Графические тесты. Проверка на монотонность. Оценочные тесты ПЗ5 2 ОПК-9 ЛЗ.1 1.14 Лабораторная работа № 3 Генерация дискретных случайных величин (событий) с помощью датчика ПСП. СРС 28 ОПК-6 Л1.1 1.9 История появления шифров. Обеспечение сохранения коммерческой тайны предприятия. Катапот обобщенных мероприятий по защите конфиденциальной информации. Подходы к оценке стойкости апторитмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевлослучайные последовательности. Свойства, разновидности. СРС 28 ОПК-6 Л1.1 Модуль 2 Криптографические системы защиты информации (50-28) Л7 4 ОПК-6 Л1.1 1.1 Схема Фейстеля. Типичные операции. Достоинства и педестатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES Л7 4 ОПК-9 Л1.2		КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ.				
Методы аналитических преобразований Практическое занятие № 3 ПЗЗ 2 ОПК-9 ЛЗ.1 1.9 Практическое занятие № 4 Метод полиномов. ПЗ4 2 ОПК-9 ЛЗ.1 1.10 Лабораторная работа №1. ЛР1 4 ОПК-9 ЛЗ.2 Шифры замены. ЛР2 4 ОПК-9 ЛЗ.2 Шифры перестановки. ЛР2 4 ОПК-9 ЛЗ.2 Пабораторная работа №2. ЛР2 4 ОПК-9 ЛЗ.2 Пифры перестановки. Л6 4 ОПК-9 ЛЗ.1 1.12 Лекция №6. Л6 4 ОПК-9 Л1.1 Памирования. Методы тестирования псевдослучайных посиседовательностей. Комбинирования посиседовательностей. Комбинирования посиседовательности посисиской оценовательностей посисиской случайных величин (событий) с помощью датчика ПСП. ПЗ5 2 ОПК-9 Л3.1 1.14 Лабораторная работа № 3 Геперация дискретных случайных величин (событий) с помощью датчика ПСП. Доктрина информационной безопасности Российской Федерации. ОПК-9 Л3.1 1.9 История появления шифоры появления шифоры появления перестайны прединия комфирации.		· ·				Л1.3
1.8 Практическое занятие № 3 ПЗЗ 2 ОПК-9 ЛЗ.1 1.9 Практическое занятие № 4 Метод полиномов. ПЗ4 2 ОПК-9 ЛЗ.1 1.10 Лабораторная работа №1. ЛР1 4 ОПК-9 ЛЗ.2 Пифры замены. ЛР2 4 ОПК-9 ЛЗ.2 Шифры перестаповки. ЛР2 4 ОПК-9 ЛЗ.2 Пифры перестаповки. ЛВ6 4 ОПК-9 ЛЗ.1 1.12 Лекция №6. ЛВ6 4 ОПК-9 ЛЗ.1 1.13 Практическое занятие № 5 Графические тесты. Проверка на монотопность. ПЗ5 2 ОПК-9 ЛЗ.1 1.14 Лабораторная работа № 3 Генерация дискретных случайных величин (событий) е помощью датчика ПСП. ЛР3 4 ОПК-9 ЛЗ.1 1.9 История появления шифров. СРС 28 ОПК-6 ЛП.1 1.0		-				
Методы умножения матриц, «укладки ранца». ПЗ4 2 ОПК-9 ЛЗ.1 1.10 Лабораторная работа №1. Шифры замены. ЛР1 4 ОПК-9 ЛЗ.2 1.11 Лабораторная работа №2. Шифры перестановки. ЛР2 4 ОПК-9 ЛЗ.2 1.12 Лекция №6. Гаммирование. Основные понятия. Методы тестирования псевдослучайных последовательностей. Комбинированные методы шифрования Л6 4 ОПК-9 Л1.1 Л1.2 Л1.3 1.13 Практическое занятие № 5 Графические тесты. Проверка на монотонность. Оценочные тесты ПЗ5 2 ОПК-9 Л3.1 1.14 Лабораторная работа № 3 Генерация дискретных случайных величин (событий) с помощью датчика ПСП. ЛРЗ 4 ОПК-9 Л3.1 1.9 История появления шифров. Доктрина информационной безопасности Российской Федерации. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Подходы к оценке стойкости алторитмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Л7 4 ОПК-6 Л1.1 Модуль 2 Кринтографические системы защиты информации (50+28) Л7 4 ОПК-6 Л1.1 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шиф	1.8		П33	2.	ОПК-9	ПЗ 1
