МИНИСТЕРСТВО НАУКИ И УКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Югорский государственный университет» (ЮГУ)
НЕФТЯНОЙ ИНСТИТУТ
(ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ЮГОРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(НефтИн (филиал) ФГБОУ ВО «ЮГУ»)

РАССМОТРЕНО
На заседании ПЦК МиЕНД
Протокол заседания
№ 07 от «31» августа 2022 г.
_____ Бойко Я.С

УТВЕРЖДАЮ
Зам. директора по УВР
НефтИн (филиал) ФГБОУ ВО «ЮГУ»
«31» августа 2022 г.
_____Хайбулина Р.И

КОМПЛЕКТ КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫХ МАТЕРИАЛОВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

(МЕЖДИСЦИПЛИНАРНОМУ КУРСУ)

МДК.02.02 КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ
(наименование учебной дисциплины, МДК)

программы подготовки специалистов среднего звена (ППССЗ)

по специальности СПО

10.02.05 Обеспечение информационной безопасности автоматизированных систем
(код, наименование)
программы подготовки специалистов среднего звена (ППССЗ)

базовой подготовки

г. Нижневартовск

-2022-

Комплект контрольно-измерительных материалов по учебной дисциплине МДК.02.02 Криптографические средства защиты информации программы подготовки специалистов среднего звена (ППССЗ) разработан на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем, в соответствии с рабочей программой учебной дисциплины МДК.02.02 Криптографические средства защиты информации.

Разработчики:

НефтИн (филиал) ФГБОУ ВО «ЮГУ»	преподаватель	Т.А Романова
(место работы)	(занимаемая должность)	(инициалы, фамилия)

1. Паспорт комплекта контрольно-измерительных материалов

1.1. Область применения

Комплект контрольно-измерительных материалов предназначен для проверки результатов освоения учебной дисциплины (далее - УД) МДК.02.02 Криптографические средства защиты информации программы подготовки специалистов среднего звена (ППССЗ) по специальности СПО *10.02.05 Обеспечение информационной безопасности автоматизированных систем.*

Комплект контрольно-измерительных материалов позволяет оценивать:
1.1.1. Освоение профессиональных компетенций (ПК) и общих компетенций (ОК)

Профессиональные и общие компетенции	Средства проверки (№ задания)
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	ПЗ 1-58, Выполнение практических работ
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	ПЗ 1-58, Выполнение практических работ
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	ПЗ 1-58, Выполнение практических работ
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	ПЗ 1-58, Выполнение практических работ
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	ПЗ 1-58, Выполнение практических работ
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	ПЗ 1-58, Выполнение практических работ
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	ПЗ 1-58, Выполнение практических работ
ОК 07. Содействовать сохранению окружающей среды, ресурсосбереже-	ПЗ 1-58, Выполнение практических работ

нию, эффективно действовать в чрезвычайных ситуациях.	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	ПЗ 1-58, Выполнение практических работ
ОК 09. Использовать информационные технологии в профессиональной деятельности.	ПЗ 1-58, Выполнение практических работ
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	ПЗ 1-58, Выполнение практических работ

1.1.2. Освоение умений и усвоение знаний

Освоенные умения, усвоенные знания	№ заданий для проверки
1	2
У1: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;	ПЗ 1-58
У2: диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;	ПЗ 1-58
У3: проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;	ПЗ 1-58
З1: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;	ПЗ 1-58
З2: методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;	ПЗ 1-58
З3: типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;	ПЗ 1-58

(Освоенные умения и усвоенные знания перечисляются из части ФГОС соответствующей УД (МДК), при наличии здесь указываются и дополнительные умения, и знания, введенные за счёт вариативной части).
Номера заданий для проверки – номера методических указаний к выполнению ЛПЗ, номера заданий в методические указания в ЛПЗ)

1.2. Система контроля и оценки освоения программы учебной дисциплины МДК.02.02 Криптографические средства защиты информации.

1.2.1. Формы промежуточной аттестации по ППССЗ при освоении учебной дисциплины МДК.02.02 Криптографические средства защиты информации.

Учебная дисциплина (междисциплинарный курс)	Формы промежуточной аттестации
1	2
МДК.02.02 Криптографические средства защиты информации 4-6 семестр	Другие формы контроля
МДК.02.02 Криптографические средства защиты информации 7 семестр	Экзамен

(Формы промежуточной аттестации указываются в соответствии с учебным планом)

1.2.2. Организация контроля и оценки освоения программы учебной дисциплины МДК.02.02 Криптографические средства защиты информации.

Промежуточный контроль по дисциплине осуществляется в форме экзамена.

Условием положительной аттестации по дисциплине на экзамене является положительная оценка освоения всех умений, знаний, а также формируемых профессиональных компетенций по всем контролируемым показателям.

2. Комплект материалов для оценки уровня освоения умений и усвоения знаний, сформированности общих и профессиональных компетенций при изучении учебной дисциплины МДК.02.02 Криптографические средства защиты информации.

2.1. Комплект материалов для оценки уровня освоения умений, усвоения знаний, сформированности общих и профессиональных компетенций

ТЕМЫ РЕФЕРАТОВ (ДОКЛАДОВ)

по учебной дисциплине МДК.02.02 Криптографические средства защиты информации.

1. История развития криптографии
2. Программная реализация классических шифров
3. Оптимизация методов частотного анализа моноалфавитных шифров.Программная реализация классических шифров
4. Методы механизации шифрования
5. Цифровое представление различных форм информации
6. Анализ современных симметричных криптоалгоритмов
7. Анализ современных асимметричных криптоалгоритмов

8. Программная реализация современных криптоалгоритмов
9. Сравнительный анализ функций хеширования
10. Аутентификация сообщений
11. Законодательство в области криптографической защиты информации
12. Перспективные направления криптографии

Оценка «4» ставится, если:
• Содержание реферата соответствует теме;
• Тема раскрыта полностью;
• Оформление реферата соответствует принятым стандартам;
• При работе над рефератом автор использовал современную литературу;
• В реферате отражена практическая работа автора по данной теме;
• В сообщении автор допускает одну ошибку или два-три недочета, допускает неполноту
ответа, которые исправляет только с помощью учителя.
Оценка «3» ставится, если:
• Содержание реферата не полностью соответствует теме;
• Тема раскрыта недостаточно полно;
• В оформлении реферата допущены ошибки;
• Литература, используемая автором, при работе над рефератом устарела;
• В реферате не отражена практическая работа автора по данной теме;
• Сообщение по теме реферата допускаются 2-3 ошибки;
• Сообщение неполно, построено несвязно, но выявляет общее понимание работы;
• При ответе на дополнительные вопросы допускаются ошибки, ответ
неуверенный, требует постоянной помощи учителя.
Оценка «2» ставится, если:
• Содержание реферата не соответствует теме;.
Оценка «1» ставится, если:
• Обучающийся не представил рефератную работу соответствующую выбранной теме

Составители _____ / Романова Т.А. /
подпись Ф.И.О.
«_____ » _____ 2022 г.

