Контрольные задания для студентов заочной формы обучения

по дисциплине «Методы и средства защиты компьютерной информации»

**Ст. преподаватель кафедры ИСТ** Захарова Ильсияр Нилевна **(каб. 514 Б)**

**Принцип, по которому темы (варианты) должны выдаваться студентам:** номер варианта контрольного задания - последние две цифры номера зачетки студента. При выполнении 4-го задания номер варианта выбирается согласно условию, изложенного в задании.

**Тематика: Контрольная работа содержит 5 заданий,** которые включают теоретические вопросы методов и средств защиты информации и практическую работу которая базируется на знании криптографических методов защиты информации. Цель заданий: иметь представление и получения определенных навыков по принципам, методам и средствам защиты программ и данных от различных типов угроз с привлечением аппаратных и программных средств защиты.

Перед выполнением контрольной работы следует изучить теоретический материал по указанной литературе, выработать навыки решения типовых задач и примеров по соответствующей теме.

Контрольная работа оформляется в программной среде MS Office (или аналогичном офисном продукте). Листы в документе должны быть пронумерованы. Шрифт – Times New Roman, размер 14 пт. Выравнивание по ширине. Межстрочный интервал – одинарный. На второй странице в содержании следует указать страницу, с которой начинается каждое задание. Титульный лист оформляется по стандарту. Завершается работа списком использованной литературы, электронных изданий. Условия задач и формулировки вопросов переписываются полностью, без сокращения слов, после чего приводится подробное решение, ответы на поставленные вопросы.

Возвращенные на доработку контрольные работы, должны быть исправлены с учетом замечаний, изложенных в рецензии, и сданы на повторную проверку.

Никакие исправления в тексте уже проверенной работы не допускают**ся!** Все исправления записываются после рецензии преподавателя.

Контрольную работу студент после проверки предъявляет к защите. На защите студент должен показать свое умение решать задачи, подобные тем, что имеются в его контрольной работе. Без предъявления защищенных работ студент к экзамену (зачету) не допускается.

**Задания контрольной работы.**

Вариант 1.

1. Понятие безопасности автоматизированных систем обработки нформации.

2. Проблема удаленной аутентификации пользователей. Протоколы CHAP и S/KEY.

3. Электронные ключи HASP. Их классификации, архитектура.

Вариант 2.

1. Субъект и объект доступа. Санкционированный и несанкционированный доступ.

2. Защита баз данных аутентификации в ОС Windows. Алгоритмы.

3. Разрушающие программные воздействия. Определение, принцип опосредованного НСД.

Вариант 3.

1. Конфиденциальность, целостность, доступность информации. Примеры нарушения данных свойств.

2. Защита баз данных аутентификации. Типовые схемы хранения ключевой информации.

3. Классификация разрушающих программных воздействий.

Вариант 4.

1. Способы защиты от угроз нарушения конфиденциальности, целостности, доступности. Угрозы и уязвимости. Классификация защитных мер и их характеристика.

2. Шифр RSA.

3. Вирусы как класс разрушающих программных воздействий. Защита от вирусов.

Вариант 5.

1. Принципы проектирования систем защиты информации и их характеристика.

2. Однонаправленные функции и особенности их использования в асимметричных криптосистемах.

3. Основные методы защиты от разрушающих программных воздействий.

Вариант 6.

1. Классификация технических каналов утечки.

2. Электронно-цифровая подпись и функции хеширования.

3. Проверка ПО на наличие недекларированных возможностей.

Вариант 7.

1. Защита информации от утечки по техническим каналам.

2. Алгоритм шифрования DES.

3. Классы защищенности АС и СВТ от НСД. Показатели защищенности,

требования.

Вариант 8.

1. Политики безопасности. Дискреционные и мандатные политики.

2. Симметричные и асимметричные криптосистемы.

3. Защита информации в компьютерных сетях.

Вариант 9.

1. Политика безопасности Белла-ЛаПадулы.

2. Требования к реализации стойких криптографических систем.

3. Межсетевые экраны.

Вариант 10.

1. Идентификация и аутентификация субъектов. Технические устройства идентификации и аутентификации.

2. Шифры гаммирования. Формирование гаммы шифра.

3. Сети VPN на основе шифрования.

Вариант 11.

1. Парольные системы идентификации и аутентификации. Количественная оценка стойкости парольной защиты.

2. Традиционные криптографические системы. Шифры перестановки.

3. Сканеры уязвимостей.

Вариант 12.

1. Биометрические системы идентификации и аутентификации личности.

2. Традиционные криптографические системы. Моноалфавитные и многоалфавитные замены.

3. Защита документов Microsoft Office и архивов.

Вариант 13.