1.9 Практическое занятие № 4 Метод полиномов. ПЗ4 2 ОПК-9 ЛЗ.1 1.10 Лабораторная работа №1. ЛР1 4 ОПК-9 ЛЗ.2 1.11 Лабораторная работа №2. ЛР2 4 ОПК-9 ЛЗ.2 1.12 Лекция №6. Л6 4 ОПК-9 Л1.1 Гаммирование. ЛР3 4 ОПК-9 Л1.1 Практическое занятие № 5 Графические тесты. Проверка на монотонность. ПЗ5 2 ОПК-9 Л3.1 1.14 Лабораторная работа № 3 Генерация дискретных случайных величин (событий) с помощью датчика ПСП. ЛР3 4 ОПК-9 Л3.1 1.19 История появления шифров. Доктрина информационной безопасности Российской Федерации. СРС 28 ОПК-9 Л1.2 1.0 История появления шифромации. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. СРС 28 ОПК-9 Л1.3 Модуль 2 Кринтографические системы защиты информации (50-28) Пл. 4 ОПК-9 Л1.1 Модуль 2 Кринтографические системы защиты информации (50-28	1.0	<u> </u>	1133	_		313.1
1.10 Лабораторная работа №1. ЛР1 4 ОПК-9 Л3.2 1.11 Лабораторная работа №2. ЛР2 4 ОПК-9 Л3.2 1.12 Лекция №6. Л6 4 ОПК-9 Л1.1 1.12 Лекция №6. Л6 4 ОПК-9 Л1.2 Методы тестирования псевдослучайных последовательностей . Комбинированные методы шифрования Л1.3 П35 2 ОПК-9 Л3.1 1.13 Практическое занятие № 5 Графические тесты. Проверка на монотонность. Опеночные тесты П35 2 ОПК-9 Л3.1 1.14 Лабораторная работа № 3 Генерация дискретных случайных величин (событий) с помощью датчика ПСП. ЛР3 4 ОПК-9 Л3.1 1.9 История появления шифров. Доктрина информации. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Полходы к оценке стойкости алгоритмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Л1.3 Л1.3 Модуль 2 Криптографические системы защиты информации (50+28) 2.1 Лекция №7. Л7 4 ОПК-9 Л1.1 Симметричные операции. Достоинства и недостатки	1 0		ПЗЛ	2	ОПК-0	ПЗ 1
Шифры замены. 1.11 Лабораторная работа №2. ЛР2 4 ОПК-9 Л3.2	1.9	практическое занятие му 4 метод полиномов.	1134	2	OHK-9	113.1
IIIифры замены. ЛР2 4 ОПК-9 Л3.2 IIIифры перестановки. Л6 4 ОПК-9 Л1.1 1.12 Лекция №6. Л6 4 ОПК-9 Л1.1 Комбинирования псевдослучайных последовательностей: Комбинированные методы шифрования Л1.3 Л1.3 1.13 Практическое занятие № 5 П35 2 ОПК-9 Л3.1 Графические тесты. Проверка на монотопность. Оценочные тесты Пабораторная работа № 3 Генерация дискретных случайных величин (событий) с помощью датчика ПСП. ЛР3 4 ОПК-9 Л3.1 1.9 История появления шифров. Доктрина информационной безопасности Российской Федерации. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Подходы к оценке стойкости алгоритмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Вобить в фактеритеритеритеритеритеритеритеритеритери	1.10	Лабораторная работа №1.	ЛР1	4	ОПК-9	Л3.2
IIIифры перестановки. Л6 4 ОПК-9 Л1.1 1.12 Лекция №6. Л6 4 ОПК-9 Л1.1 1.12 Лекция №6. Л1.2 Л1.2 Л1.3 Методы тестирования псевдослучайных последовательностей . Комбинированные методы шифрования Л1.3 Л1.3 <td></td> <td>Шифры замены.</td> <td></td> <td></td> <td></td> <td></td>		Шифры замены.				
1.12 Лекция №6. Л6 4 ОПК-9 Л1.1 Гаммирование. Основные понятия. Методы тестирования псевдослучайных последовательностей . Комбинированные методы шифрования Л1.3 П35 2 ОПК-9 Л3.1 1.13 Практическое занятие № 5 Графические тесты. Проверка на монотонность. Опеночные тесты ЛВ3 2 ОПК-9 Л3.1 1.14 Лабораторная работа № 3 Генерация дискретных случайных величин (событий) с помощью датчика ПСП. ЛРЗ 4 ОПК-9 Л3.1 1.9 История появления шифров. Доктрина информации. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Подходы к оценке стойкости аргоритмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. ДГ 4 ОПК-6 Л1.1 Модуль 2 Криптографические системы защиты информации (50+28) ДГ 4 ОПК-6 Л1.1 2.1 Лекция №7. СиммЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES ЛГ 4 ОПК-6 Л1.1	1.11	Лабораторная работа №2.	ЛР2	4	ОПК-9	Л3.2