КОМПЛЕКТ ТЕСТОВЫХ ЗАДАНИЙ

по учебной дисциплине МДК.02.02 Криптографические средства защиты информации:

Тестирование по теме «Основы криптографии»

F1: МДК.02.02 Криптографические средства защиты информации.
F2: Романова Татьяна Александровна
F3: Экзамен
I:
S: Что такое шифрование?
+: способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого

-: совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств
-:удобная среда для вычисления конечного пользователя
I:
S: Что такое кодирование?
+: преобразование обычного, понятного текста в код+
-: преобразование
-: написание программы
I:
S: Для восстановления защитного текста требуется:
+: ключ
-: матрица
-: вектор
I:
S: Сколько лет назад появилось шифрование?
+: четыре тысячи лет назад
-: две тысячи лет назад
-: пять тысяч лет назад
I:
S: Первое известное применение шифра:
+: египетский текст
-: русский
-: нет правильного ответа
I:
S: Секретная информация, которая хранится вWindows:
+: пароли для доступа к сетевым ресурсам
+: пароли для доступа в Интернет
+: сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере
I:
S: Что такое алфавит?
+: конечное множество используемых для кодирования информации знаков
-: буквы текста
-: нет правильного ответа
I:
S: Что такое текст?
+: упорядоченный набор из элементов алфавита
-: конечное множество используемых для кодирования информации знаков
-: все правильные
I:
S: Выберите примеры алфавитов:
+: Z256 – символы, входящие в стандартные коды ASCII и КОИ-8
+: восьмеричный и шестнадцатеричный алфавиты
-: AEE
I:
S: Что такое шифрование?
+: преобразовательный процесс исходного текста в зашифрованный
-: упорядоченный набор из элементов алфавита
-: нет правильного ответа
I:
S: Что такое дешифрование?
+: на основе ключа шифрованный текст преобразуется в исходный
-: пароли для доступа к сетевым ресурсам
-: сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

I:
S: Что представляет собой криптографическая система?
+: семейство T преобразований открытого текста, члены его семейства индексируются символом k
-: программу
-: систему
I:
S: Что такое пространство ключей k?
+: набор возможных значений ключа
-: длина ключа
-: нет правильного ответа
I:
S: На какие виды подразделяют криптосистемы?
+: симметричные
+: ассиметричные
+: с открытым ключом
I:
S: Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования:
+: 1
-: 2
-: 3

I:
S: Количество используемых ключей в системах с открытым ключом:
+: 2
-: 3
-: 1
I:
I:
S: Ключи, используемые в системах с открытым ключом:
+: открытый
+: закрытый
-: нет правильного ответа
I:
S: Выберите то, как связаны ключи друг с другом в системе с открытым ключом:
+: математически
-: логически
-: алгоритмически
I:
S: Что принято называть электронной подписью?
+: присоединяемое к тексту его криптографическое преобразование
-: текст
-: зашифрованный текст
I:
S: Что такое криптостойкость?
+: характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа
-: свойство гаммы
-: все ответы верны
I:
S: Выберите то, что относится к показателям криптостойкости:
+: количество всех возможных ключей
+: среднее время, необходимое для криптоанализа
-: количество символов в ключе

I:
S: Требования, предъявляемые к современным криптографическим системам защиты информации:
+: знание алгоритма шифрования не должно влиять на надежность защиты
+: структурные элементы алгоритма шифрования должны быть неизменными
+: не должно быть простых и легко устанавливаемых зависимостью между ключами
+последовательно используемыми в процессе шифрования
I:
S: Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:
+: длина шифрованного текста должна быть равной лине исходного текста
+: зашифрованное сообщение должно поддаваться чтению только при наличии ключа
-: нет правильного ответа
I:
S: Основными современными методами шифрования являются:
+: алгоритм гаммирования
+: алгоритмы сложных математических преобразований
+: алгоритм перестановки
I:
S: Чем являются символы исходного текста, складывающиеся с символами некой случайной последовательности?
+: алгоритмом гаммирования
-: алгоритмом перестановки
-: алгоритмом аналитических преобразований
I:
S: Чем являются символы оригинального текста, меняющиеся местами по определенному принципу, которые являются секретным ключом?
+: алгоритм перестановки
-: алгоритм подстановки
-: алгоритм гаммирования
I:
S: Самая простая разновидность подстановки:
+: простая замена
-: перестановка
-: простая перестановка
I:
S: Количество последовательностей, из которых состоит расшифровка текста по таблице Вижинера:
+: 3
-: 4
-: 5
I:
S: Таблицы Вижинера, применяемые для повышения стойкости шифрования:
+: во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке
-: в качестве ключа используется случайность последовательных чисел+
-: нет правильного ответа
I:
S: Суть метода перестановки:
+: символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов
-: замена алфавита
-: все правильные
I:
S: Цель криптоанализа:
+: Определение стойкости алгоритма

-: Увеличение количества функций замещения в криптографическом алгоритме
-: Уменьшение количества функций подстановок в криптографическом алгоритме
-: Определение использованных перестановок
I:
S: По какой причине произойдет рост частоты применения брутфорс-атак?
-: Возросло используемое в алгоритмах количество перестановок и замещений
-: Алгоритмы по мере повышения стойкости становились менее сложными и более подверженными атакам
+: Мощность и скорость работы процессоров возросла
-: Длина ключа со временем уменьшилась
I:
S: Не будет являться свойством или характеристикой односторонней функции хэширования:
-: Она преобразует сообщение произвольной длины в значение фиксированной длины
-: Имея значение дайджеста сообщения, невозможно получить само сообщение
-: Получение одинакового дайджеста из двух различных сообщений невозможно, либо случается крайне редко
+: Она преобразует сообщение фиксированной длины в значение переменной длины
I:
S: Выберите то, что указывает на изменение сообщения:
-: Изменился открытый ключ
-: Изменился закрытый ключ
-: Изменился дайджест сообщения+
-: Сообщение было правильно зашифровано
I:
S: Алгоритм американского правительства, который предназначен для создания безопасных дайджестов сообщений:
-: Data Encryption Algorithm
-: Digital Signature Standard
+:) Secure Hash Algorithm
-: Data Signature Algorithm
I:
S: Выберите то, что лучшеописывает отличия между HMAC и CBC-MAC?
-: HMAC создает дайджест сообщения и применяется для контроля целостности; CBC-MAC используется для шифрования блоков данных с целью обеспечения конфиденциальности
-: HMAC использует симметричный ключ и алгоритм хэширования; CBC-MAC использует первый блок в качестве контрольной суммы
+: HMAC обеспечивает контроль целостности и аутентификацию источника данных; CBC-MAC использует блочный шифр в процессе создания MAC
-: HMAC зашифровывает сообщение на симметричном ключе, а затем передает результат в алгоритм хэширования; CBC-MAC зашифровывает все сообщение целиком
I:
3 S: Определите преимущество RSA над DSA?
+: Он может обеспечить функциональность цифровой подписи и шифрования
-: Он использует меньше ресурсов и выполняет шифрование быстрее, поскольку использует симметричные ключи
-: Это блочный шифр и он лучше поточного
-: Он использует одноразовые шифровальные блокноты
I:
S: С какой целью многими странами происходит ограничение использования и экспорта криптографических систем?
-: Без ограничений может возникнуть большое число проблем совместимости при попытке использовать различные алгоритмы в различных программах
-: Эти системы могут использоваться некоторыми странами против их местного населения

