Приложение 5

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»
Институт математики, физики и информационных технологий
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:
Директор института

И. Н. Якунина
«20» января 2021 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.В.ОД.2 Криптографические методы защиты информации

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 2020

Тамбов, 2021

Авторы программы:
Кандидат физико-математических наук, доцент Лопатин Дмитрий Валерьевич
Кандидат технических наук, Соловьев Денис Сергеевич

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 - Информационная безопасность (уровень бакалавриата) (приказ Министерства образования и науки РФ от «01» декабря 2016 г. № 1515).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «22» декабря 2020 г. Протокол № 4

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «20» января 2021 г. № 1.

СОДЕРЖАНИЕ

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ОПК-2 Способность применять соответствующий математический аппарат для решения профессиональных задач

ПК-1 Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

1.2 Виды и задачи профессиональной деятельности по дисциплине:

- эксплуатационная
  - установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований
  - администрирование подсистем информационной безопасности объекта
  - участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем

1.3 В результате освоения дисциплины у обучающихся должны быть сформированы следующие компетенции:

Обобщенные трудовы	Код и наименование ко	Знания и умения, необходимые дл
	ОПК-2 Способность приме	Знает и понимает: Знает и понимает:основные теоретические понятия «К
		Умеет (способен продемонстрировать): Умеет (способен продемонстрировать):решать типовые
		Владеет: Владеет:основными навыками решения задач; методам
	ПК-1 Способность выполня	Знает и понимает: Знает: методы криптографической защиты информаци
		Умеет (способен продемонстрировать): Умеет: применять знания на практике в области крипт
		Владеет: Владеет: необходимыми навыками по установке, настр

1.4 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ОПК-2 Способность применять соответствующий математический аппарат для решения профессиональных задач

№ п/п	Наименование д	Форма о		
		Очная (семест		
		1	2	3
1	Алгоритмизация и пр	+	+	+
2	Математика	+		

ПК-1 Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

№ п/п	Наименование д	Форма об			
		Очная (семестр)			
		3	4	5	7

1	Адаптационная дисци	+			
2	Основы электро- и ра	+			
3	Программно-аппаратн		+	+	
4	Техническая защита и		+	+	
5	Эксплуатационная пр				+
6	Электроника и схемот	+			

2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Криптографические методы защиты информации» относится к вариативной части учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность.

Дисциплина «Криптографические методы защиты информации» изучается в 6, 7 семестрах.

3.Объем и содержание дисциплины

3.1.Объем дисциплины: 9 з.е.

Очная: 9 з.е.

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	**324**
Контактная работа	144
Лекции (Лекции)	72
Лабораторные (Лаб. раб.)	72
Самостоятельная работа (СР)	142
Курсовая работа	2
Экзамен	36
Зачет	-

3.2.Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лекции	Лаб. раб.	СР	
		О	О	О	
6 семестр					
1	Основы информационной безопасности и защиты информации	2	-	4	Собеседование
2	История криптографии	2	-	4	Собеседование
3	Основные термины и определения. Классификация шифров	2	-	8	Тестирование; Собеседование
4	Шифры замены	2	4	8	Лабораторная работа; Собеседование

5	Шифры перестановки	2	4	8	Лабораторная работа; Тестирование; Собеседование
6	Шифры гаммирования	4	6	8	Лабораторная работа; Собеседование
7	Квантовое шифрование	2	-	8	Собеседование
8	Комбинированные шифры	4	6	8	Лабораторная работа; Собеседование
9	Шифрование с открытым ключом	4	6	8	Лабораторная работа; Тестирование; Собеседование
10	Хеш-функции	4	6	8	Лабораторная работа; Собеседование
11	Криптографические протоколы	4	-	8	Собеседование
7 семестр					
12	Протоколы обмена ключами	4	-	4	Собеседование
13	Протоколы аутентификации (идентификации)	4	6	4	Лабораторная работа; Собеседование
14	Протоколы электронной подписи	4	6	6	Лабораторная работа; Собеседование
15	Протоколы контроля целостности	4	6	6	Лабораторная работа; Собеседование
16	Протоколы электронных платежей	4	-	6	Собеседование
17	Протоколы голосования	4	-	6	Собеседование
18	Протоколы тайных многосторонних вычислений и разделения секрета	4	6	6	Лабораторная работа; Собеседование
19	Некоторые сведения из теорий алгоритмов и чисел	4	-	6	Тестирование; Собеседование
20	Основы криптоанализа	4	-	6	Собеседование; Тестирование
21	Стеганография	2	8	6	Лабораторная работа; Собеседование

22	Кодирование информации	2	8	6	Лабораторная работа; Собеседование

Тема 1. Основы информационной безопасности и защиты информации (ОПК-2)

Лекция.

Информация и информационная безопасность, основные составляющие информационной безопасности, объекты защиты, категории и носители информации, средства защиты информации.

Лабораторные работы.

Не предусмотрено

Задания для самостоятельной работы.

1. Дайте определение понятиям: «информация», «информационная безопасность», «защита информации», «информационная угроза».
2. Дайте характеристику основным составляющим информационной безопасности.
3. Перечислите основные объекты защиты.
4. Дайте характеристику понятиям «государственная тайна», «конфиденциальная информация» и «персональные данные».
5. Дайте характеристику средствам защиты информации.

Тема 2. История криптографии (ОПК-2)

Лекция.

Наивная криптография, формальная криптография, математическая криптография.

Лабораторные работы.

Не предусмотрено

Задания для самостоятельной работы.

1. Перечислите способы тайной передачи информации на расстоянии.
2. Назовите основные этапы развития криптографии.

Тема 3. Основные термины и определения. Классификация шифров (ОПК-2)

Лекция.

Основные термины и определения, основные требования к криптосистемам, классификация криптографических систем.

Лабораторные работы.

Не предусмотрено

Задания для самостоятельной работы.

1. Дайте определение понятиям «шифр», «ключ», «дешифрование».
2. Перечислите основные требования, предъявляемые к криптосистемам.
3. Дайте классификацию криптосистем по алгоритму шифрования.
4. Дайте классификацию криптосистем по стойкости шифра.

Тема 4. Шифры замены (ПК-1)

Лекция.

Основы шифрования. Шифры однозначной замены. Полиграммные шифры. Омофонические шифры. Полеалфавитные шифры. Нерегулярные шифры.

Лабораторные работы.

В лабораторной работе необходимо зашифровать свою фамилию с помощью следующих шифров:

- шифра Цезаря;
- лозунгового шифра;
- полибианского квадрата;

- шифрующей системы Трисемуса;
- шифра Playfair;
- системы омофонов (допускается для каждой буквы алфавита привести всего по две шифрозамены, т.е. принять, что все буквы имеют одинаковую вероятность появления в текстах);
- шифра Виженера.

При оформлении отчета необходимо привести исходное сообщение (фамилию), таблицу шифрозамен, ключ (если таблица шифрозамен не является ключом) и зашифрованное сообщение.

Задания для самостоятельной работы.

1. В чем заключается основная идея криптографических преобразований шифров замены?
2. Перечислите основные разновидности шифров замены.
3. Дайте характеристику разновидностям шифров замены.
4. Назовите основной недостаток шифра однозначной замены.

Тема 5. Шифры перестановки (ПК-1)

Лекция.

Основы шифрования, шифры одинарной и множественной перестановки.

Лабораторные работы.

В лабораторной работе необходимо зашифровать свою фамилию (для первых двух шифров) или фамилию и имя (для остальных) с помощью следующих шифров:

- простой одинарной перестановки;
- блочной одинарной перестановки;
- табличной маршрутной перестановки;
- вертикальной перестановки;
- поворотной решетки;
- магический квадрат (размер квадрата - 4x4);
- двойной перестановки.

При оформлении отчета необходимо привести исходное сообщение (фамилию или фамилию и имя), таблицы, ключевые слова (выбираются произвольно), маршруты вписывания и выписывания, повороты решетки и зашифрованное сообщение

Задания для самостоятельной работы.

1. В чем заключается основная идея криптографических преобразований шифров перестановки?
2. Перечислите основные разновидности шифров перестановки.
3. Дайте характеристику разновидностям шифров перестановки.

Тема 6. Шифры гаммирования (ПК-1)

Лекция.

Основы шифрования, шифрование по модулю N и 2, генерация гаммы, генераторы гамм.

Лабораторные работы.

В лабораторной работе необходимо зашифровать свою фамилию с помощью шифров гаммирования по модулю N и модулю 2.

При оформлении отчета необходимо привести исходное сообщение (фамилию), гамму и таблицы зашифрования/дешифрования.

Задания для самостоятельной работы.

1. В чем заключается основная идея криптографических преобразований аддитивных шифров?
2. Назовите основные характеристики гаммы.
3. При каких условиях применения гаммы аддитивный шифр можно считать совершенным.
4. Дайте характеристику программным способам генерации гаммы (алгоритм RANDU и BBS).
5. Что такое паритетный бит?

6. Опишите схемы шифрования с использованием синхронных и самосинхронизирующихся потоковых шифров.

Тема 7. Квантовое шифрование (ОПК-2)

Лекция.

Основы квантовой физики. Основы квантового шифрования. Шифрования с использованием линейных поляризаторов на принимающей стороне. Шифрования с использованием поляризационной разделительной призмы на принимающей стороне.

Лабораторные работы.

не предусмотрено.

Задания для самостоятельной работы.