Подходы к оценке стойкости алгоритмов шифрования. Подходы к оценке стойкости алгоритмов шифрования. Подходы к оценке стойкости алгоритмов шифрования. 2. Пекция №7. СиммЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES		Шифры перестановки.				
Методы тестирования псевдослучайных последовательностей . Комбинированные методы шифрования Л1.3 1.13 Практическое занятие № 5 Графические тесты. Проверка на монотонность. Оценочные тесты ПЗ5 2 ОПК-9 Л3.1 1.14 Лабораторная работа № 3 Генерация дискретных случайных величин (событий) с помощью датчика ПСП. ЛР3 4 ОПК-9 Л3.1 1.9 История появления шифров. Доктрина информационной безопасности Российской Федерации. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Подходы к оценке стойкости алгоритмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Войства, разновидности. Л7 4 ОПК-6 Л1.1 2.1 Лекция №7. СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES Л7 4 ОПК-9 Л1.2	1.12	Лекция №6.	Л6	4	ОПК-9	Л1.1
последовательностей . Комбинированные методы шифрования последовательностей . Комбинированные методы шифрования ПЗ5 2 ОПК-9 ЛЗ.1 1.13 Практическое занятие № 5 Графические гесты. Проверка на монотонность. Оценочные тесты ПЗ5 2 ОПК-9 ЛЗ.1 1.14 Лабораторная работа № 3 Генерация дискретных случайных величин (событий) с помощью датчика ПСП. ЛРЗ 4 ОПК-9 ЛЗ.1 1.9 История появления шифров. Доктрина информационной безопасности Российской Федерации. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Подходы к оценке стойкости алгоритмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Видение тесты При на предприятий информации (50+28) 2.1 Лекция №7. СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES Л7 4 ОПК-6 Л1.1 ОПК-9 Л1.2 Л1.3		Гаммирование. Основные понятия.				Л1.2
шифрования 1.13 Практическое занятие № 5 ПЗ5 2 ОПК-9 ЛЗ.1 1.14 Лабораторная работа № 3 Генерация дискретных случайных величин (событий) с помощью датчика ПСП. ЛР3 4 ОПК-9 ЛЗ.1 1.9 История появления шифров. Доктрина информационной безопасности Российской Федерации. СРС 28 ОПК-6 Л1.1 Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Подходы к оценке стойкости алгоритмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Л7 4 ОПК-6 Л1.1 2.1 Лекция №7. СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES Л7 4 ОПК-9 Л1.2		Методы тестирования псевдослучайных				Л1.3
шифрования 1.13 Практическое занятие № 5 ПЗ5 2 ОПК-9 ЛЗ.1 1.14 Лабораторная работа № 3 Генерация дискретных случайных величин (событий) с помощью датчика ПСП. ЛР3 4 ОПК-9 ЛЗ.1 1.9 История появления шифров. Доктрина информационной безопасности Российской Федерации. СРС 28 ОПК-6 Л1.1 Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Подходы к оценке стойкости алгоритмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Л7 4 ОПК-6 Л1.1 2.1 Лекция №7. СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES Л7 4 ОПК-9 Л1.2						