+: Криминальные элементы могут использовать шифрование, чтобы избежать обнаружения и преследования
-: Законодательство сильно отстает, а создание новых типов шифрования еще больше усиливает эту проблему
I:
S: Выберите то, что используют для создания цифровой подписи:
-: Закрытый ключ получателя
-: Открытый ключ отправителя
+: Закрытый ключ отправителя
-: Открытый ключ получателя
I:
S: Выберите то, что лучше всего описывает цифровую подпись:
-: Это метод переноса собственноручной подписи на электронный документ
-: Это метод шифрования конфиденциальной информации
-: Это метод, обеспечивающий электронную подпись и шифрование
+: Это метод, позволяющий получателю сообщения проверить его источник и убедиться в целостности сообщения
I:
S: Эффективная длина ключа в DES:
+: 56
-: 64
-: 32
-: 16
I:
S: Причина, по которой удостоверяющий центр отзывает сертификат:
-: Если открытый ключ пользователя скомпрометирован
-: Если пользователь переходит на использование модели PEM, которая использует сеть доверия
+: Если закрытый ключ пользователя скомпрометирован
-: Если пользователь переходит работать в другой офис
I:
S: Выберите то, что лучше всего описывает удостоверяющий центр?
-: Организация, которая выпускает закрытые ключи и соответствующие алгоритмы
-: Организация, которая проверяет процессы шифрования
-: Организация, которая проверяет ключи шифрования
+: Организация, которая выпускает сертификаты
I:
S: Расшифруйте аббревиатуру DEA:
-: Data Encoding Algorithm
-: Data Encoding Application
+: Data Encryption Algorithm
-: Digital Encryption Algorithm
I:
S: Разработчик первого алгоритма с открытыми ключами:
-: Ади Шамир
-: Росс Андерсон
-: Брюс Шнайер
+: Мартин Хеллман
I:
S: Процесс, выполняемый после создания сеансового ключа DES:
-: Подписание ключа
-: Передача ключа на хранение третьей стороне (key escrow)
-: Кластеризация ключа
+: Обмен ключом

I:
S: Количество циклов перестановки и замещения, выполняемый DES:
+: 16
-: 32
-: 64
-: 56
I:
S: Выберите правильное утверждение в отношении шифрования данных, выполняемого с целью их защиты:
-: Оно обеспечивает проверку целостности и правильности данных
+: Оно требует внимательного отношения к процессу управления ключами
-: Оно не требует большого количества системных ресурсов
-: Оно требует передачи ключа на хранение третьей стороне (escrowed)
I:
S: Название ситуации, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст:
-: Коллизия
-: Хэширование
-: MAC
+: Кластеризация ключей
I:
S: Определение фактора трудозатрат для алгоритма:
-: Время зашифрования и расшифрования открытого текста
+: Время, которое займет взлом шифрования
-: Время, которое занимает выполнение 16 циклов преобразований
-: Время, которое занимает выполнение функций подстановки
I:
S: Основная цельиспользования одностороннего хэширования пароля пользователя:
-: Это снижает требуемый объем дискового пространства для хранения пароля пользователя
+: Это предотвращает ознакомление кого-либо с открытым текстом пароля
-: Это позволяет избежать избыточной обработки, требуемой асимметричным алгоритмом
-: Это предотвращает атаки повтора (replay attack)
I:
S: Алгоритм, основанный на сложности разложения больших чисел на два исходных простых сомножителя:
-: ECC
+: RSA
-: DES
-: Диффи-Хеллман
I:
S: Что является описанием разницы алгоритмов DES и RSA:
+: DES – это симметричный алгоритм, а RSA – асимметричный
-: DES – это асимметричный алгоритм, а RSA – симметричный
-: Они оба являются алгоритмами хэширования, но RSA генерирует 160-битные значения хэша
-: DES генерирует открытый и закрытый ключи, а RSA выполняет шифрование сообщений
I:
S: Алгоритм, использующий симметричный ключ и алгоритм хэширования:
+: HMAC
-: 3DES
-: ISAKMP-OAKLEY
-: RSA
I:

S: Количество способов гаммирования:
+: 2
-: 5
-: 3
I:
S: Показатель стойкости шифрования методом гаммирования:
+: свойство гаммы
-: длина ключа
-: нет правильного ответа
I:
S: То, что применяют в качестве гаммы:
+: любая последовательность случайных символов
-: число
-: все ответы верны
I:
S: Метод, который применяют при шифровании с помощью аналитических преобразований:
+: алгебры матриц
-: матрица
-: факториал
I:
S: То, что применяют в качестве ключа при шифровании с помощью аналитических преобразований:
+: матрица А
-: вектор
-: обратная матрица
I:
S: Способ осуществления дешифрования текста при аналитических преобразованиях:
+: умножение матрицы на вектор
-: деление матрицы на вектор
-: перемножение матриц

КОМПЛЕКС ПРАКТИЧЕСКИХ ЗАНЯТИЙ
по учебной дисциплине МДК.02.02. Криптографические средства защиты информации
ТЕМАТИКА ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Номер темы	Номер работы	Наименование работы (занятия)	Количество аудиторных часов
1	2	3	4
1.1	1.	Практическое занятие № 1 «Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений».	2
1.1	2.	Практическое занятие № 2 «Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений».	2
1.1	3.	Практическое занятие №3 «Проверка чисел на простоту»	2
1.1	4.	Практическое занятие №4 «Проверка чисел на простоту»	2
1.1	5.	Практическое занятие №5 «Решение задач с элементами теории чисел.»	2
1.1	6.	Практическое занятие №6 «Решение задач с элементами теории чисел.»	2
2.1	7.	Практическое занятие №7 «Применение классических шифров замены »	2
2.1	8.	Практическое занятие №8 «Применение классических шифров замены »	2
2.1	9.	Практическое занятие № 9 «Применение классических шифров перестановки»	2
2.1	10.	Практическое занятие № 10 «Применение классических шифров перестановки»	2
2.1	11.	Практическое занятие № 11 «Применение метода гаммирования»	2
2.1	12.	Практическое занятие № 12 «Применение метода гаммирования»	2
2.2	13.	Практическое занятие №13 «Криптоанализ шифра простой замены методом анализа частотности символов»	2
2.2	14.	Практическое занятие №14 «Криптоанализ шифра простой замены методом анализа частотности символов»	2
2.2	15.	Практическое занятие № 15 «Криптоанализ шифра простой замены методом анализа частотности символов»	2
2.2	16.	Практическое занятие №16 «Криптоанализ шифра простой замены методом анализа частотности символов»	2