1. Понятие безопасности автоматизированных систем обработки информации.

2. Элементы теории чисел. Сравнимость по модулю.

3. Электронные ключи HASP. Их классификации, архитектура.

Вариант 14.

1. Субъект и объект доступа. Санкционированный и несанкционированный доступ.

2. Традиционные криптографические системы. Моноалфавитные и многоалфавитные замены.

3. Разрушающие программные воздействия. Определение, принцип опосредованного НСД.

Вариант 15.

1. Конфиденциальность, целостность, доступность информации. Примеры нарушения данных свойств.

2. Традиционные криптографические системы. Шифры перестановки.

3. Классификация разрушающих программных воздействий.

Вариант 16.

1. Способы защиты от угроз нарушения конфиденциальности, целостности, доступности. Угрозы и уязвимости. Классификация защитных мер и их характеристика.

2. Шифры гаммирования. Формирование гаммы шифра.

3. Вирусы как класс разрушающих программных воздействий. Защита от вирусов.

Вариант 17.

1. Принципы проектирования систем защиты информации и их характеристика.

2. Требования к реализации стойких криптографических систем.

3. Основные методы защиты от разрушающих программных воздействий.

Вариант 18.

1. Классификация технических каналов утечки.

2. Симметричные и асимметричные криптосистемы.

3. Проверка ПО на наличие недекларированных возможностей.

Вариант 19.

1. Защита информации от утечки по техническим каналам.

2. Алгоритм шифрования DES.

3. Классы защищенности АС и СВТ от НСД. Показатели защищенности, требования.

Вариант 20.

1. Политики безопасности. Дискреционные и мандатные политики.

2. Электронно-цифровая подпись и функции хеширования.

3. Защита информации в компьютерных сетях.

Вариант 21.

1. Политика безопасности Белла-ЛаПадулы.

2. Однонаправленные функции и особенности их использования в асимметричных криптосистемах.

3. Межсетевые экраны.

Вариант 22.

1. Идентификация и аутентификация субъектов. Технические устройства идентификации и аутентификации.

2. Шифр RSA.

3. Сети VPN на основе шифрования.

Вариант 23.

1. Парольные системы идентификации и аутентификации. Количественная оценка стойкости парольной защиты.

2. Защита баз данных аутентификации. Типовые схемы хранения ключевой информации.

3. Сканеры уязвимостей.

Вариант 24.

1. Биометрические системы идентификации и аутентификации личности.

2. Защита баз данных аутентификации в ОС Windows. Алгоритмы.

3. Защита документов Microsoft Office и архивов.

Вариант 25.

1. Политики безопасности. Дискреционные и мандатные политики.

2. Проблема удаленной аутентификации пользователей. Протоколы CHAP и S/KEY.

3. Основные методы защиты от разрушающих программных воздействий.

Вариант 26.

1. Политика безопасности Белла-ЛаПадулы.

2. Электронно-цифровая подпись и функции хеширования.

3. Классификация разрушающих программных воздействий.

Вариант 27.

1. Идентификация и аутентификация субъектов. Технические устройства идентификации и аутентификации.

2. Алгоритм шифрования DES.

3. Вирусы как класс разрушающих программных воздействий. Защита от вирусов.

Вариант 28.

1. Способы защиты от угроз нарушения конфиденциальности, целостности,

доступности. Угрозы и уязвимости. Классификация защитных мер и их характеристика.

2. Симметричные и асимметричные криптосистемы.

3. Электронные ключи HASP. Их классификации, архитектура.

Вариант 29.

1. Принципы проектирования систем защиты информации и их характеристика.

2. Защита баз данных аутентификации. Типовые схемы хранения ключевой информации.

3. Разрушающие программные воздействия. Определение, принцип

опосредованного НСД.

Вариант 30.

1. Классификация технических каналов утечки.

2. Защита баз данных аутентификации в ОС Windows. Алгоритмы.

3. Вирусы как класс разрушающих программных воздействий. Защита от вирусов.

**4. (практическое) задание**базируется на знании криптографических методов защиты информации. Исходные данные для выполнения задания выбираются из таблицы № 1. Вариант выбирается в соответствии с последними цифрами номера студенческого билета. Например, студент, у которого номер студенческого билета 94034, должен выбрать вариант № 14 (остаток от деления 34 на 20). В качестве ключа берем свой вариант.