Графические тесты. Проверка на монотонность. Оценочные тесты 1.14 Лабораторная работа № 3 Генерация дискретных случайных величин (событий) с помощью датчика ПСП. ЛРЗ 4 ОПК-9 ЛЗ.1 1.9 История появления шифров. Доктрина информационной безопасности Российской Федерации. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Подходы к оценке стойкости алгоритмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Модуль 2 Криптографические системы защиты информации (50+28) 2.1 Лекция №7. СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES Л7 4 ОПК-6 Л1.1 Л1.3						
Графические тесты. Проверка на монотонность. Оценочные тесты 1.14 Лабораторная работа № 3 Генерация дискретных случайных величин (событий) с помощью датчика ПСП. ЛРЗ 4 ОПК-9 ЛЗ.1 1.9 История появления шифров. Доктрина информационной безопасности Российской Федерации. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Подходы к оценке стойкости алгоритмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Модуль 2 Криптографические системы защиты информации (50+28) 2.1 Лекция №7. СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES Л7 4 ОПК-6 Л1.1 Л1.3	1.13	Практическое занятие № 5	П35	2	ОПК-9	Л3.1
 Лабораторная работа № 3 Генерация дискретных случайных величин (событий) с помощью датчика ПСП. История появления шифров. Доктрина информационной безопасности Российской Федерации. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Подходы к оценке стойкости алгоритмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Модуль 2 Криптографические системы защиты информации (50+28) Лекция №7. СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES 						
Случайных величин (событий) с помощью датчика ПСП. 1.9 История появления шифров. Доктрина информационной безопасности Российской Федерации. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Подходы к оценке стойкости алгоритмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Модуль 2 Криптографические системы защиты информации (50+28) 2.1 Лекция №7. СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES		Оценочные тесты				
1.9 История появления шифров. Доктрина информационной безопасности Российской Федерации. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Подходы к оценке стойкости алгоритмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Войства	1.14	Лабораторная работа № 3 Генерация дискретных	ЛР3	4	ОПК-9	Л3.1
Доктрина информационной безопасности Российской Федерации. ОПК-9 Л1.2 Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Подходы к оценке стойкости алгоритмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Видерации (50+28) 2.1 Лекция №7. СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES Л7 4 ОПК-6 Л1.1		случайных величин (событий) с помощью датчика ПСП.				
 Федерации. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Подходы к оценке стойкости алгоритмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Модуль 2 Криптографические системы защиты информации (50+28) 2.1 Лекция №7. СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES 	1.9		CPC	28	ОПК-6	
Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Подходы к оценке стойкости алгоритмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Модуль 2 Криптографические системы защиты информации (50+28) 2.1 Лекция №7. Л7 4 ОПК-6 Л1.1 СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. ОПК-9 Л1.2 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES		Доктрина информационной безопасности Российской			ОПК-9	Л1.2
предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Подходы к оценке стойкости алгоритмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Модуль 2 Криптографические системы защиты информации (50+28) 2.1 Лекция №7. Л7 4 ОПК-6 Л1.1 СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES						Л1.3
защите конфиденциальной информации. Подходы к оценке стойкости алгоритмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Модуль 2 Криптографические системы защиты информации (50+28) 2.1 Лекция №7. СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES		Обеспечение сохранения коммерческой тайны				
Подходы к оценке стойкости алгоритмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Модуль 2 Криптографические системы защиты информации (50+28) 2.1 Лекция №7. СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES						
Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Модуль 2 Криптографические системы защиты информации (50+28) 2.1 Лекция №7. СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. Л7 4 ОПК-6 Л1.1 Симметричные операции. Достоинства и недостатки. Л1.3 Л1.3 2. Алгоритм DES. Режим шифрования. Алгоритм AES Л1.3		защите конфиденциальной информации.				
Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности. Модуль 2 Криптографические системы защиты информации (50+28) 2.1 Лекция №7. Л7 4 ОПК-6 Л1.1 СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 0ПК-9 Л1.2 1.2 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. Л1.3 Л1.3 2. Алгоритм DES. Режим шифрования. Алгоритм AES Попкта правина править						
Модуль 2 Криптографические системы защиты информации (50+28) 2.1 Лекция №7. Л7 4 ОПК-6 Л1.1 СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. Достоинства и Л1.3 2. Алгоритм DES. Режим шифрования. Алгоритм AES Л7 4 ОПК-9 Л1.2						
Модуль 2 Криптографические системы защиты информации (50+28) 2.1 Лекция №7. Л7 4 ОПК-6 Л1.1 СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. Л1.3 Л1.3 2. Алгоритм DES. Режим шифрования. Алгоритм AES 1. Схема Фейстеля. 1. Схема Фейстеля.<		Калькуляторы.				
Модуль 2 Криптографические системы защиты информации (50+28) 2.1 Лекция №7. Л7 4 ОПК-6 Л1.1 СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. Л1.3 Л1.3 2. Алгоритм DES. Режим шифрования. Алгоритм AES 1 П. Схема Пинана правина		Псевдослучайные последовательности. Свойства,				
2.1 Лекция №7. Л7 4 ОПК-6 Л1.1 СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. Достоинства и недостатки. Л1.3 2. Алгоритм DES. Режим шифрования. Алгоритм AES Л1.3		разновидности.				
2.1 Лекция №7. Л7 4 ОПК-6 Л1.1 СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. Достоинства и недостатки. Л1.3 2. Алгоритм DES. Режим шифрования. Алгоритм AES Л1.3						
2.1 Лекция №7. Л7 4 ОПК-6 Л1.1 СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. Достоинства и недостатки. Л1.3 2. Алгоритм DES. Режим шифрования. Алгоритм AES Л1.3		Модуль 2 Криптографические системы зашиты и	нформа	апии (5	50+28)	
СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES	2.1					Л1.1
1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES						
недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES						
2. Алгоритм DES. Режим шифрования. Алгоритм AES						
		<u> </u>				