2.2	**17.**	Практическое занятие № 17 Криптоанализ классических шифров методом полного перебора ключей	**2**
2.2	**18.**	Практическое занятие № 18 Криптоанализ классических шифров методом полного перебора ключей	**2**
2.2	**19.**	Практическое занятие № 19 Криптоанализ классических шифров методом полного перебора ключей	**2**
2.2	**20.**	Практическое занятие № 20 «Криптоанализ шифра Вижинера»	**2**
2.2	**21.**	Практическое занятие № 21 «Криптоанализ шифра Вижинера»	**2**
2.2	**22.**	Практическое занятие № 22 «Криптоанализ шифра Вижинера»	**2**
2.3	**23.**	Практическое занятие № 23 «Применение методов генерации ПСЧ»	**2**
3.1	**24.**	Практическое занятие № 24 «Кодирование информации»	**2**
3.1	**25.**	Практическое занятие № 25 «Кодирование информации»	**2**
3.1	**26.**	Практическое занятие № 26 «Кодирование информации»	**2**
3.1	**27.**	Практическое занятие №27 «Программная реализация классических шифров»	**2**
3.1	**28.**	Практическое занятие №28 «Программная реализация классических шифров»	**2**
3.1	**29.**	Практическое занятие №29 «Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге».	**2**
3.1	**30.**	Практическое занятие №30 «Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге».	**2**
3.2	**31.**	Практическое занятие №31 «Изучение программной реализации современных симметричных шифров».	**2**
3.2	**32.**	Практическое занятие №32 «Изучение программной реализации современных симметричных шифров».	**2**

3.2	**33.**	Практическое занятие №33 «Изучение программной реализации современных симметричных шифров».	**2**
3.2	**34.**	Практическое занятие №34 «Изучение программной реализации современных симметричных шифров».	**2**
3.3	**35.**	Практическое занятие №35 «Применение различных асимметричных алгоритмов».	**2**
3.3	**36.**	Практическое занятие №36 «Применение различных асимметричных алгоритмов».	**2**
3.3	**37.**	Практическое занятие №37 «Применение различных асимметричных алгоритмов».	**2**
3.3	**38.**	Практическое занятие №38 «Применение различных асимметричных алгоритмов».	**2**
3.4	**39.**	Практическое занятие №39 «Применение различных функций хеширования, анализ особенностей хешей».	**2**
3.4	**40.**	Практическое занятие №40 «Применение различных функций хеширования, анализ особенностей хешей».	**2**
3.4	**41.**	Практическое занятие №41 «Применение различных функций хеширования, анализ особенностей хешей».	**2**
3.4	**42.**	Практическое занятие №42 «Применение криптографических атак на хеш-функции».	**2**
3.4	**43.**	Практическое занятие №43 «Применение криптографических атак на хеш-функции».	**2**
3.4	**44.**	Практическое занятие №44 «Изучение программно-аппаратных средств, реализующих основные функции ЭП».	**2**
3.4	**45.**	Практическое занятие №45 «Изучение программно-аппаратных средств, реализующих основные функции ЭП».	**2**
3.5	**46.**	Практическое занятие №46 «Применение протокола Диффи-Хеллмана для обмена ключами шифрования».	**2**
3.5	**47.**	Практическое занятие №47 «Применение протокола Диффи-Хеллмана для обмена ключами шифрования».	**2**
3.5	**48.**	Практическое занятие №48 «Применение протокола Диффи-Хеллмана для обмена ключами шифрования».	**2**

3.5	**49.**	Практическое занятие №49«Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos».	**2**
3.5	**50.**	Практическое занятие №50 «Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos».	**2**
3.5	**51.**	Практическое занятие №51 «Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos».	**2**
3.7	**52.**	Практическое занятие №52 «Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых Паролей».	**2**
3.7	**53.**	Практическое занятие №53 «Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых Паролей».	**2**
3.7	**54.**	Практическое занятие №54 «Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых Паролей».	**2**
3.8	**55.**	Практическое занятие №55 «Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ».	**2**
3.8	**56.**	Практическое занятие №56 «Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ».	**2**
3.8	**57.**	Практическое занятие №57 «Реализация простейших стеганографических алгоритмов».	**2**
3.8	**58.**	Практическое занятие №58 «Реализация простейших стеганографических алгоритмов».	**2**
Всего:			**116**

Критерии оценки:

Процент результативности (правильных ответов)	**Качественная оценка индивидуальных образовательных достижений**	
90 ÷ 100	5	отлично
80 ÷89	4	хорошо
70 ÷79	3	удовлетворительно
менее 70	2	не удовлетворительно

Составители _____ / Романова Т.А. /
подпись Ф.И.О.
«_____ » _____ 2022 г.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1-2

***Применение алгоритма Евклида для нахождения НОД. Решение линейных* диофантовых уравнений**

Цель: научиться решать линейные диофантовые уравнения с двумя неизвестными, используя алгоритм Евклида.

Теоретические вопросы

1. Алгоритм Евклида для нахождения НОД.
2. Понятие неопределенного уравнения.
3. Понятие диофантового уравнения.
4. Понятие линейного диофантового уравнения.
5. Алгоритм решения линейных диофантовых уравнений.

Задание 1. Повторить алгоритм Евклида. Как с помощью алгоритма Евклида найти НОД двух чисел?

Задание 2. Найти НОД и его линейное выражение:

а) НОД(11,8);

б) НОД(654,792);

в) НОД(3660,525);

г) НОД(400,288);

д) НОД(490,518);

е) НОД(510,272).

Задание 3. Приведите определение неопределенного уравнения.

Задание 4. Приведите определение диофантового уравнения.

Задание 5. Приведите примеры линейных дтофантовых уравнений.

Задание 6. Изучите пример решения линейного диофантового уравнения: Решить уравнение $11x + 13y = 300$ в натуральных числах.