1. Дайте определение понятиям «квант» и «фотон».
2. В чем заключается природа корпускулярно-волнового дуализма фотона?
3. В чем суть шифрования с помощью фотонов?

Тема 8. Комбинированные шифры (ОПК-2)

Лекция.

Шифры ADFGX и ADFGVX. Основы блочного комбинированного шифрования. DES. ГОСТ 28147-89. AES. ГОСТ 34.12-2015. ГОСТ 34.13-2015.

Лабораторные работы.

В лабораторной работе необходимо зашифровать свою фамилию и имя с помощью шифра ADFGVX. При оформлении отчета необходимо привести исходное сообщение (фамилию и имя), таблицу шифрозамен, ключевое слово, перестановочную таблицу и зашифрованное сообщение.

Задания для самостоятельной работы.

1. Дайте описание ячейки Фейстеля.
2. Назовите основные режимы DES.
3. Перечислите методы шифрования, используемые в DES-ECB.
4. Приведите схему алгоритма DES в режиме сцепления блоков шифра.
5. Назовите сферы применения разных режимов DES
6. Какова длина ключа шифра ГОСТ и как генерируются ключевые элементы.
7. Назовите основные различия между DES и ГОСТ.

Тема 9. Шифрование с открытым ключом (ПК-1)

Лекция.

Основы шифрования, алгоритм RSA, алгоритм на основе задачи об укладке ранца, вероятностное шифрование, алгоритм шифрования Эль-Гамаля, алгоритм на основе эллиптических кривых.

Лабораторные работы.

В лабораторной работе необходимо зашифровать свою фамилию с помощью следующих шифров:

- алгоритма RSA;
- алгоритма на основе задачи об укладке ранца;
- алгоритма шифрования Эль-Гамаля.

При оформлении отчета необходимо привести исходное сообщение (фамилию) и таблицы генерации ключей, шифрования и расшифрования. Для первого и третьего способов принять, что код символа соответствует его положению в алфавите, для второго – в соответствии с кодировкой Windows 1251.

Задания для самостоятельной работы.

1. В чем заключается суть и основная предпосылка появления шифрования с открытым ключом?
2. Основные требования, предъявляемые к криптосистемам с открытым ключом.
3. Перечислите типы односторонних преобразований, применяемых при асиметричном шифровании.
4. Дайте краткую характеристику алгоритма RSA.

5. В чем отличие сверхвозрастающей последовательности от обыкновенной?
6. Что означает обратное число по модулю?
7. В чем отличие вероятностного шифрования с открытым ключом от детерминированного?
8. В чем суть задачи дискретного логарифмирования?
9. Приведите уравнение эллиптической кривой в короткой форме Вейерштрасса.

Тема 10. Хеш-функции (ОПК-2)

Лекция.

Основные понятия, MD5, применение шифрования для получения хеш-образа

Лабораторные работы.

В лабораторной работе необходимо по алгоритму MD5 получить хеш-образ сообщения, состоящего из первых трех букв своей фамилии.

При оформлении отчета необходимо привести:

- теоретическую часть, включающую "Шаг основного цикла вычисления хеша", "Шаг цикла раунда" и таблицу "Раундовые функции RF";
- исходное сообщение (3 буквы фамилии) в символьном и десятичном представлениях в соответствии с кодировкой Windows 1251;
- прообраз сообщения в шестнадцатеричном представлении (512 бит), включая вспомогательные единичный и нулевые биты, а также биты, определяющие длину сообщения;
- исходные значения переменных A, B, C и D в шестнадцатеричном представлении (по 32 бита);
- для 1-го, 2-го и 16-го 32-битового блока прообраза - результаты вычислений переменных A, B, C и D в шестнадцатеричном представлении для всех раундов;
- результат итогового сложения по модулю 232 исходных значений переменных A, B, C и D со значениями этих переменных, полученных после 4-го раунда в шестнадцатеричном представлении (128 бит) до и после перестановки байт.

Задания для самостоятельной работы.

1. Дайте определение понятиям: «хеширование», «хеш-функция», «коллизия».
2. В каких целях используют хеш-функции на практике?
3. Приведите стандартную схему алгоритма генерации хеш-образа.
4. Как называется хеш-образ, полученный с применением закрытого ключа шифрования?

Тема 11. Криптографические протоколы (ОПК-2)

Лекция.

Основные сведения о криптографических протоколах, протоколы обмена ключами.

Лабораторные работы.

Не предусмотрено

Задания для самостоятельной работы.

1. Перечислите основные задачи, для решения которых используется криптография.
2. Перечислите основные отличия криптопротоколов от традиционных криптосистем.
3. Дайте определение понятию «протокол».
4. Дайте классификацию криптопротоколов в зависимости от наличия третьей стороны.
5. Перечислите основные криптопротоколы.

Тема 12. Протоколы обмена ключами (ПК-1)

Лекция.

Общие положения. Алгоритм Диффи-Хеллмана-Меркла. Протокол BB84.

Лабораторные работы.

Не предусмотрено

Задания для самостоятельной работы.

1. Дайте определение понятию «сеансовый ключ».

2. Опишите алгоритм обмена ключами Диффи-Хеллмана-Меркла.
3. В чем отличие квантового шифрования от квантового протокола обмена ключами.

Тема 13. Протоколы аутентификации (идентификации) (ПК-1)

Лекция.

Общие сведения, парольная идентификация / аутентификация, протокол идентификации / аутентификации с использованием хеш-функции, протокол идентификации / аутентификации на основе шифрования с открытым ключом, сервер аутентификации Kerberos, идентификация / аутентификация с помощью биометрических данных, идентификационные карты (ID-cards) и электронные ключи.

Лабораторные работы.

В лабораторной работе необходимо привести последовательность выполнения процедур идентификации/аутентификации с использованием следующих способов:

- на основе алгоритма RSA;
- по схеме Шнорра;
- по схеме Фейге-Фиата-Шамира.

При оформлении отчета необходимо привести таблицы генерации ключей и аутентификации. В качестве случайного числа (k или r) принять коды, соответственно, 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите.

Задания для самостоятельной работы.

1. Дайте определение понятиям: «идентификация», «аутентификация», «авторизация».
2. Что может служить в качестве аутентификатора?
3. Перечислите основные способы организации идентификации и аутентификации.
4. Перечислите достоинтства и недостатки парольной аутентификации.
5. Опишите схему протокола идентификации и аутентификации на основе алгоритма RSA.
6. В чем суть доказательства с нулевым разглашением.
7. Опишите схему протокола сервера аутентификации Kerberos.
8. Перечислите основные биометрические характеристики.

Тема 14. Протоколы электронной подписи (ПК-1)

Лекция.

Общие сведения. Протокол на базе алгоритма RSA. Алгоритм цифровой подписи ГОСТ 34.10-94. Алгоритм цифровой подписи ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012. Разновидности ЭП. Юридические основания использования ЭП.

Лабораторные работы.

В лабораторной работе необходимо привести последовательность выполнения процедур генерации и проверки ЭЦП с использованием следующих способов:

- на базе алгоритма RSA;
- по ГОСТ 34.10-94;
- по ГОСТ 34.10-2001.

При оформлении отчета необходимо привести таблицы генерации ключей, отправки сообщения с ЭЦП и получения сообщения с ЭЦП. В качестве хеш-образа исходного сообщения h(T) принять коды, соответственно, 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите.

Задания для самостоятельной работы.

1. Дайте определение понятию "электронная подпись".
2. Опишите последовательность действий участников протокола при отправке и проверке ЭП.
3. Какой порядок использования ключей (открытый; закрытый) при отправке и проверке ЭП?
4. Опишите схему протокола ЭП на основе алгоритма RSA.
5. Перечислите специальные схемы ЭП.
6. Назовите цель введения в действие Федерального закона "Об электронной подписи".

Тема 15. Протоколы контроля целостности (ПК-1)

Лекция.

Общие сведения. Проверка четности. Использование контрольных цифр. Использование контрольных сумм. Использование кодов Хэмминга. Использование ECC. Использование ЭП. Использование MAC-кодов. Комбинированные методы (на примере жестких магнитных дисков).

Лабораторные работы.

Задание 1:

В лабораторной работе необходимо определить контрольные данные с использованием следующих способов:

- битов четности. В качестве исходных данных принять битовое представление букв фамилии в соответствии с кодировкой Windows 1251;

- контрольных цифр. В качестве исходных данных принять необходимое количество цифр (за исключением контрольной) из строки, состоящей из кодов букв фамилии, имени и отчества согласно их положению в алфавите:

- по алгоритму Луна (15 цифр);

- для штрихкода по стандарту EAN-13 (12 цифр);

- для ИНН физического лица (10 цифр);

- для кодов станций на железнодорожном транспорте (5 цифр);

- контрольных сумм (CRC). В качестве исходных данных принять коды 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите для порождающего полинома - $G(x) = x4 + x1 + x0$.

- кода коррекции ошибок (ECC). В качестве исходных данных принять первые 11 битов первых двух буквы своей фамилии в соответствии с кодировкой Windows 1251. Рассчитать вектора контрольных битов и синдромов, а также паритетные биты при отсутствии ошибки, одиночной и двойной ошибке.

При оформлении отчета необходимо привести необходимые таблицы, исходные данные, расчеты и результаты.