Таблица № 1

|  |  |
| --- | --- |
| № варианта | Название темы |
| **0** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   165554106909618929904944100802732132835474   1. Используя шифр Цезаря, зашифруйте слово ИНФОРМАЦИЯ и расшифруйте слово ГОЁСУМХП. 2. Используя шифр Виженера, зашифруйте слово УГРОЗА и расшифруйте слово ЛТАУ с ключевым словом МОРЕ. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   129133135142143128145141142145146156 |
| **1** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   415577102368082066907644216190552161835442   1. Используя шифр Цезаря, зашифруйте слово ПРАВИЛА и расшифруйте слово ЪЗОСЕЗН. 2. Используя шифр Виженера, зашифруйте слово ЯДРО и расшифруйте слово ДЦДХ с ключевым словом МОРЕ. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   136141148142144140128146136138128 |
| **2** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   573027109168322080024945403246554008832717   1. Используя шифр Цезаря, зашифруйте слово ШИФР и расшифруйте слово ТУСЕЗУНГ. 2. Используя шифр Виженера, зашифруйте слово ШИФР и расшифруйте слово МАРПА с ключевым словом МОРЕ. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   143144142131144128140140128 |
| **3** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   2990494453714077462408831353310932732132245474   1. Используя шифр Цезаря, зашифруйте слово АЛГОРИТМ и расшифруйте слово МРЧСУПГЩМВ. 2. Используя шифр Виженера, зашифруйте слово АТАКА и расшифруйте слово ПИЬО с ключевым словом РЕКА. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   143133144133145146128141142130138128 |
| **4** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   6646250468634077907061706709155361552161707742   1. Используя шифр Цезаря, зашифруйте слово РАБОТА и расшифруйте слово ФШЗПГ. 2. Используя шифр Виженера, зашифруйте слово СЕТЬ и расшифруйте слово ЧЕГИВЕ с ключевым словом РЕКА. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   140133134145133146133130142137157138144128141 |
| **5** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   8002764468711027028332833909155332302132835474   1. Используя шифр Цезаря, зашифруйте слово ПЕРЕСТАНОВКА и расшифруйте слово ЛГПЗРГ. 2. Используя шифр Виженера, зашифруйте слово СИСТЕМА и расшифруйте слово КШЮВТТ с ключевым словом КЛЮЧ. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   136141148142144140129146136135128150136159 |
| **6** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   235331900453141027022402272553043240434602   1. Используя шифр Цезаря, зашифруйте слово БЕЗОПАСНОСТЬ и расшифруйте слово ФМФХЗПГ. 2. Используя шифр Виженера, зашифруйте слово ЗАЩИТА и расшифруйте слово ЗХОЧЧ с ключевым словом КЛЮЧ. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   129144128141132140128147157144 |
| **7** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   910901024468631054902490772553453221859002   1. Используя шифр Цезаря, зашифруйте слово ЦЕЛОСТНОСТЬ и расшифруйте слово УГДСХГ. 2. Используя шифр Виженера, зашифруйте слово ИНФОРМАЦИЯ и расшифруйте слово ЙААИФА с ключевым словом ВАЗА. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   152136148144142130128141136133135128140133141142137 |
| **8** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   690901904409711077028390544968443221850290   1. Используя шифр Цезаря, зашифруйте слово ТЕХНОЛОГИЯ и расшифруйте слово УГДСХГ. 2. Используя шифр Виженера, зашифруйте слово ЭКРАН и расшифруйте слово МРППФО с ключевым словом ВАЗА. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   138142132142130128159146128129139136150128 |
| **9** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   29024944858373404441   1. Используя шифр Цезаря, зашифруйте слово КРИПТОГРАФИЯ и расшифруйте слово ТУСХСНСО. 2. Используя шифр Виженера, зашифруйте слово ТЕХНОЛОГИЯ и расшифруйте слово СМЧЪЩ с ключевым словом ЯДРО. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   143144128130136139142135128143136145136 |
| **10** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   664625457102888327834521   1. Используя шифр Цезаря, зашифруйте слово СИСТЕМА и расшифруйте слово ЁУГЧМН. 2. Используя шифр Виженера, зашифруйте слово МОНИТОР и расшифруйте слово ТЗАЫЖД с ключевым словом ЯДРО. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   145136145146133140128135128153136146155 |
| **11** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   46736170448377022490774968443240850290   1. Используя шифр Цезаря, зашифруйте слово МОНИТОР и расшифруйте слово ГЦЖМХ. 2. Используя шифр Виженера, зашифруйте слово ПРОГРАММА и расшифруйте слово БМАБР с ключевым словом ЯДРО. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   142129154133140136141148142144140128150136136 |
| **12** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   734080904945681421775483526853375024540283   1. Используя шифр Цезаря, зашифруйте слово УГРОЗА и расшифруйте слово ГХГНГ. 2. Используя шифр Виженера, зашифруйте слово ШИВРОВАНИЕ и расшифруйте слово ЙШАЕЩ с ключевым словом МОРЕ. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   133132136141136150128136135140133144133141136159 |
| **13** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   52908913830840525890523824774616   1. Используя шифр Цезаря, зашифруйте слово ЗАМЕНА и расшифруйте слово ЦЁУСЛГ. 2. Используя шифр Виженера, зашифруйте слово ОБНАРУЖЕНИЕ и расшифруйте слово ОЦАШЭ с ключевым словом МОРЕ. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   145136145146133140128145151136145139133141136159 |
| **14** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   91533102455363681927404139102612468521   1. Используя шифр Цезаря, зашифруйте слово ШИФРОВАНИЕ и расшифруйте слово НУМТХСЁУГЧМВ. 2. Используя шифр Виженера, зашифруйте слово ВТОРЖЕНИЕ и расшифруйте слово РУЕДД с ключевым словом КЛЮЧ. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   144128135140133144148128137139128 |
| **15** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   60042171027268696801024409149190   1. Используя шифр Цезаря, зашифруйте слово ОБНАРУЖЕНИЕ и расшифруйте слово ВЖУС. 2. Используя шифр Виженера, зашифруйте слово КРИПТОГРАФИЯ и расшифруйте слово СЛЧЯЫЛ с ключевым словом КЛЮЧ. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   140133146142132143133144133145146128141142130138136 |
| **16** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   4677495344324085026827774057372430096021207753893948   1. Используя шифр Цезаря, зашифруйте слово ВТОРЖЕНИЕ и расшифруйте слово ЕМУЦФ. 2. Используя шифр Виженера, зашифруйте слово БЕЗОПАСНОСТЬ и расшифруйте слово ЪОАУЧИ с ключевым словом МОРЕ. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   130136144146147128139156141128159145133146156 |
| **17** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   088362528339247109907891444077   1. Используя шифр Цезаря, зашифруйте слово ПРОГРАММА и расшифруйте слово ФЗХЯ. 2. Используя шифр Виженера, зашифруйте слово ПЕРЕСТАНОВКА и расшифруйте слово ЭУВЯ с ключевым словом МОРЕ. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   140133149128141136135140155135128153136146155 |
| **18** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   217740724630732181908124277768521346   1. Используя шифр Цезаря, зашифруйте слово ВИРУС и расшифруйте слово ЖСФХЦТ. 2. Используя шифр Виженера, зашифруйте слово ЗАМЕНА и расшифруйте слово ЫЕЫРШЪК с ключевым словом РЕКА. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   152136148144150133135128144159 |
| **19** | 1. Используя кодировочную таблицу №4, зашифруйте свои имя и фамилию. Какое сообщение зашифровано с помощью этой таблицы?   907725094561218546537727428367797527091253224690   1. Используя шифр Цезаря, зашифруйте слово СРЕДСТВО и расшифруйте слово ХГДОМЩГ. 2. Используя шифр Виженера, зашифруйте слово ПРАВИЛО и расшифруйте слово ВЕЛЛШЪК с ключевым словом РЕКА. 3. Придумайте свой шифр перестановки и с его помощью зашифруйте свои имя и фамилию. 4. Декодируйте с помощью кодировочной таблицы ASCII текст, заданный десятичным кодом:   145133144130136145155139133135142143128145141142145146136 |