1. НОД(11,13) = 1.
2. Находим линейное разложение $1 = 11\cdot 6 + 13\cdot(-5)$.
3. Умножаем обе части на 300, получаем

$$\begin{cases} x = 1800 + 13t, \\ y = -1500 - 11t. \end{cases} \quad t \in Z$$

4. Найдём решение в натуральных числах, для этого решим систему неравенств:

$$\begin{cases} 1800 + 13t > 0, \\ -1500 - 11t > 0; \end{cases}$$

$$\begin{cases} t > -138\frac{6}{13}; \\ t < -136\frac{4}{11}; \end{cases} \quad t \in Z.$$

Таким образом, получаем два целых решения системы $t = -138$ и $t = -137$. Найдём решения задачи для полученных значений t.

При $t = -138$ $x = 6$, $y = 18$.

При $t = -137$ $x = 19$, $y = 7$.

Задание 7. Решить уравнения в целых числах:

1) $8x + 14y = 32$;

2) $9x - 18y = 5$.

Задание 8. Решите диофантово уравнение при помощи линейного представления

a) $43x - 111y = 87$; b) $39x - 111y = 89$;

c) $41x - 111y = 87$; d) $38x - 111y = 89$.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 3-4

Проверка чисел на простоту

Цель: научиться проверять числа на простоту.

Теоретические вопросы

1. Понятие простого числа.
2. Способы проверки числа на простоту.

Задание 1. Изучите способ проверки числа на простоту «Пробное деление».

Словесное описание: способ состоит в последовательном делении числа на все нечетные числа, которые содержатся в интервале. Если в процессе деления получим целый результат, то число составное. Если же при переборе всех нечетных чисел из интервала разделить число на эти числа нацело нельзя, то число простое (рисунок 1).

Программная реализация на языке C++:

```
bool prime(long long n){
        for(long long i=2;i<=sqrt(n);i++)
                if(n%i==0)
                        return false;
        return true;
}
```

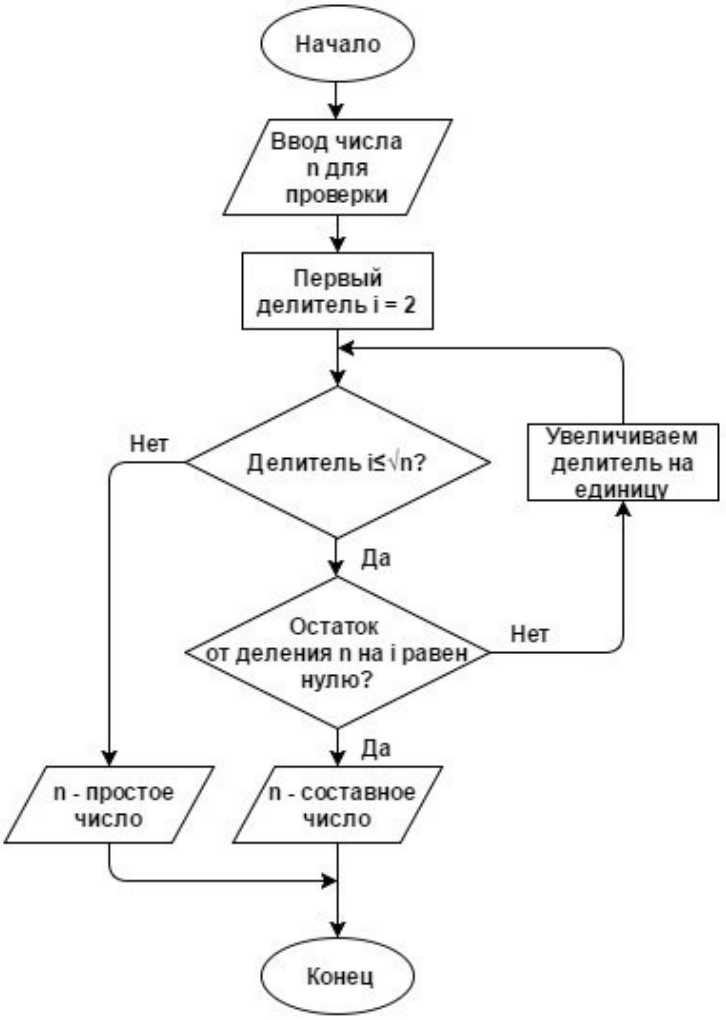

Рисунок 1 – Схема алгоритма

Задание 2. Изучите вероятностный алгоритм проверки на простоту числа «Тест на основе малой теоремы Ферма».

Малая теорема Ферма утверждает, что если *n* простое, то выполняется условие: при всех *a* из {1, 2, …, n−1} имеет место сравнение:

$$a^{n-1} \equiv 1 \ (mod\ n) \qquad (1)$$

Из этой теоремы следует, что если сравнение (1) не выполнено хотя бы для одного числа *a* в интервале *{1, 2, …, n−1}*, то *n* — составное. Поэтому можно предложить следующий вероятностный тест простоты.

1. выбираем случайное число *a* из *{1, 2, ..., n−1}* и проверяем с помощью алгоритма Евклида условие *(a, n) = 1*;
2. если оно не выполняется, то ответ «*n* — составное»;
3. проверяем выполнимость сравнения (1);
4. если сравнение не выполнено, то ответ «*n* — составное»;
5. если сравнение выполнено, то ответ неизвестен, но можно повторить тест еще раз.

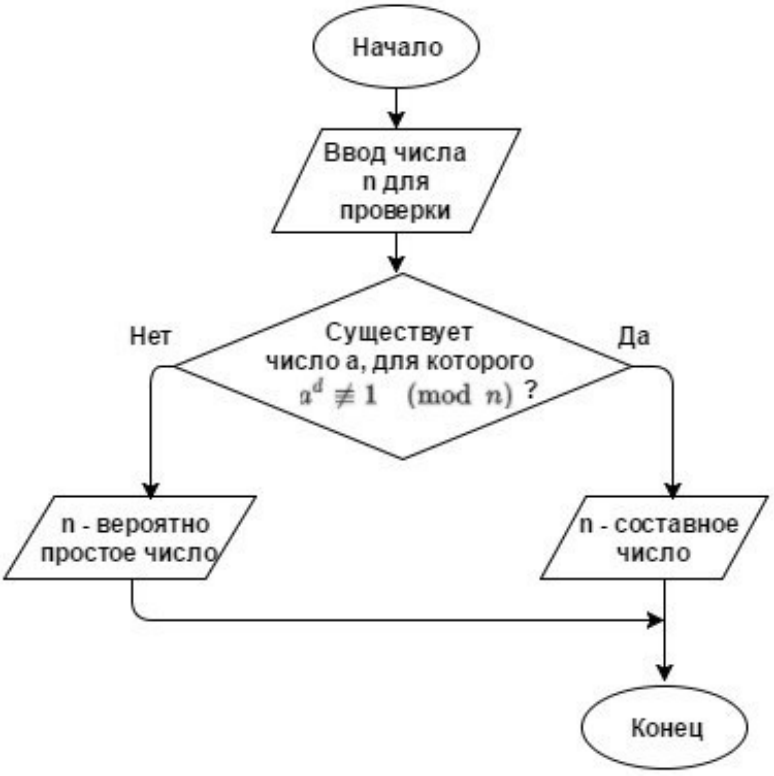

Рисунок 2. Схема алгоритма Программная реализация на языке C++:

```
bool ferma(long long x){
        if(x == 2)
                return true;
        srand(time(NULL));
        for(int i=0;i<100;i++){
                long long a = (rand() % (x - 2)) + 2;
                if (gcd(a, x) != 1)
                        return false;
                if( pows(a, x-1, x) != 1)
                        return false;
        }
        return true;
}
```