Задание 2:

В лабораторной работе необходимо по алгоритму DES-CBC получить MAC-код сообщения, состоящего из первых восьми букв своей фамилии. Если количество букв в фамилии меньше 8 букв, то необходимо добавить недостающее количество букв из имени. В качестве ключа выбрать первые 7 букв сообщения; синхропосылки - 64-битовую строку из чередующихся 1 и 0 (10101010 ... 10).

При оформлении отчета необходимо привести:

- теоретическую часть, включающую "Схему шифрования блока", "Схему функции шифрования", "Схему выработки ключевых элементов" и "Схему алгоритма DES в режиме сцепления блоков шифра";

- шифруемое сообщение (8 букв фамилии) в символьном и битовом представлении в соответствии с кодировкой Windows 1251;

- синхропосылку в битовом представлении;

- результат сложения по модулю 2 шифруемого сообщения и синхропосылки;

- ключ (7 букв фамилии) в символьном и битовом представлении в соответствии с кодировкой Windows 1251;

- ключ в битовом представлении с учетом битов контроля четности;

- ключевые элементы ki;

- результат начальной перестановки IP;

- полублокиHi и Li, f(ki, Li), $Hi \oplus f(ki, Li)$;

- результат конечной перестановки IP-1.

Задания для самостоятельной работы.

1. Перечислите основные способы контроля целостности.

2. Что такое бит четности и как с помощью него осуществляется контроль целостности?

3. Для чего предназначена технология S.M.A.R.T.?

Тема 16. Протоколы электронных платежей (ПК-1)

Лекция.

Общие сведения, пластиковые карты, суррогатные платежные средства в Internet, расчеты пластиковыми карточками в Internet, электронные кошелки в Internet, цифровые деньги.

Лабораторные работы.

Не предусмотрено

Задания для самостоятельной работы.

1. Перечислите основные разновидности электронных платежей.
2. В чем отличие персонофицированных платежных систем от анонимных?
3. В чем отличие дебетовых карт от кредитных?
4. Для чего используется «закрывающий множитель»?

Тема 17. Протоколы голосования (ОПК-2)

Лекция.

Общие сведения, некоторые варианты реализации протоколов электронного голосования, российский опыт электронного голосования.

Лабораторные работы.

Не предусмотрено

Задания для самостоятельной работы.

1. Назовите достоинства и недостатки традиционного («бумажного») голосования.
2. Что понимается под электронным голосованием?
3. Назовите основные свойства идеального протокола голосования (по Б. Шнайеру).
4. В чем отличие УСГ от КОИБ?

Тема 18. Протоколы тайных многосторонних вычислений и разделения секрета (ОПК-2)

Лекция.

Тайные многосторонние вычисления. Протоколы разбиения и разделения секрета. Разбиение секрета с использование гаммирования. Разделение секрета по схеме Шамира (интерполяционных полиномов Лагранжа). Разделение секрета по схеме Асмута-Блума. Другие разновидности схем разделения секрета.

Лабораторные работы.

В лабораторной работе необходимо привести последовательность выполнения следующих протоколов:

- тайных многосторонних вычислений для расчета средней величины трех чисел. В качестве исходных данных принять коды 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите;
- разбиения секрета с использование гаммирования для трех участников. В качестве секрета принять первые 3 буквы фамилии, для гамм - любые трехбуквенные сочетания;
- разделения секрета по схеме Шамира для (3, 5)-пороговой схемы. В качестве секрета S принять код 1 своей фамилии согласно ее положению в алфавите;
- разделения секрета по схеме Асмута-Блума для (3, 5)-пороговой схемы. В качестве секрета S принять код 1-ой буквы своей фамилии согласно ее положению в алфавите.

При оформлении отчета необходимо привести исходные данные и таблицы, содержащие последовательность выполнения протоколов.

Задания для самостоятельной работы.

1. Для чего необходимо применение шифрования с открытым ключом в тайных многосторонних вычислениях?
2. Что означает (m, n)–пороговая схема разделения секрета.
3. Назначение интерполяционного полинома Лагранжа.
4. Сущность китайской теоремы об остатках.

Тема 19. Некоторые сведения из теорий алгоритмов и чисел (ОПК-2)

Лекция.

Сложность алгоритмов, простые числа, разложение числа на простые сомножители, нахождение начального списка простых чисел, тестирование числа на простоту, определение наибольшего общего делителя.

Лабораторные работы.

Не предусмотрено

Задания для самостоятельной работы.

1. Дайте классификацию алгоритмов в соответствии с их временной сложностью.
2. В чем суть основной теоремы арифметики?
3. Опишите метод факторизации Ферма.
4. Опишите алгоритм решета Эратосфена.
5. В чем суть теста Ферма на простоту числа.
6. Опишите алгоритм Евклида.
7. Приведите соотношение Безу.
8. Опишите расширенный алгоритм Евклида.

Тема 20. Основы криптоанализа (ПК-1)

Лекция.

Угрозы безопасности при использовании криптографии, общие сведения о криптоанализе, разновидности атак на криптосистемы.

Лабораторные работы.

Не предусмотрено

Задания для самостоятельной работы.

1. Перечислите основные угрозы безопасности при использовании криптографических систем.
2. Перечислите основные разновидности адаптивной атаки с выбором открытого текста.

Тема 21. Стеганография (ПК-1)

Лекция.

Общие сведения, классическая стеганография, компьютерная стеганография.

Лабораторные работы.

1) Для заданного файла необходимо определить скрытое сообщение и использованный метод его стеганографического сокрытия.

2) Способы форматирования символов, применяемые для секретных сообщений (символов целиком, нулей или единиц):

- цвет символов;
- цвет фона;
- размер шрифта;
- масштаб шрифта;
- межсимвольный интервал.

3) Применяемые двоичные кодировки символов:

- без кодировки;
- код Бодо (МТК-2);
- КОИ-8R;
- cp866;
- Windows 1251.

4) Варианты индивидуальных заданий (выбираются согласно номеру в журнале).

В качестве текстов использованы стихи Агния Барто, секретных сообщений – японские пословицы и поговорки.

5) Отчет по лабораторной работе должен содержать:

- фрагмент стиха, содержащий секретное сообщение:
- с подчеркиванием символов, соответствующих единицам (вместо выделения красным цветом);
- с битовыми строками;
- с символами секретного сообщения;
- вывод (например, «В файле «variant01.docx», скрыта фраза «Один бог забыл - другой поможет.» посредством использования кодировки cp866 и размера символов: для нулей – 14пт, для единиц – 14.5пт»).

Задания для самостоятельной работы.

1. Перечислите основные методы классической стеганографии и дайте им характеристику.
2. В каких целях применяется компьютерная стеганография?
3. Опишите метод сокрытия информации с пмощью потоков NTFS.
4. За счет чего достигается сокрытие информации в аудио- и видеофайлах?

Тема 22. Кодирование информации (ПК-1)

Лекция.

Общие сведения, общедоступные и секретные кодовые системы, номенклаторы.

Лабораторные работы.

В лабораторной работе необходимо представить:

- первых три числа в прямом, обратном и дополнительном двоичном коде;
- четвертое число в двоичном формате с плавающей запятой, включающем знаки порядка и мантиссы. В отчете привести исходное число в нормализованной научной записи по основанию 2 и порядок получения дробной части в двоичном виде;
- пятое число в двоичном формате одинарной точности (single) по стандарту IEEE 754.

Варианты заданий выбрать согласно таблице.

Задания для самостоятельной работы.

1. Назовите основные отличия кодовых систем от криптографических.
2. Дайте характеристику общедоступным кодовым системам.
3. Перечислите основные способы обеспечения конфиденциальности информации в секретных кодовых системах.

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

6 семестр

- посещаемость – 10 баллов
- текущий контроль – 60 баллов
- контрольные срезы – 3 среза по 10 баллов каждый
- премиальные баллы – 20 баллов

Распределение баллов по заданиям:

№ т мы	Название т	Формы	Max. ко	Методика проведения занятия и оце

1.	Основы инф	Собесе	2	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения по - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 2-1 балла – студент умеет сопоставить полученную при подготовк Если студент не владеет проблематикой практического занятия, не
2.	История	Собесе	2	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения по - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 2-1 балла – студент умеет сопоставить полученную при подготовк Если студент не владеет проблематикой практического занятия, не
3.	Основные те	**Тестирование(контрольный срез)**	10	Тестирование подразумевает 5 вопросов. За прохождение тестиро - 90 % - 10 баллов; - 65 % - 5 баллов; - 50 % - 2 балла; - менее 50 % - балл не начисляется.
		Собесе	2	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения по - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 1-2 балла – студент умеет сопоставить полученную при подготовк Если студент не владеет проблематикой практического занятия, не
4.	Шифры з	Лабора	4	Лабораторные работы выполняются по текущему разделу или тем 4 баллов – лабораторная работа выполнена в полном объёме, студе 2 балла – лабораторная работа выполнена, но имеет некоторые нет 1 балл - лабораторная работа в целом выполнена, однако в процес
		Собесе	4	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения по - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 4 балла – студент умеет сопоставить полученную при подготовке к Если студент не владеет проблематикой практического занятия, не