	Алгоритм. Основные режимы шифрования. Основной				
	шаг криптопреобразования.				
2.2	Практическое занятие №6	П36	2	ОПК -9	Л3.1
	Режимы гаммирования и гаммирования с обратной				
2.2	СВЯЗЬЮ	IID4	4	OTIL	паа
2.3	Лабораторная работа № 4 Блочный шифр DES, разновидности алгоритма DES.	ЛР4	4	ОПК-6 ОПК-9	Л3.2
2.4	Лабораторная работа № 5	ЛР5	4	ОПК-9	Л3.2
2.4	Алгоритм ГОСТ 28147-89.	311 3	7	OIIK-1	313.2
2.5	Лекция №8	Л8	4	ОПК-6	Л1.1
	АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ			ОПК-9	Л1.2
	1. Обобщенная схема асимметричной криптосистемы				Л1.3
	шифрования.				
	2. Характерные особенности асимметричных				
	криптосистем.				
2.6	Лекция №9	Л9	4	ОПК-6	Л1.1
	АСИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ		•	ОПК-9	Л1.2
	1. Алгоритм рюкзака.				Л1.3
	2. Схемы шифрования RSA и Эль Гамаля.				
	3. Процедуры шифрования и дешифрования.				
	4. Гибридные схемы шифрования				
2.7	Практическое занятие №7	П37	4	ОПК-6	Л3.1
	Г Криптоалгоритмы RSA и Эль Гамаля			ОПК-9	
2.8	Лабораторная работа № 6	ЛР6	4	ОПК-6	Л3.2
	Криптоалгоритм RSA			ОПК-9	
2.9	Лекция №10	Л10	2	ОПК-6	Л1.1
	АЛГОРИТМЫ ХЭШИРОВАНИЯ			ОПК-9	Л1.2
	1. Криптографические хэш-функции.				Л1.3
	2. Конструкция Меркла-Дамгарда.				
	3. Сравнительный анализ известных функций				
	хэширования.				
	4. Функция ГОСТЗ 34.11-94				
2.10	Практическое занятие №8	П38	2	ОПК-6	Л3.1
	ТРЕБОВАНИЯ К ХЭШ-ФУНКЦИЯМ. СВОЙСТВА.			ОПК-9	
2.11	Лабораторная работа № 7	ЛР7	2	ОПК-6	Л3.2
	АЛГОРИТМЫ ХЭШИРОВАНИЯ			ОПК-9	
2.12	Лекция №11	Л11	4	ОПК-6	Л1.1
	АЛГОРИТМЫ ЭЛЕКТРОННОЙ ПОДПИСИ (ЭП)			ОПК-9	Л1.2
	1. Электронная я подпись. Назначение и классификация.				Л1.3
	2. Алгоритмы электронной цифровой подписи RSA и				
	Эль Гамаля (EGSA).				
	3. Стандарт ГОСТ 3 34.10-2011				
2.13	Практическое занятие №9	П39	2	ОПК-6	Л3.1
	Процедура формирования и проверки ЭЦП			ОПК-9	
2.14	Лабораторная работа № 8 Стандарты на электронную	ЛР8	4	ОПК-6	Л3.2
	(цифровую) подпись: цифровая подпись DSS, цифровая			ОПК-9	