Нахождение НОД:

```
long long gcd(long long a, long long b){
        if(b==0)
                return a;
        return gcd(b, a%b);
}
```

Быстрое возведение в степень по модулю:

```
long long mul(long long a, long long b, long long m){
        if(b==1)
                return a;
        if(b%2==0){
                long long t = mul(a, b/2, m);
                return (2 * t) % m;
        }
        return (mul(a, b-1, m) + a) % m;
}

long long pows(long long a, long long b, long long m){
        if(b==0)
                return 1;
        if(b%2==0){
                long long t = pows(a, b/2, m);
                return mul(t , t, m) % m;
        }
        return ( mul(pows(a, b-1, m) , a, m)) % m;
}
```

Задание 3. Проверьте числа 11, 27, 119 на простоту с помощью представленных алгоритмов.

Задание 4. Изучите алгоритм проверки на простоту числа «Решето Эратосфена». Постройте схему алгоритма.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 5-6

Решение задач с элементами теории чисел.

Цель: решение задач с элементами теории чисел.

Теоретические вопросы

1. Делимость чисел. Признаки делимости. Простые и составные числа.
2. Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.
3. Отношения сравнимости. Свойства сравнений. Модулярная арифметика.
4. Мультипликативные функции. Примеры мультипликативных функций.
5. Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.
6. Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.
7. Китайская теорема об остатках.
8. Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.
9. Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод

Полларда.

10. Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.
11. Арифметические операции над большими числами.

Задание 1. Найти все простые числа, не превосходящие 60.

Задание 2. Разложить на простые множители $n = 29359$.

Задание 3. При каких натуральных n число $a = 2^n + 1$ делится на 3? ***Задание 4.*** Найти все делители числа 496 и сумму его собственных делителей. ***Задание 5.*** Доказать, что если $p > 4$ и взаимно просто с 6, то $p^2 - 1$ делится на 24.***Задание 6.*** Найти НОД (1176, 315).

Задание 7. Решить систему сравнений

$$\begin{cases} x \equiv 2(\mathrm{mod}\ 5), \\ x \equiv 8(\mathrm{mod}\ 11). \end{cases}$$

Задание 8. Решить систему сравнений

$$a)\ \begin{cases} x \equiv 2(\mathrm{mod}\ 5), \\ x \equiv 8(\mathrm{mod}\ 11); \end{cases} \qquad b)\ \begin{cases} 4x \equiv 3(\mathrm{mod}\ 15), \\ 3x \equiv 1(\mathrm{mod}\ 10). \end{cases}$$

Задание 9. Решить систему сравнений

$$\begin{cases} 3x + 4y \equiv 29(\mathrm{mod}\ 143), \\ 2x - 9y \equiv -847(\mathrm{mod}\ 143). \end{cases}$$

Задание 10. Найти остаток от деления:

$$\text{a) } 2^{1050} \text{ на } 17; \quad \text{b) } 5^{1995} \text{ на } 9; \quad \text{c) } 7^{1018} \text{ на } 19.$$

Задание 10. Докажите, что число вида $5m + 2$ (при целом m) не является полным квадратом.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 7-8

Применение классических шифров замены

Цель: научиться применять классические шифры замены.

Теоретические вопросы

1. Понятие криптографии.
2. Понятие шифра.
3. Шифр замены.
4. Шифр многоалфавитной замены.
5. Сходства и различия шифра Гронсфельда и шифра Цезаря.
6. Биграммный шифр замены.

Задание 1. Выбрать один из методов замены:
а)шифр
Атбаш; б)
Шифр
Цезаря;
в) шифр Полбианский квадрат; г)
шифр
Трисимуса;
д) шифр многоалфвитной заменыВижинера; е)
шифр биграммами; ж) шифр Гронсфельда.
Составить алгоритм программы шифрования по выбранному методу.
Задание 2. Составить программу шифрования по выбранному методу.
Задание 3. Составить алгоритм программы расшифрования по выбранному методу.
Составить программу расшифрования по выбранному методу.
Задание 4. Расшифровать текст,
а) зашифрованный шифром Цезаря со сдвигом на 4 позиции:

Уокдгнбэылмбаноюбожмдлокндне

биь б) зашифрованный шифром Цезаря со сдвигом на 6 позиции:

Иыфщлзвмелнмцйкяиыкъбиьъзвгйякялмъзиьдъвбъ жязъ в) зашифрованный заменой по кодовому слову «пароль»:

випигьпжоймгсзпчгумйрпигяиьлйжбийржгясыипипльбийнсынгнсьзъ

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №9-10

Применение классических шифров перестановки

Цель: научиться применять классические шифры перестановки.

Теоретические вопросы

1. Понятие криптографии.
2. Понятие шифра.
3. Шифр перестановки.
4. Модификации шифров перестановки по таблице.
5. Понятие «магический квадрат».
6. Особенность шифра решетками.

Задание 1. Выбрать один из методов перестановки:
а) обратное написание текста;
б) простая перестановка по таблице;
в) одиночная перестановка по ключу по таблице;
г) одиночная перестановка символов с пропусками по таблице;
д) двойные перестановки столбцов и строк;
е) шифр «Магический квадрат»;
ж) шифр «Решетки» или «Трафареты».

Составить алгоритм программы шифрования по выбранному методу.

Задание 2. Составить программу шифрования по выбранному методу.

Задание 3. Составить алгоритм программы расшифрования по выбранному методу.

Составить программу расшифрования по выбранному методу.

Задание 4. Дешифровать сообщения:

а) Бирои имч еыеес витсч арзки танет есарл лпюсп мотоо еипнф кйаои крслт мн;

б) тиооско нцрпоед иявдттж афэелиа ткокнбв еапанъг уитриоб;

в) икинорткелэоидаржделлок.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 11-12
Применение метода гаммирования

Цель: научиться применять метод гаммирования.

Теоретические вопросы

1. Гаммирование: основные определения.
2. Алгоритм шифрования текста методом гаммирования.
3. Двоичное гаммирование: основные особенности.