5.	Шифры п	Лабора	4	Лабораторные работы выполняются по текущему разделу или тем 4 баллов – лабораторная работа выполнена в полном объёме, студе 2 балла – лабораторная работа выполнена, но имеет некоторые нет 1 балл - лабораторная работа в целом выполнена, однако в процес
		Тестиров ание(кон трольны й срез)	10	Тестирование подразумевает 5 вопросов. За прохождение тестиро - 90 % - 10 баллов; - 65 % - 5 баллов; - 50 % - 2 балла; - менее 50 % - балл не начисляется.
		Собесе	3	Собеседование предполагает организацию беседы преподавателя Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения п - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 3-1 балл – студент умеет сопоставить полученную при подготовке Если студент не владеет проблематикой практического занятия, не
6.	Шифры га	Лабора	4	Лабораторные работы выполняются по текущему разделу или тем 4 баллов – лабораторная работа выполнена в полном объёме, студе 2 балла – лабораторная работа выполнена, но имеет некоторые нет 1 балл - лабораторная работа в целом выполнена, однако в процес
		Собесе	4	Собеседование предполагает организацию беседы преподавателя Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения п - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 4 балла – студент умеет сопоставить полученную при подготовке Если студент не владеет проблематикой практического занятия, не
7.	Квантовое	Собесе	4	Собеседование предполагает организацию беседы преподавателя Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения п - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 4 балла – студент умеет сопоставить полученную при подготовке Если студент не владеет проблематикой практического занятия, не
8.	Комбинир	Лабора	4	Лабораторные работы выполняются по текущему разделу или тем 4 баллов – лабораторная работа выполнена в полном объёме, студе 2 балла – лабораторная работа выполнена, но имеет некоторые нет 1 балл - лабораторная работа в целом выполнена, однако в процес

		Собесе	4	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения по - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 4 балла – студент умеет сопоставить полученную при подготовке к Если студент не владеет проблематикой практического занятия, не
9.	Шифрован	Лабора	4	Лабораторные работы выполняются по текущему разделу или тем 4 баллов – лабораторная работа выполнена в полном объёме, студе 2 балла – лабораторная работа выполнена, но имеет некоторые нет 1 балл - лабораторная работа в целом выполнена, однако в процес
		Тестиров ание(кон трольны й срез)	10	Тестирование подразумевает 5 вопросов. За прохождение тестиро - 90 % - 10 баллов; - 65 % - 5 баллов; - 50 % - 2 балла; - менее 50 % - балл не начисляется.
		Собесе	3	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения по - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 3 балла – студент умеет сопоставить полученную при подготовке к Если студент не владеет проблематикой практического занятия, не
10.	Хеш-фун	Лабора	4	Лабораторные работы выполняются по текущему разделу или тем 4 баллов – лабораторная работа выполнена в полном объёме, студе 2 балла – лабораторная работа выполнена, но имеет некоторые нет 1 балл - лабораторная работа в целом выполнена, однако в процес
		Собесе	4	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения по - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 4 балла – студент умеет сопоставить полученную при подготовке к Если студент не владеет проблематикой практического занятия, не

11.	Криптогра	Собесе	4	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталь - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения по - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 4 балла – студент умеет сопоставить полученную при подготовке к Если студент не владеет проблематикой практического занятия, не
12.	Посещаемость		10	10 баллов – стопроцентное посещение занятий студентом 7-9 баллов – посещаемость студента составляет не менее 80 % зан 4-6 баллов – посещаемость студента составляет не менее 50 % зан 1-3 балла – посещаемость студента составляет не менее 25 % заня
13.	Премиальные б		20	Дополнительные премиальные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный - постоянная активность во время практических занятий – 10 балл - полностью подготовленная к публикации статья по тематике в ра - участие с докладом во всероссийской олимпиаде по тематике изу - участие в выставке по тематике изучаемой дисциплины – 20 балл - публикация статьи по тематике изучаемой дисциплины в сборни
14.	Итого за семес		100	

7 семестр

- посещаемость – 10 баллов
- текущий контроль – 40 баллов
- контрольные срезы – 2 среза по 10 баллов каждый
- премиальные баллы – 10 баллов
- ответ на экзамене: не более 30 баллов

Распределение баллов по заданиям:

№ т мы	Название т	Формы	Мах. ко	Методика проведения занятия и оце
1.	Протоколы	Собесе	1	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталь - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения по - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 1 балл – студент умеет сопоставить полученную при подготовке к Если студент не владеет проблематикой практического занятия, не
2.	Протоколы	Лабора	3	Лабораторные работы выполняются по текущему разделу или тем 3 балла – лабораторная работа выполнена в полном объёме, студен 2 балла – лабораторная работа выполнена, но имеет некоторые нет 1 балл - лабораторная работа в целом выполнена, однако в процес

		Собесе	3	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения по - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 3 балла – студент умеет сопоставить полученную при подготовке к Если студент не владеет проблематикой практического занятия, не
3.	Протоколь	Лабора	3	Лабораторные работы выполняются по текущему разделу или тем 3 балла – лабораторная работа выполнена в полном объёме, студен 2 балла – лабораторная работа выполнена, но имеет некоторые нет 1 балл - лабораторная работа в целом выполнена, однако в процес
		Собесе	3	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения по - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 3 балла – студент умеет сопоставить полученную при подготовке к Если студент не владеет проблематикой практического занятия, не
4.	Протоколь	Лабора	3	Лабораторные работы выполняются по текущему разделу или тем 3 балла – лабораторная работа выполнена в полном объёме, студен 2 балла – лабораторная работа выполнена, но имеет некоторые нет 1 балл - лабораторная работа в целом выполнена, однако в процес
		Собесе	3	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения по - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 3 балла – студент умеет сопоставить полученную при подготовке к Если студент не владеет проблематикой практического занятия, не
5.	Протоколь	Собесе	1	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения по - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 1 балл – студент умеет сопоставить полученную при подготовке к Если студент не владеет проблематикой практического занятия, не

6.	Протокол	Собесе	1	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения по - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 1 балл – студент умеет сопоставить полученную при подготовке к Если студент не владеет проблематикой практического занятия, не
7.	Протоколы т	Лабора	3	Лабораторные работы выполняются по текущему разделу или тем 3 балла – лабораторная работа выполнена в полном объёме, студен 2 балла – лабораторная работа выполнена, но имеет некоторые нет 1 балл - лабораторная работа в целом выполнена, однако в процес
		Собесе	3	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения по - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 3 балла – студент умеет сопоставить полученную при подготовке к Если студент не владеет проблематикой практического занятия, не
8.	Некоторые	**Тестирование(контрольный срез)**	10	Тестирование подразумевает 5 вопросов. За прохождение тестиро - 90 % - 10 баллов; - 65 % - 5 баллов; - 50 % - 2 балла; - менее 50 % - балл не начисляется.
		Собесе	1	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения по - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 1 балл – студент умеет сопоставить полученную при подготовке к Если студент не владеет проблематикой практического занятия, не
9.	Основы кр	Собесе	1	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения по - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 1 балл – студент умеет сопоставить полученную при подготовке к Если студент не владеет проблематикой практического занятия, не

		Тестирование(контрольный срез)	10	Тестирование подразумевает 5 вопросов. За прохождение тестиро - 90 % - 10 баллов; - 65 % - 5 баллов; - 50 % - 2 балла; - менее 50 % - балл не начисляется.
10.	Стеганогр	Лабора	3	Лабораторные работы выполняются по текущему разделу или тем 3 балла – лабораторная работа выполнена в полном объёме, студен 2 балла – лабораторная работа выполнена, но имеет некоторые нет 1 балл - лабораторная работа в целом выполнена, однако в процес
		Собесе	3	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения п - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 3 балла – студент умеет сопоставить полученную при подготовке к Если студент не владеет проблематикой практического занятия, не
11.	Кодирован	Лабора	3	Лабораторные работы выполняются по текущему разделу или тем 3 балла – лабораторная работа выполнена в полном объёме, студен 2 балла – лабораторная работа выполнена, но имеет некоторые нет 1 балл - лабораторная работа в целом выполнена, однако в процес
		Собесе	2	Собеседование предполагает организацию беседы преподавателя с Устный опрос может применяться в различных формах: фронталы - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения п - своевременность и эффективность использования наглядных пос - использование дополнительного материала; - рациональность использования времени, отведенного на задание 2 балла – студент умеет сопоставить полученную при подготовке к Если студент не владеет проблематикой практического занятия, не
12.	Посещаемость		10	10 баллов – стопроцентное посещение занятий студентом 7-9 баллов – посещаемость студента составляет не менее 80 % зан 4-6 баллов – посещаемость студента составляет не менее 50 % зан 1-3 балла – посещаемость студента составляет не менее 25 % заня
13.	Премиальные б		10	Дополнительные премиальные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный - постоянная активность во время практических занятий – 10 балл - полностью подготовленная к публикации статья по тематике в ра - участие с докладом во всероссийской олимпиаде по тематике изу - участие в выставке по тематике изучаемой дисциплины – 20 балл - публикация статьи по тематике изучаемой дисциплины в сборни
14.	Ответ на экзам		30	Оценка «удовлетворительно»- студент имеет достаточный минима Оценка «хорошо» – ▪достаточно полные и систематизированные з научных и профессиональных задач; усвоение основной и дополн - Оценка «отлично» – систематизированные и гл и полные знани дисциплины, а также по основным вопросам, выходящим за преде глубокое усвоение основной и дополнительной литературы, реком
15.	Итого за семес		100	

Итоговая оценка по экзамену выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система
85 - 100 баллов	Отлично
70 - 84 баллов	Хорошо
50 - 69 баллов	Удовлетворительно
Менее 50	Неудовлетворительно

Распределение баллов по курсовой работе:

- представление содержательной части – не более 55 баллов,
- оформление и информационное сопровождение – не более 20 баллов,
- защита курсовой работы – не более 25 баллов.