Методические указания к заданию 5

«Шифры замены». Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы (см. табл. 2).

Таблица № 2

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **А** | **Б** | **В** | **Г** | **Д** | **Е** | **Ж** | **З** | **И** | **К** | **Л** | **М** | **Н** | **О** | **П** | **Р** |
| 21 | 37 | 14 | 22 | 01 | 24 | 62 | 73 | 46 | 23 | 12 | 08 | 27 | 53 | 35 | 04 |
| 40 | 26 | 63 | 47 | 31 | 83 | 88 | 30 | 02 | 91 | 72 | 32 | 77 | 68 | 60 | 44 |
| 10 | 03 | 71 | 82 | 15 | 70 | 11 | 55 | 90 | 69 | 38 | 61 | 54 | 09 | 84 | 45 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **С** | **Т** | **У** | **Ф** | **Х** | **Ц** | **Ч** | **Ш** | **Щ** | **Ъ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |
| 20 | 13 | 59 | 25 | 75 | 43 | 19 | 29 | 06 | 65 | 74 | 48 | 36 | 28 | 16 |
| 52 | 39 | 07 | 49 | 33 | 85 | 58 | 80 | 50 | 34 | 17 | 56 | 78 | 64 | 41 |
| 89 | 67 | 93 | 76 | 18 | 51 | 87 | 66 | 81 | 92 | 42 | 79 | 86 | 05 | 57 |

Например: 351044687256⇔ПАРОЛЬ