Задание 1. Выбрать один из способов гаммирования:

а) гаммирование по модулю К;

б) двоичное гаммирование.

Составить алгоритм программы шифрования по выбранному методу.

Задание 2. Составить программу шифрования по выбранному методу.

Задание 3. Составить алгоритм программы расшифрования по выбранному методу.

Составить программу расшифрования по выбранному методу.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №13-16
Криптоанализ шифра простой замены методом анализа частотности символов

Цель: научиться выполнять криптоанализ шифра простой замены методом анализа частотности символов.

Теоретические вопросы

1. Понятие криптоанализа.
2. Методика криптоанализа, основанная на исследовании частотности закрытого текста.
3. Правило А. Керхоффа.

Задание 1. Получить от преподавателя текстовый файл, содержащий большойхудожественный текст на русском языке в открытом виде. Написать программу «Частота символов». Исследовать частотность символов открытого теста.

Задание 2. Получить от преподавателя текстовый файл, содержащий большой объем зашифрованного текста на русском языке. Исследовать частотность зашифрованного текста.

Задание 3. Сравнивая реальную частотность символов русского языка, полученную в пункте 1, с частотностями зашифрованного текста, составить таблицу замен алгоритма шифрования и расшифровать зашифрованный текст, реализовав программу дешифровки. Дешифровке подвергните только первые 15–20 символов, наиболее часто встречающиеся в шифротексте.

Задание 4. Выполнить эвристический анализ текста, полученного в результате дешифровки. По смыслу текста выявить те замены, которые оказались неверными, и сформировать верные

замены. Доведите результат дешифровки до приемлемого (удобочитаемого) вида.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 17-19

Криптоанализ классических шифров методом полного перебора ключей

Цели: научиться выполнять криптоанализ классических шифров методом полного перебора ключей.

Теоретические вопросы

1. Понятие криптоанализа.
2. Понятие стойкости криптографического алгоритма.
3. Типовые методы криптоанализа классических алгоритмов.
4. Инструменты криптоанализа

Задание 1. Расшифровать фразу, зашифрованную столбцовой перестановкой:

a) ОКЕСНВРП_ЫРЕАДЕЫН_В_РСИКО;

b) ДСЛИЕЗТЕА_Ь_ЛЬЮВМИ_ _АОЧХК;

c) НМВИАИ_НЕВЕ_СМСТУОРДИАНКМ;

d) ЕДСЗЬНДЕ_МУБД_УЭ_КРЗЕМНАЫ;

e) СОНРЧОУО_ХДТ_ИЕИ_ВЗКАТРРИ.

Задание 2. Расшифровать фразу, зашифрованную двойной перестановкой (сначала были переставлены столбцы, затем строки):

a) СЯСЕ_ _ЛУНЫИАККННОГЯДУЧАТН;

b) МСЕЫ_ЛЫВЕНТОСАНТУЕИ_РЛПОБ;

c) АМНРИД_УЕБСЫ_ЕЙРСООКОТНВ_;

d) ОПЧУЛС_БООНЕВ_ОЖАЕОНЕЩЕИН;

e) ЕШИАНИРЛПГЕЧАВРВ_СЕЫНА_ЛО.

Задание 3. Расшифровать текст. Каждой букве алфавита соответствует двузначное число:

1) 39 25 20 34 82 63 66 46 35 20 25 82 86 39 51 74 35 51 66 20 44 37 25 27
51 35 44 20 90 37 51 25 25 51 63 91 20 11 37 46 48 25 20 37 61 51 14 82 82 66 82
35 29 82 91 25 51 74 51 24 78 51 24 59 46 86 51 44 74 20 25 37 37, 37 44 82 31 11
37 82 51 46 25 51 34 82 25 37 82 86 37 25 27 51 35 44 20 90 37 51 25 25 48 44
46 82 78 25 51 14 51 18 37 59 44, 51 74 82 35 20 90 37 59 44 66 90 82 25 25 48 44
37 61 10 44 20 18 20 44 37, 86 61 20 25 86 51 39 66 86 51 44 10 66 82 86 46 51
35 10 37 66 51 46 51 39 51 63 66 39 59 91 37. 56 46 51 86 20 66 20 82 46 66
59 24 35 10 18 37 78 51 35 18 20 25 37 91 20 90 37 63, 4651, 66 51 18 14 20 66
25 51 35 82 91 10 14 29 46 20 46 20 44 35 20 91 14 37 56 25 48 78 37 66 66 14 82
24 51 39 20 25 37 63, 35 10 86 51 39 51 24 37 46 82 14 37 44 25 51 18 37 78 37 91
25 37 78 91 25 20 31 46 51 61 51 66 25 51 39 25 48 78 39 37 24 20 78 10 18
35 51 91, 25 51 25 82 10 24 82 14 59 31 46 24 51 14 42 25 51 18 51 39 25 37
44 20 25 37 59 24 20 25 25 48 44 39 51 74 35 51 66 20 44, 66 56 37 46 20 59,
56 46 51 51 61 82 66 74 82 56 82 25 37 82 37 25 27 51 35 44 20 90 37 51 25 25 51 63

61 82 91 51 74 20 66 25 51 66 46 37 25 82 37 44 82 82 46 66 44 48 66 14 20, 82
66 14 37 51 46 66 10 46 66 46 39 10 82 46 39 37 24 37 44 20 59 10 18 35 51 91 20
2) 74 29 23 27 17 99 71 25 49 32 29 34 27 63 32 25 17 99 60 62 25 34 95 29 53
59 82 27 71 29 77 99 34 27 91 17 99 71 49 99 27 15 60 32 25 50 27 17 62 27 95 27
50 25 91 32 59 77 95 29 50 25 99 59, 25 99 74 29 53 25 59 17 99 25 91 23 49 71 25
17 99 60 49 25 34 32 25 71 95 27 82 27 32 32 25 29 50 17 25 15 77 99 32 59 77
62 95 25 53 95 29 23 32 25 17 99 60 34 15 35 17 27 99 27 71 25 12 25 99 95 29 45
49 74 29. 62 95 27 63 34 27 71 17 27 12 25, 50 27 17 62 27 95 27 50 25 91 32 29
35 95 29 50 25 99 29 17 29 82 49 83 62 25 17 27 50 27 62 95 25 34 59 74 99 25
71 50 27 53 25 62 29 17 32 25 17 99 49 17 71 35 53 29 32 29 17 32 29 15 49 23
49 27 82 32 29 34 27 63 32 25 95 29 50 25 99 29 77 10 27 12 25 25 50 25 95 59 34
25 71 29 32 49 35 49 95 27 53 27 95 71 49 95 25 71 29 32 49 27 82 74 95 49 99 49 23
32 89 83 74 25 99 74 29 53 59 50 15 25 74 25 71 62 49 99 29 32 49 35 49 53
29 62 25 82 49 32 29 77 10 49 83 59 17 99 95 25 91 17 99 71. 34 15 35 62 25 17 15
27 34 32 49 83 25 62 99 49 82 29 15 60 32 25 62 95 49 82 27 32 27 32 49 27 34 49
17 74 25 71 89 83 82 29 17 17 49 71 25 71 12 25 95 35 23 27 91 53 29 82 27 32 89.
74 29 23 27 17 99 71 25 49 32 29 34 27 63 32 25 17 99 60 95 29 50 25 99 89 34
25 17 99 49 12 29 27 99 17 35 25 62 99 49 82 49 53 29 67 49 27 91 62 95 25 12 95 29
82 82 32 25 12 25 25 50 27 17 62 27 23 27 32 49 35.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 20-22
Криптоанализ шифра Вижинера

Цель: научиться выполнять криптоанализ шифра Виженера.