Распределение баллов по видам учебной работы и методика начисления баллов:

№	Вид учебной работы	Max. кол-во баллов	Методика начисления баллов
1.	Представление содержатель	55	41-55 баллов – содержание работы соответствует выбранному нап раскрыта глубоко и всесторонне, материал изложен логично; теоре 21-40 баллов – содержание работы в целом соответствует выбранн соответствуют поставленным задачам; 1-20 баллов – имеет место определенное несоответствие содержан носят формальный бездоказательный характер
2.	Оформление и информацио	20	16-20 баллов – широко представлена библиография по теме работ 8-15 баллов – приложения, используемые в исследовании, составл 1-7 баллов – в работе не полностью использована необходимая дл
3.	Защита курсовой работы	25	19-25 баллов – защита отличается полнотой раскрытия темы и пре 10-18 баллов – структура и регламент выступления в целом соблю 1-9 баллов – студент демонстрирует невысокое качество устного д
	ИТОГО:	**100**	

Итоговая оценка по курсовой работе выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система
85 - 100 баллов	Отлично
70 - 84 баллов	Хорошо
50 - 69 баллов	Удовлетворительно
Менее 50	Неудовлетворительно

4.2 Типовые оценочные средства текущего контроля

Лабораторная работа

Тема 4. Шифры замены

шифра Цезаря;
- лозунгового шифра;

- полибианского квадрата;
- шифрующей системы Трисемуса;
- шифра Playfair;
- системы омофонов (допускается для каждой буквы алфавита привести всего по две шифрозамены, т.е. принять, что все буквы имеют одинаковую вероятность появления в текстах);
- шифра Виженера.

При оформлении отчета необходимо привести исходное сообщение (фамилию), таблицу шифрозамен, ключ (если таблица шифрозамен не является ключом) и зашифрованное сообщение.

Тема 5. Шифры перестановки

- простой одинарной перестановки;
- блочной одинарной перестановки;
- табличной маршрутной перестановки;
- вертикальной перестановки;
- поворотной решетки;
- магический квадрат (размер квадрата - 4x4);
- двойной перестановки.

Тема 6. Шифры гаммирования

В лабораторной работе необходимо зашифровать свою фамилию с помощью шифров гаммирования по модулю N и модулю 2.

При оформлении отчета необходимо привести исходное сообщение (фамилию), гамму и таблицы зашифрования/дешифрования.

Тема 8. Комбинированные шифры

В лабораторной работе необходимо зашифровать свою фамилию и имя с помощью шифра ADFGVX.

При оформлении отчета необходимо привести исходное сообщение (фамилию и имя), таблицу шифрозамен, ключевое слово, перестановочную таблицу и зашифрованное сообщение.

Тема 9. Шифрование с открытым ключом

В лабораторной работе необходимо зашифровать свою фамилию с помощью следующих шифров:

- алгоритма RSA;
- алгоритма на основе задачи об укладке ранца;
- алгоритма шифрования Эль-Гамаля.

При оформлении отчета необходимо привести исходное сообщение (фамилию) и таблицы генерации ключей, шифрования и расшифрования. Для первого и третьего способов принять, что код символа соответствует его положению в алфавите, для второго – в соответствии с кодировкой Windows 1251.

Тема 10. Хеш-функции

В лабораторной работе необходимо по алгоритму MD5 получить хеш-образ сообщения, состоящего из первых трех букв своей фамилии.

При оформлении отчета необходимо привести:

- теоретическую часть, включающую "Шаг основного цикла вычисления хеша", "Шаг цикла раунда" и таблицу "Раундовые функции RF";
- исходное сообщение (3 буквы фамилии) в символьном и десятичном представлениях в соответствии с кодировкой Windows 1251;
- прообраз сообщения в шестнадцатеричном представлении (512 бит), включая вспомогательные единичный и нулевые биты, а также биты, определяющие длину сообщения;
- исходные значения переменных A, B, C и D в шестнадцатеричном представлении (по 32 бита);

- для 1-го, 2-го и 16-го 32-битового блока прообраза - результаты вычислений переменных A, B, C и D в шестнадцатеричном представлении для всех раундов;

- результат итогового сложения по модулю 232 исходных значений переменных A, B, C и D со значениями этих переменных, полученных после 4-го раунда в шестнадцатеричном представлении (128 бит) до и после перестановки байт.

Тема 13. Протоколы аутентификации (идентификации)

В лабораторной работе необходимо привести последовательность выполнения процедур идентификации/аутентификации с использованием следующих способов:

- на основе алгоритма RSA;

- по схеме Шнорра;

- по схеме Фейге-Фиата-Шамира.

При оформлении отчета необходимо привести таблицы генерации ключей и аутентификации. В качестве случайного числа (k или r) принять коды, соответственно, 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите.

Тема 14. Протоколы электронной подписи

В лабораторной работе необходимо привести последовательность выполнения процедур генерации и проверки ЭЦП с использованием следующих способов:

- на базе алгоритма RSA;

- по ГОСТ 34.10-94;

- по ГОСТ 34.10-2001.

При оформлении отчета необходимо привести таблицы генерации ключей, отправки сообщения с ЭЦП и получения сообщения с ЭЦП. В качестве хеш-образа исходного сообщения h(T) принять коды, соответственно, 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите.

Тема 15. Протоколы контроля целостности

Задание 1:

В лабораторной работе необходимо определить контрольные данные с использованием следующих способов:

- битов четности. В качестве исходных данных принять битовое представление букв фамилии в соответствии с кодировкой Windows 1251;

- контрольных цифр. В качестве исходных данных принять необходимое количество цифр (за исключением контрольной) из строки, состоящей из кодов букв фамилии, имени и отчества согласно их положению в алфавите:

- по алгоритму Луна (15 цифр);

- для штрихкода по стандарту EAN-13 (12 цифр);

- для ИНН физического лица (10 цифр);

- для кодов станций на железнодорожном транспорте (5 цифр);

- контрольных сумм (CRC). В качестве исходных данных принять коды 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите для порождающего полинома - G(x) = x4 + x1 + x0.

- кода коррекции ошибок (ECC). В качестве исходных данных принять первые 11 битов первых двух буквы своей фамилии в соответствии с кодировкой Windows 1251. Рассчитать вектора контрольных битов и синдромов, а также паритетные биты при отсутствии ошибки, одиночной и двойной ошибке.

При оформлении отчета необходимо привести необходимые таблицы, исходные данные, расчеты и результаты.

Задание 2:

В лабораторной работе необходимо по алгоритму DES-CBC получить MAC-код сообщения, состоящего из первых восьми букв своей фамилии. Если количество букв в фамилии меньше 8 букв, то необходимо добавить недостающее количество букв из имени. В качестве ключа выбрать первые 7 букв сообщения; синхропосылки - 64-битовую строку из чередующихся 1 и 0 (10101010 ... 10).

При оформлении отчета необходимо привести:

- теоретическую часть, включающую "Схему шифрования блока", "Схему функции шифрования", "Схему выработки ключевых элементов" и "Схему алгоритма DES в режиме сцепления блоков шифра";
- шифруемое сообщение (8 букв фамилии) в символьном и битовом представлении в соответствии с кодировкой Windows 1251;
- синхропосылку в битовом представлении;
- результат сложения по модулю 2 шифруемого сообщения и синхропосылки;
- ключ (7 букв фамилии) в символьном и битовом представлении в соответствии с кодировкой Windows 1251;
- ключ в битовом представлении с учетом битов контроля четности;
- ключевые элементы ki;
- результат начальной перестановки IP;
- полублокиHi и Li, f(ki, Li), Hi⊕ f(ki, Li);
- результат конечной перестановки IP-1.

Тема 18. Протоколы тайных многосторонних вычислений и разделения секрета

В лабораторной работе необходимо привести последовательность выполнения следующих протоколов:

- тайных многосторонних вычислений для расчета средней величины трех чисел. В качестве исходных данных принять коды 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите;
- разбиения секрета с использование гаммирования для трех участников. В качестве секрета принять первые 3 буквы фамилии, для гамм - любые трехбуквенные сочетания;
- разделения секрета по схеме Шамира для (3, 5)-пороговой схемы. В качестве секрета S принять код 1-ой буквы своей фамилии согласно ее положению в алфавите;
- разделения секрета по схеме Асмута-Блума для (3, 5)-пороговой схемы. В качестве секрета S принять код 1-ой буквы своей фамилии согласно ее положению в алфавите.

При оформлении отчета необходимо привести исходные данные и таблицы, содержащие последовательность выполнения протоколов.

Тема 21. Стеганография

1) Для заданного файла необходимо определить скрытое сообщение и использованный метод его стеганографического сокрытия.

2) Способы форматирования символов, применяемые для секретных сообщений (символов целиком, нулей или единиц):

- цвет символов;
- цвет фона;
- размер шрифта;
- масштаб шрифта;
- межсимвольный интервал.

3) Применяемые двоичные кодировки символов:

- без кодировки;
- код Бодо (МТК-2);
- КОИ-8R;
- ср866;
- Windows 1251.

4) Варианты индивидуальных заданий (выбираются согласно номеру в журнале).

В качестве текстов использованы стихи Агния Барто, секретных сообщений – японские пословицы и поговорки.