	подпись ГОСТ Р34.10-94. Цифровые подписи,						
	основанные на симметричных криптосистемах.						
2.15	Лабораторная работа № 9 «Анализ электронной	ЛР9	4	ОПК-6	Л3.2		
	цифровой подписи на основе криптосистемы Эль			ОПК-9			
	Гамаля».						
2.16	Алгоритм симметричной системы шифрования данных — стандарт ГОСТ 28147-89. Алгоритм ассиметричной (двухключевой) системы шифрования данных RSA. Алгоритмы хэширования MD5, SHA. Федеральный закон Российской Федерации «Об электронной подписи» 6.04.2011г. № 63-ФЗ РФ Нормативно-правовые акты Российской Федерации о ведении электронного документооборота. Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация.	CPC	26	ОПК-1	Л1.1 Л1.2 Л1.3		
	Экзамен – 36 часов						

Итого – 180 часов

5. Учебно-методическое и информационное обеспечение дисциплины

		5.1. Рекомендуемая литература				
	5.1.1. Основная литература					
Код	Авторы, составители	Заглавие	Издательство, год	Кол.		
Л1.1	Бабаш А. В.	1. Криптографические методы защиты информации: Учебное пособие для вузов. http://znanium.com/catalog/product/1022055	М.: ИЦ РИОР, НИЦ ИНФРА- М, 2019 413 с.:	Э1		
Л1.2	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: учеб. пособие / — 3-е изд., перераб. и доп.	М.: РИОР: ИНФРА-М, 2017. — 322 с.	Э2		
Л1.3	А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков;	информации: Учебник для вузов / Под ред. А.П. Зайцева - 7 изд., исправ; 60х90 1/16 - (Уч. для вузов). http://znanium.com/catalog/product/390284	М.: Гор. линия- Телеком, 2012. - 442c.			
Л1.4	Скрыль С. В.	Технические средства и методы защиты информации / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В: ISBN 978-5-9912-0084-4 - Режим доступа: http://znanium.com/catalog/product/560580	М.:Гор. линия- Телеком, 2012. - 616 с	Э4		
	Авторы,	6.1.2. Дополнительная литература	Издательство,			
Код	составители	Заглавие	год	Кол.		
Л2.1	Басалова Г.В	Основы криптографии [Электронный ресурс]/ Басалова Г.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 282 с. Режим доступа: http://www.iprbookshop.ru/52158.— ЭБС «IPRbooks»	М.— М.: Интернет- Университет Информацион ных Технологий (ИНТУИТ), 2016.— 282 с с	3 3		
Л2.2	Жук, О.М. Лепешкин, А.И. Тимошкин.	Магистратура). (переплет) ISBN 978-5-369- 01378-6 - Режим доступа: http://znanium.com/catalog/product/474838	- М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 392 с.:	Э6		
		етодическое обеспечение для самостоятельной раб	•	ся		
Код	Авторы, составители	Заглавие	Издательство, год	Кол.		
Л3.1	Рыбалко И.П.	Методические указания по проведению практических занятий по дисциплине «Основы криптографии»/ Рыбалко И.П. – Ростов-на - Дону: Изд-во СКФ МТУСИ, 2019. – 49 с.: ил.	РнД: СКФ МТУСИ, 2019			
Л3.2	Рыбалко И.П.	Методические указания по проведению лабораторных работ по дисциплине «Основы криптографии»/ Рыбалко И.П. – Ростов-на - Дону: Изд-во СКФ МТУСИ, 2019. – 59 с.: ил. 6.2. Электронные образовательные ресурсы	РнД: СКФ МТУСИ, 2019	98		
Э1	http://znanium	com/catalog/product/1022055				
Э2		com/catalog/product/763644				
52	prup.//Zmamum.c	oni catalog product 1000 11				

Э3	http://znanium.com/catalog/product/390284
Э4	http://znanium.com/catalog/product/560580
Э5	http://www.iprbookshop.ru/52158
Э6	http://znanium.com/catalog/product/474838
Э7	http://www.skf-mtusi.ru/?page_id=659
Э8	http://www.skf-mtusi.ru/?page_id=659
	6.3. Программное обеспечение
П.1	Window 8,10
П.2	Word processor Microsoft Word or LibreOffice Writer или аналог.
П.3	MS Power Point или аналог.

6. Материально-техническое обеспечение дисциплины

6.1 МТО лек	6.1 МТО лекционных занятий				
1 Лекционная аудитория, оборудованная интерактивной доской, проектором					
6.2 МТО лаб	6.2 МТО лабораторных работ и практических занятий				
1 Компьютерная аудитория с выходом в интернет					
6.3 МТО рубежных контролей, экзамена					
1	Компьютерная аудитория				

7. Методические указания для обучающихся по освоению дисциплины

7.1 Указания по самостоятельной работе студента

Достижение целей эффективной подготовки студентов в вузах невозможно без их целеустремленной самостоятельной работы. При этом, безусловно, нельзя обойтись без живого общения и консультирования со стороны профессорско-преподавательского состава Самостоятельная работа студентов является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам. Обязательным компонентом самостоятельной работы студентов является внеаудиторный практикум по иностранному языку.

Самостоятельная работа организуется преподавателями, обеспечивается и контролируется кафедрами. Она предусматривает, как правило, разработку рефератов, выполнение расчетно-графических, вычислительных работ, моделирования и других творческих заданий в соответствии с учебной программой (тематическим планом изучения дисциплины). Основная цель данного вида занятий состоит в обучении курсантов методам самостоятельной работы с учебным материалом.