5) Отчет по лабораторной работе должен содержать:

- фрагмент стиха, содержащий секретное сообщение:
- с подчеркиванием символов, соответствующих единицам (вместо выделения красным цветом);
- с битовыми строками;
- с символами секретного сообщения;
- вывод (например, «В файле «variant01.docx», скрыта фраза «Один бог забыл - другой поможет.» посредством использования кодировки cp866 и размера символов: для нулей – 14пт, для единиц – 14.5пт»).

Тема 22. Кодирование информации

В лабораторной работе необходимо представить:

- первых три числа в прямом, обратном и дополнительном двоичном коде;
- четвертое число в двоичном формате с плавающей запятой, включающем знаки порядка и мантиссы. В отчете привести исходное число в нормализованной научной записи по основанию 2 и порядок получения дробной части в двоичном виде;
- пятое число в двоичном формате одинарной точности (single) по стандарту IEEE 754.

Варианты заданий выбрать согласно таблице.

Собеседование

Тема 1. Основы информационной безопасности и защиты информации

1. Дайте определение понятиям: «информация», «информационная безопасность», «защита информации», «информационная угроза».
2. Дайте характеристику основным составляющим информационной безопасности.
3. Перечислите основные объекты защиты.
4. Дайте характеристику понятиям «государственная тайна», «конфиденциальная информация» и «персональные данные».
5. Дайте характеристику средствам защиты информации.

Тема 2. История криптографии

1. Перечислите способы тайной передачи информации на расстоянии.
2. Назовите основные этапы развития криптографии.

Тема 3. Основные термины и определения. Классификация шифров

1. Дайте определение понятиям «шифр», «ключ», «дешифрование».
2. Перечислите основные требования, предъявляемые к криптосистемам.
3. Дайте классификацию криптосистем по алгоритму шифрования.
4. Дайте классификацию криптосистем по стойкости шифра.

Тема 4. Шифры замены

1. В чем заключается основная идея криптографических преобразований шифров замены?
2. Перечислите основные разновидности шифров замены.
3. Дайте характеристику разновидностям шифров замены.
4. Назовите основной недостаток шифра однозначной замены.

Тема 5. Шифры перестановки

1. В чем заключается основная идея криптографических преобразований шифров перестановки?
2. Перечислите основные разновидности шифров перестановки.

3. Дайте характеристику разновидностям шифров перестановки.

Тема 6. Шифры гаммирования

1. В чем заключается основная идея криптографических преобразований аддитивных шифров?
2. Назовите основные характеристики гаммы.
3. При каких условиях применения гаммы аддитивный шифр можно считать совершенным.
4. Дайте характеристику программным способам генерации гаммы (алгоритм RANDU и BBS).
5. Что такое паритетный бит?
6. Опишите схемы шифрования с использованием синхронных и самосинхронизирующихся потоковых шифров.

Тема 7. Квантовое шифрование

1. Дайте определение понятиям «квант» и «фотон».
2. В чем заключается природа корпускулярно-волнового дуализма фотона?
3. В чем суть шифрования с помощью фотонов?

Тема 8. Комбинированные шифры

1. Дайте описание ячейки Фейстеля.
2. Назовите основные режимы DES.
3. Перечислите методы шифрования, используемые в DES-ECB.
4. Приведите схему алгоритма DES в режиме сцепления блоков шифра.
5. Назовите сферы применения разных режимов DES
6. Какова длина ключа шифра ГОСТ и как генерируются ключевые элементы.
7. Назовите основные различия между DES и ГОСТ.

Тема 9. Шифрование с открытым ключом

1. В чем заключается суть и основная предпосылка появления шифрования с открытым ключом?
2. Основные требования, предъявляемые к криптосистемам с открытым ключом.
3. Перечислите типы односторонних преобразований, применяемых при асиметричном шифровании.
4. Дайте краткую характеристику алгоритма RSA.
5. В чем отличие сверхвозрастающей последовательности от обыкновенной?
6. Что означает обратное число по модулю?
7. В чем отличие вероятностного шифрования с открытым ключом от детерминированного?
8. В чем суть задачи дискретного логарифмирования?
9. Приведите уравнение эллиптической кривой в короткой форме Вейерштрасса.

Тема 10. Хеш-функции

1. Дайте определение понятиям: «хеширование», «хеш-функция», «коллизия».
2. В каких целях используют хеш-функции на практике?
3. Приведите стандартную схему алгоритма генерации хеш-образа.
4. Как называется хеш-образ, полученный с применением закрытого ключа шифрования?

Тема 11. Криптографические протоколы

1. Перечислите основные задачи, для решения которых используется криптография.
2. Перечислите основные отличия криптопротоколов от традиционных криптосистем.
3. Дайте определение понятию «протокол».

4. Дайте классификацию криптопротоколов в зависимости от наличия третьей стороны.
5. Перечислите основные криптопротоколы.

Тема 12. Протоколы обмена ключами

1. Дайте определение понятию «сеансовый ключ».
2. Опишите алгоритм обмена ключами Диффи-Хеллмана-Меркла.
3. В чем отличие квантового шифрования от квантового протокола обмена ключами.

Тема 13. Протоколы аутентификации (идентификации)

1. Дайте определение понятиям: «идентификация», «аутентификация», «авторизация».
2. Что может служить в качестве аутентификатора?
3. Перечислите основные способы организации идентификации и аутентификации.
4. Перечислите достоинтства и недостатки парольной аутентификации.
5. Опишите схему протокола идентификации и аутентификации на основе алгоритма RSA.
6. В чем суть доказательства с нулевым разглашением.
7. Опишите схему протокола сервера аутентификации Kerberos.
8. Перечислите основные биометрические характеристики.

Тема 14. Протоколы электронной подписи

1. Дайте определение понятию "электронная подпись".
2. Опишите последовательность действий участников протокола при отправке и проверке ЭП.
3. Какой порядок использования ключей (открытый; закрытый) при отправке и проверке ЭП?
4. Опишите схему протокола ЭП на основе алгоритма RSA.
5. Перечислите специальные схемы ЭП.
6. Назовите цель введения в действие Федерального закона "Об электронной подписи".

Тема 15. Протоколы контроля целостности

1. Перечислите основные способы контроля целостности.
2. Что такое бит четности и как с помощью него осуществляется контроль целостности?
3. Для чего предназначена технология S.M.A.R.T.?

Тема 16. Протоколы электронных платежей

1. Перечислите основные разновидности электронных платежей.
2. В чем отличие персонофицированных платежных систем от анонимных?
3. В чем отличие дебетовых карт от кредитных?
4. Для чего используется «закрывающий множитель»?

-

Тема 17. Протоколы голосования

1. Назовите достоинства и недостатки традиционного («бумажного») голосования.
2. Что понимается под электронным голосованием?
3. Назовите основные свойства идеального протокола голосования (по Б. Шнайеру).
4. В чем отличие УСГ от КОИБ?

Тема 18. Протоколы тайных многосторонних вычислений и разделения секрета

1. Для чего необходимо применение шифрования с открытым ключом в тайных многосторонних вычислениях?
2. Что означает (m, n)–пороговая схема разделения секрета.

3. Назначение интерполяционного полинома Лагранжа.
4. Сущность китайской теоремы об остатках.

Тема 19. Некоторые сведения из теорий алгоритмов и чисел

1. Дайте классификацию алгоритмов в соответствии с их временной сложностью.
2. В чем суть основной теоремы арифметики?
3. Опишите метод факторизации Ферма.
4. Опишите алгоритм решета Эратосфена.
5. В чем суть теста Ферма на простоту числа.
6. Опишите алгоритм Евклида.
7. Приведите соотношение Безу.
8. Опишите расширенный алгоритм Евклида.

Тема 20. Основы криптоанализа

1. Перечислите основные угрозы безопасности при использовании криптографических систем.
2. Перечислите основные разновидности адаптивной атаки с выбором открытого текста.

Тема 21. Стеганография

1. Перечислите основные методы классической стеганографии и дайте им характеристику.
2. В каких целях применяется компьютерная стеганография?
3. Опишите метод сокрытия информации с пмощью потоков NTFS.
4. За счет чего достигается сокрытие информации в аудио- и видеофайлах?

Тема 22. Кодирование информации

1. Назовите основные отличия кодовых систем от криптографических.
2. Дайте характеристику общедоступным кодовым системам.
3. Перечислите основные способы обеспечения конфиденциальности информации в секретных кодовых системах.

Тестирование

Тема 3. Основные термины и определения. Классификация шифров

1. Что является целью криптоанализа?

A. Определение стойкости алгоритма
B. Увеличение количества функций замещения в криптографическом алгоритме
C. Уменьшение количества функций подстановкм в криптографическом алгоритме
D. Определение использованных перестановок

2. Частота применения брутфорс-атак возросла, поскольку:

A. Возросло используемое в алгоритмах количество перестановок и земещений
B. Алгоритмы по мере повышения стойкости становились менее сложными и более подверженными атакам
C. Мощность и скорость работы процессоров возросла
D. Длина ключа со временем уменьшилась

3. Что из перечисленного ниже не является свойством или характеристикой односторонней функции хэширования?

A. Она преобразует сообщение произвольной длины в значение фиксированной длины

B. Имея значение дайджеста сообщения, невозможно получить само сообщение

C. Получение одинакового дайджеста из двух различных сообщений невозможно, либо случается крайне редко

D. Она преобразует сообщение фиксированной длины в значение переменной длины

4. Что может указывать на изменение сообщения?

A. Изменился открытый ключ

B. Изменился закрытый ключ

C. Изменился дайджест сообщения

D. Сообщение было правильно зашифровано

5. Какой из перечисленных ниже алгоритмов является алгоритмом американского правительства, предназначенным для создания безопасных дайджестов сообщений?

A. Data Encryption Algorithm

B. Digital Signature Standard

C. Secure Hash Algorithm

D. Data Signature Algorithm

Тема 5. Шифры перестановки

1. Что из перечисленного ниже лучше всего описывает отличия между HMAC и CBC-MAC?

A. HMAC создает дайджест сообщения и применяется для контроля целостности; CBC-MAC используется для шифрования блоков данных с целью обеспечения конфиденциальности

B. HMAC использует симметричный ключ и алгоритм хэширования; CBC-MAC использует первый блок в качестве контрольной суммы

C. HMAC обеспечивает контроль целостности и аутентификацию источника данных; CBC-MAC использует блочный шифр в процессе создания MAC

D. HMAC зашифровывает сообщение на симметричном ключе, а затем передает результат в алгоритм хэширования; CBC-MAC зашифровывает все сообщение целиком

2. В чем преимущество RSA над DSA?

A. Он может обеспечить функциональность цифровой подписи и шифрования

B. Он использует меньше ресурсов и выполняет шифрование быстрее, поскольку использует симметричные ключи

C. Это блочный шифр и он лучше поточного

D. Он использует одноразовые шифровальные блокноты

3. Многие страны ограничивают использование и экспорт криптографических систем. Зачем они это делают?

A. Без ограничений может возникнуть большое число проблем совместимости при попытке использовать различные алгоритмы в различных программах

B. Эти системы могут использоваться некоторыми странами против их местного населения

C. Криминальные элементы могут использовать шифрование, чтобы избежать обнаружения и преследования

D. Законодательство сильно отстает, а создание новых типов шифрования еще больше усиливает эту проблему

4. Что используется для создания цифровой подписи?

A. Закрытый ключ получателя

B. Открытый ключ отправителя

C. Закрытый ключ отправителя
D. Открытый ключ получателя

5. Что из перечисленного ниже лучше всего описывает цифровую подпись?
A. Это метод переноса собственноручной подписи на электронный документ
B. Это метод шифрования конфиденциальной информации
C. Это метод, обеспечивающий электронную подпись и шифрование
D. Это метод, позволяющий получателю сообщения проверить его источник и убедиться в целостности сообщения

Тема 9. Шифрование с открытым ключом

1. Какова эффективная длина ключа в DES?
A. 56
B. 64
C. 32
D. 16

2. По какой причине удостоверяющий центр отзывает сертификат?
A. Если открытый ключ пользователя скомпрометирован
B. Если пользователь переходит на использование модели PEM, которая использует сеть доверия
C. Если закрытый ключ пользователя скомпрометирован
D. Если пользователь переходит работать в другой офис

3. Что из перечисленного ниже лучше всего описывает удостоверяющий центр?
A. Организация, которая выпускает закрытые ключи и соответствующие алгоритмы
B. Организация, которая проверяет процессы шифрования
C. Организация, которая проверяет ключи шифрования
D. Организация, которая выпускает сертификаты

4. Как расшифровывается аббревиатура DEA?
A. Data Encoding Algorithm
B. Data Encoding Application
C. Data Encryption Algorithm
D. Digital Encryption Algorithm
5. Кто участвовал в разработке первого алгоритма с открытыми ключами?
A. Ади Шамир
B. Росс Андерсон
C. Брюс Шнайер
D. Мартин Хеллман

Тема 19. Некоторые сведения из теорий алгоритмов и чисел

1. Какой процесс обычно выполняется после создания сеансового ключа DES?
A. Подписание ключа
B. Передача ключа на хранение третьей стороне (key escrow)
C. Кластеризация ключа
D. Обмен ключом

2. Сколько циклов перестановки и замещения выполняет DES?
A. 16

B. 32
C. 64
D. 56

3. Что из перечисленного ниже является правильным утверждением в отношении шифрования данных, выполняемого с целью их защиты?
A. Оно обеспечивает проверку целостности и правильности данных
B. Оно требует внимательного отношения к процессу управления ключами
C. Оно не требует большого количества системных ресурсов
D. Оно требует передачи ключа на хранение третьей стороне (escrowed)

4. Как называется ситуация, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст?
A. Коллизия
B. Хэширование
C. MAC
D. Кластеризация ключей

5. Что из перечисленного ниже является определением фактора трудозатрат для алгоритма?
A. Время зашифрования и расшифрования открытого текста
B. Время, которое займет взлом шифрования
C. Время, которое занимает выполнение 16 циклов преобразований
D. Время, которое занимает выполнение функций подстановки

Тема 20. Основы криптоанализа

1. Что является основной целью использования одностороннего хэширования пароля пользователя?
A. Это снижает требуемый объем дискового пространства для хранения пароля пользователя
B. Это предотвращает ознакомление кого-либо с открытым текстом пароля
C. Это позволяет избежать избыточной обработки, требуемой асимметричным алгоритмом
D. Это предотвращает атаки повтора (replay attack)

2. Какой из перечисленных ниже алгоритмов основан на сложности разложения больших чисел на два исходных простых сомножителя?
A. ECC
B. RSA
C. DES
D. Диффи-Хеллман

3. Что из перечисленного ниже описывает разницу между алгоритмами DES и RSA?
A. DES – это симметричный алгоритм, а RSA – асимметричный
B. DES – это асимметричный алгоритм, а RSA – симметричный
C. Они оба являются алгоритмами хэширования, но RSA генерирует 160-битные значения хэша
D. DES генерирует открытый и закрытый ключи, а RSA выполняет шифрование сообщений

4. Какой из перечисленных ниже алгоритмов использует симметричный ключ и алгоритм хэширования?
A. HMAC
B. 3DES
C. ISAKMP-OAKLEY

D. RSA

5. Генерация ключей, для которой используются случайные значения, называется Функцией генерации ключей (KDF). Какие значения обычно не используются при этом в процессе генерации ключей?

A. Хэши
B. Асимметричные значения
C. Соль
D. Пароли

4.3 Промежуточная аттестация по дисциплине проводится в форме зачета, экзамена

Типовые вопросы зачета (ОПК-2, ПК-1)

1. Понятия "информационная безопасность" и "защита информации". Основные составляющие информационной безопасности.
2. Объекты защиты. Категории и носители информации.
3. Средства защиты информации.
4. Криптография. Основные термины и определения.
5. Классификация криптографических систем.
6. Шифры замены. Основные методы шифрования.
7. Шифры перестановки. Основные методы шифрования.
8. Шифры гаммирования. Основные методы шифрования.
9. Шифры гаммирования. Способы генерации гаммы. Генераторы гамм.
10. Схема режима шифрования DES-ECB.
11. Схема режима шифрования DES-CBC.
12. Схема режима шифрования DES-CPB и DES-OFB.
13. Тройной DES. Сферы применения различных режимов DES.
14. Схема режима шифрования простой замены ГОСТ 28147-89.
15. Шифрование с открытым ключом. Основные понятия.
16. Алгоритм шифрования RSA.
17. Алгоритм шифрования Эль-Гамаля.
18. Алгоритм шифрования на основе задачи об укладке ранца.
19. Эллиптические кривые. Основные понятия. Сложение и умножение точки.
20. Алгоритм шифрования на основе эллиптических кривых.
21. Хэш-функции. Основные понятия и разновидности.
22. Хэш-функция. MD5.
23. Криптографические протоколы. Основные понятия.

Типовые задания для зачета (ОПК-2, ПК-1)

Не предусмотрены

Типовые вопросы экзамена (ОПК-2, ПК-1)

1. Протоколы обмена ключами.
2. Протоколы аутентификации. Разновидности и краткая характеристика.
3. Парольная идентификация/аутентификация.
4. Протокол идентификации/аутентификации на основе шифрования с открытым ключом.
5. Сервер аутентификации Kerberos.
6. Идентификация/аутентификация с помощью биометрических данных.

7. Идентификационные карты (ID-cards) и электронные ключи.
8. Электронная цифровая подпись. Общие сведения и разновидности ЭЦП.
9. ЭЦП на базе алгоритма RSA.
10. Алгоритм цифровой подписи ГОСТ 34.10-94.
11. Алгоритм цифровой подписи ГОСТ 34.10-2001.
12. Протоколы контроля целостности.
13. Электронные платежи.
14. Классическое ("бумажное") голосования.
15. Российский опыт электронного голосования.
16. Протокол разделения секрета.
17. Протокол подбрасывания монеты по телефону.
18. Тайные многосторонние вычисления.
19. Сложность алгоритмов.
20. Простые числа.
21. Разложение числа на простые сомножители.
22. Нахождение начального списка простых чисел.
23. Тестирование числа на простоту.
24. Определение наибольшего общего делителя.
25. Основные сведения о криптоанализе и атаки на криптосистемы.
26. Классическая стеганография.
27. Компьютерная стеганография.
28. Общие сведения о кодировании.
29. Общедоступные кодовые системы.
30. Секретные кодовые системы.