Материал, подлежащий обработке на самостоятельных занятиях, намечается при разработке программы самостоятельной работы. Опыт, накопленный кафедрами в организации самостоятельных занятий, что материал, выделяемый на такие занятия, должен удовлетворять следующим требованиям:

- быть изложенным в учебнике достаточно полно и с примерами;
- обеспечиваться достаточным количеством литературы, учебных пособий. учебнометодических материалов, образцов техники
 - содержать материал. углубляющий знания, полученные на лекции;
 - осваивать проблемные еще не полностью решенные вопросы.

Проведению самостоятельной работы (как и любого другого вида занятий) должна предшествовать подготовка как преподавателя, так и обучаемых.

Постановку задачи обучаемым на проведение самостоятельного занятия преподаватель осуществляет на одном из занятия, предшествующему данному. Он разъясняет смысл занятия и указывает, что к нему студенты должны приготовить. Задание на самостоятельную работу должно быть выдано заблаговременно с тем, чтобы слушатели имели время на информационный поиск в библиотеке необходимых пособий.

Методику самостоятельной работы все обучаемые выбирают индивидуально, но методика достижения конечной цели может определяться преподавателем и включать: последовательность изучения и усвоения учебно-методического материала, пособий, руководств, наставлений, техники и т.д.; определение главного в изучаемом материале, материале, который необходимо законспектировать; просмотр учебных кинофильмов и их обсуждение; работу студентов по индивидуальным заданиям; опрос обучаемых в течении 7-10 минут с целью проверки усвоения главного из прочитанного материала.

При возникновении затруднений у обучаемых в разрешении вопросов задания преподавателю необходимо предусмотреть, чтобы каждый обучаемый мог получить оперативную консультацию по любому вопросу, если же при самостоятельной работе возникают затруднения по одному и тому же материалу (вопросу) у многих обучаемых, то желательно провести групповую консультацию.

Для контроля усвоения учебного материала целесообразно проводить в групповое собеседование или обсуждение изучаемого материала, проведение контрольных работ и т.п. Контрольные мероприятия при должной их организации позволяют не только оценивать знания материала, но и углубить и закрепить его у обучаемых.

Приветствуется использование компьютеров, которое:

- расширяет информационную баз) учебных занятий;
- повышает активность обучаемых, из пассивного получателя информации они превращаются в её добытчиков:
- способствует развитию способностей к анализу и обобщению, улучшает связанность, широту и глубину мышления;
- облегчает усвоение абстрактного материала, позволяет многое из него представить в виде конкретных образов;
- приучает к точности, аккуратности, последовательности действий способствует развитию самостоятельности.

Компьютерные технологии и программные продукты для выполнения самостоятельной работы по освоению учебного материала необходимо использовать в соответствии с указаниями методических разработок раздела 5 настоящей Рабочей программы.

Для более углубленного изучения материала по дисциплине целесообразно использовать учебные курсы сайта http://www.intuit.ru/.

Таблица 7.1 – Учебный материал, выносимый на самостоятельное изучение студентам очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 54	Неделя
	Модуль 1 – 26 часа		
1	История появления шифров.	4	1
2	Доктрина информационной безопасности Российской Федерации.	3	2
3	Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации.	3	3

3	Подходы к оценке стойкости алгоритмов шифрования.	4	4
4	Электронные ресурсы модулярной арифметики. Калькуляторы.	6	5-6
5	Псевдослучайные последовательности. Свойства, разновидности.	6	7-8
	Модуль 2 – 28 часов		
6	Алгоритм симметричной системы шифрования данных – стандарт ГОСТ 28147-89	6	9-10
7	7 Алгоритм ассиметричной (двухключевой) системы шифрования данных RSA		11-12
8	Алгоритмы хэширования MD5, SHA	4	13
10	Федеральный закон Российской Федерации «Об электронной подписи» 6.04.2011г. № 63-ФЗ РФ	4	14
11	Нормативно-правовые акты Российской Федерации о ведении электронного документооборота	4	15
12	Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация.	4	16

Дополнения и изменения в рабочей программе