Типовые задания для экзамена (ОПК-2, ПК-1)

Зашифровать свою фамилию с помощью шифров:
- шифра масонов;
- биграмного шифра Порты;
- шифра Хилла;
- вариантного шифра;
- шифра Тени;
- совмещенного шифра.

Зашифровать свою фамилию и имя с помощью шифров:
- шифра «Перекресток»;
- шифры с использованием треугольника.

Типовые темы курсовых работ (ОПК-2, ПК-1)

1 Программная реализация шифров замены.
2 Программная реализация шифров перестановки.
3 Программная реализация шифра Плейфера.
4 Программная реализация шифра Хилла.
5 Разработка шифра, основанного на композиции шифра замены и перестановки, с оценкой его криптостойкости.
6 Анализ криптостойкости блочных криптосистем (ГОСТ 28147-89, DES, IDEA, AES).
7 Алгоритм электронной цифровой подписи на основе решения системы сравнений.
8 Анализ методов сокращения длины электронной цифровой подписи.
9 Алгоритмы коллективной электронной цифровой подписи.
10 Алгоритмы композиционной электронной цифровой подписи.

11 Сравнительный анализ современных программных, программно-аппаратных и аппаратных средств криптографической защиты информации.
12 Разработка схемы криптографического генератора, основанного на комбинировании LFSR-генераторов, с оценкой его качества.
13 Разработка схемы криптографического генератора, основанного на комбинировании конгруэнтных генераторов, с оценкой его качества.
14 Оценка качества криптографических генераторов, основанных на алгоритмах Фибоначчи.
15 Алгоритмы слепой электронной цифровой подписи.
16 Сравнительный анализ алгоритмов формирования хэш-функций.
17 Сравнительный анализ современных криптосистем с открытым ключом.
18 Сравнительный анализ криптографических протоколов распределения ключей.
19 Разработка системы аутентификации пользователей сети передачи данных о движении

4.4. Шкала оценивания промежуточной аттестации

Зачет

Оценка	Компете	Дескрипторы (уровни) – основные признак
«зачтено» (50 - 100 балл	ОПК-2	Студент показывает достаточный уровень профессиональных знаний, свободно оперирует понятиями, методами оценки принятия решений, имеет представление о междисциплинарных связях, увязывает знания, полученные при изучении различных дисциплин, умеет анализировать практические ситуации, но допускает некоторые погрешности. Ответ построен логично, материал излагается хорошим языком, привлекается информативный и иллюстрированный материал, но при ответе допускает некоторые погрешности. Вопросы, задаваемые преподавателем, не вызывают существенных затруднений
	ПК-1	Демонстрирует высокий уровень работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации. Способен использовать все методы криптографической защиты информации. Умеет применять практические знания на практике в области криптографических средств защиты информации.
«не зачтено» (0 - 49 баллов	ОПК-2	Студент показывает слабый уровень профессиональных знаний, затрудняется при анализе практических ситуаций. Не может привести примеры из реальной практики. Неуверенно и логически непоследовательно излагает материал. Неправильно отвечает на поставленные вопросы или затрудняется с ответом
	ПК-1	Демонстрирует слабый уровень работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации. Неспособен использовать все методы криптографической защиты информации. Не знает методы архивирования информации. Не владеет навыками правильного использования различных видов информации.¶

Экзамен

Оценка	Компете	Дескрипторы (уровни) – основные признак

«отлично» (85 - 100 балл	ОПК-2	Студент показывает достаточный уровень профессиональных знаний, свободно оперирует понятиями, методами оценки принятия решений, имеет представление о междисциплинарных связях, увязывает знания, полученные при изучении различных дисциплин, умеет анализировать практические ситуации, но допускает некоторые погрешности. Ответ построен логично, материал излагается хорошим языком, привлекается информативный и иллюстрированный материал, но при ответе допускает некоторые погрешности. Вопросы, задаваемые преподавателем, не вызывают существенных затруднений
	ПК-1	Демонстрирует высокий уровень работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации. Способен использовать все методы криптографической защиты информации. Умеет применять практические знания на практике в области криптографических средств защиты информации.
«хорошо» (70 - 84 балло	ОПК-2	Показывает твердые знания дисциплины в соответствии с программой курсового экзамена; самостоятельно и последовательно излагает материал
	ПК-1	Хорошо выполняет работу по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации; Демонстрирует достаточный уровень для применения практических знаний на практике в области криптографических средств защиты информации.
«удовлетворите (50 - 69 балло	ОПК-2	В основном показывает знания дисциплины в соответствии с программой курсового экзамена; допускает некоторые ошибки в изложении материала
	ПК-1	Демонстрирует не достаточный уровень работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации. Способен выявлять сущность проблем, возникающих в ходе профессиональной деятельности. Владеет недостаточными навыками использования различных видов информации.
«неудовлетвори (менее 50 бал.	ОПК-2	Студент показывает слабый уровень профессиональных знаний, затрудняется при анализе практических ситуаций. Не может привести примеры из реальной практики. Неуверенно и логически непоследовательно излагает материал. Неправильно отвечает на поставленные вопросы или затрудняется с ответом
	ПК-1	Демонстрирует слабый уровень работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации. Неспособен использовать все методы криптографической защиты информации. Не знает методы архивирования информации. Не владеет навыками правильного использования различных видов информации.¶

5. Методические указания для обучающихся по освоению дисциплины (модуля)

5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;

- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы:

- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.

- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентаци, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);

- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);

- готовить аннотации (краткое обобщение основных вопросов работы);

- создавать конспекты (развернутые тезисы).

5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели. ссылки на ресурсы. соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности. соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы:
- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература:

1. Тамб гос. ун-т им. Г.Р. Державина, Ин-т математики, физики и информатики Техническая защита информации : учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

2. Лопатин Д.В., Калинина Ю.В. Безопасные информационные технологии : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

3. Лопатин Д. В. Программно-аппаратная защита информации : электрон. учеб. пособие. - Тамбов: [Б. и.], 2014. - 1 электрон. опт. диск (CD-ROM)

4. Лопатин Д. В. Технология информационной безопасности и методология защиты информации : электрон. учеб. пособие. - Тамбов: [Б. и.], 2014. - 1 электрон. опт. диск (CD-ROM)

5. Лопатин Д. В. Защита от вредоносных программ : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

6. Лопатин Д.В., Чиркин Е.С. Защита электронного документооборота в компьютерной системе : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

7. Лопатин Д.В., Чиркин Е.С. Защита информационных процессов в автоматизированных системах : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

6.2 Дополнительная литература:

1. Бехроуз, А. Криптография и безопасность сетей : учебное пособие. - 2020-11-14; Криптография и безопасность сетей. - Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. - 782 c. - Текст : электронный // IPR BOOKS [сайт]. - URL: http://www.iprbookshop.ru/72337.html

2. Аграновский, А. В., Хади, Р. А. Практическая криптография: алгоритмы и их программирование. - 2021-05-25; Практическая криптография: алгоритмы и их программирование. - Москва: СОЛОН-Пресс, 2016. - 256 c. - Текст : электронный // IPR BOOKS [сайт]. - URL: http://www.iprbookshop.ru/90248.html

3. Грибунин, В. Г., Мартынов, А. П., Николаев, Д. Б., Фомченко, В. Н. Криптография и безопасность цифровых систем : учебное пособие. - Весь срок охраны авторского права; Криптография и безопасность цифровых систем. - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2011. - 411 c. - Текст : электронный // IPR BOOKS [сайт]. - URL: http://www.iprbookshop.ru/60851.html

4. Романьков, В. А. Алгебраическая криптография : монография. - 2023-06-30; Алгебраическая криптография. - Омск: Омский государственный университет им. Ф.М. Достоевского, 2013. - 136 c. - Текст : электронный // IPR BOOKS [сайт]. - URL: http://www.iprbookshop.ru/24868.html

6.3 Иные источники:

1. Журнал «Математические вопросы криптографии» - http://www.mathnet.ru/php/journal.phtml?jrnid=mvk&option_lang=rus

2. Журнал «BIS Journal - Информационная безопасность банков» - https://journal.ib-bank.ru/pub/169

3. Журнал «Занимательная криптография» - https://bigmir81.livejournal.com/420975.html

4. Блог«Криптография. Шифрование и криптоанализ» - https://habrahabr.ru/hub/crypto/page4/

5. Журнал «Безопасность информационных технологий» - https://bit.mephi.ru/index.php/bit

6. Журнал «Мир ПК» - https://www.osp.ru/pcworld

7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).

Лицензионное программное обеспечение:

Операционная система "Альт Образование"

LibreOffice

Microsoft Windows 10

Microsoft Office Профессиональный плюс 2007

Kaspersky Endpoint Security 10 для Windows "Лаборатория Касперского" 26.07.2018

Профессиональные базы данных и информационные справочные системы:

1. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: http://biblio.tsutmb.ru/elektronnyij-katalog

2. Университетская библиотека онлайн: электронно-библиотечная система. – URL: https://biblioclub.ru

3. Консультант студента. Гуманитарные науки: электронно-библиотечная система. – URL: https://www.studentlibrary.ru

4. Научная электронная библиотека eLIBRARY.ru. – URL: https://elibrary.ru

5. Российская государственная библиотека. – URL: https://www.rsl.ru

6. Российская национальная библиотека. – URL: http://nlr.ru

7. Электронная библиотека РФФИ. – URL: https://www.rfbr.ru/rffi/ru/library

Электронная информационно-образовательная среда

https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.