Теоретические вопросы

1. Понятие криптоанализа.
2. Шифр Виженера.

Задание 1. Составить алгоритм шифрования и расшифрования методом Виженера.

Задание 2. Задан некоторый текст зашифрованный шифром Виженера, требуется определить ключевое слово и прочитать открытый текст.

Шифрованный текст

Влцдутжбюцхъяррмшбрхцэооэцгбрьцмйфктъъюьмшэсяцпунуящэйтаьэдкцибр
ьцгбрпачкъуцпъбьсэгкцъгуущарцёэвърюуоюэкааэбрняфукабъарпяъафкъиьжяффнйо
яфывбнэнфуюгбрьсшьжэтбэёчюъюръегофкбьчябашвёэуъъюаднчжчужцёэвлрнчулб
юпцуруньъшсэюъзкцхъяррнрювяспэмасчкпэужьжыатуфуярюравртубурьпэщлафоуф
бюацмнубсюкйтаьэдйюнооэгюожбгкбръндэпотчмёодзцвбцшщвщепчдчдръюьскасэг
ъппэгюкдойрсрэвоопчщшоказръббнэугнялёкьсрбёуыэбдэулбюасшоуэтъшкрсдугэфл
бубуъчнчтртпэгюкиугюэмэгюккъъпэгяапуфуэзьрадзьжчюрмфцхраююанчёчюъыхьъ
цомэфъцпоирькнщпэтэузуябащущбаыэйчдфрпэцъьрьцъцпоилуфэдцойэдятррачкубу
фнйтаьэдкцкрннцюабугюуубурьпйюэъжтгюркующоъуфъэгясуоичщщчдцсфырэдщэ
ъуяфшёчцюйрщвяхвмкршрпгюопэуцчйтаьэдкцибрьцыяжтюрбуэтэбдуящэубъибрюв
ъежагибрбагбрымпуноцшяжцечкфодщоъчжшйуъцхчщвуэбдлдъэгясуахзцэбдэулькнъ

щбжяцэьрёдъьвюврнуяфуоухфекьгцччгэъжтанопчынажпачкъуъмэнкйрэфщэъьбуд
эндадъярьеюэлэтчоубъцэфэвлнёэгфдсэвэёкбсчоукгаутэыпуббцчкпэгючсаъбэнэфърк
ацхёваетуфяепьрювържадфёжбьфутощоявьъгупчршуитеачйчирамчюфчоуяюонкяжы
кгсцбрясшчйотъъжрсщчл

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 23
Применение методов генерации ПСЧ

Цель: изучение способов применения методов генерации ПСЧ.

Теоретические вопросы

1. Псевдослучайные числа.
2. Генератор псевдослучайных чисел.
3. Свойства генератора псевдослучайных чисел для использования в криптографических целях.
4. Принципы использования генераторов псевдослучайных чисел при потоковом шифровании.
5. Методы генерации ПСЧ.

Задание 1. Написать программу, выполняющую задачу исследования ДСЧ для одного из следующих вариантов:

1. Исследовать равномерность датчика (проверить гипотезу о равномерности распределения совокупности ДСЧ).
2. Определить период ДСЧ для различных параметров.
3. Исследовать автокорреляцию совокупности ДСЧ для различных параметров на глубину 100 отсчетов.
4. Построить гистограмму частоты появления каждого возможного значения совокупности ДСЧ.

Задание 2. Разработать и отладить ПО для исследования датчика псевдослучайных чисел. Представить результаты исследования в графическом виде.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 24-26
Кодирование информации

Цель: изучение способов кодирования информации.

Теоретические вопросы

1. Кодирование информации.
2. Символьное кодирование информации.
3. Смысловое кодирование информации.

Задание 1. Дана кодовая таблица азбуки Морзе:

А • —	Л • — • •	Ц — • — •
Б — • • •	М — —	Ч — — — •
В • — —	Н — •	Ш — — — —
Г — — •	О — — —	Щ — — • —
Д — • •	П • — — •	Ъ • — — • — •
Е •	Р • — •	Ы — • — —
Ж • • • —	С • • •	Ь — • • —
З — — • •	Т —	Э • • — • •
И • •	У • • —	Ю • • — —
Й • — — —	Ф • • — •	Я • — • —
К — • —	Х • • • •	

Декодируйте сообщение:

—— ——— • — • • ——— — • • — • — • — • ——

Закодируйте с помощью азбуки Морзе слова ПАРОЛЬ, ЭКРАНИРОВАНИЕ, КОДИРОВАНИЕ.

Задание 2. Дана таблица ASCII-кодов:

Таблица ASCII-кодов															
SP	!	"	#	$	%	&	`	(	)	*	+	,	-	.	/
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
@	A	B	C	D	E	F	G	M	I	J	K	L	M	N	O
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
`	a	e	c	d	e	f	g	h	i	j	k	l	m	n	0
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127

Расшифровать слово при помощи таблицы ASCII кодов: 49 20 6C 6FF 75.

Закодировать при помощи таблицы ASCII кодов слово Windows. Результат представить в шестнадцатеричной системе счисления.

Задание 3. Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца

	0	1	2	3	4	5	6	7	8
0	А	Б	В	Г	Д	Е	Ё	Ж	З
1	И	К	Л	М	Н	О	П	Р	С
2	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
3	Ы	Ь	Э	Ю	Я	_	.	,	?
4	:	;	-	!	»				

С помощью этой кодировочной таблицы закодируйте фразу: Я ЗНАЮ МЕТОДЫ ШИФРОВАНИЯ.

Задание 4. Используя таблицу кодирования.

	№ *п/п*	***Символ***	***Двоичный код***

1	Р	101
2	О	100
3	И	010
4	Е	011
5	П	1110
6	М	1100
7	ПРОБЕЛ	1101
8	А	0010
9	С	0011
10	Г	00000
11	В	00001
12	К	00010
13	Б	00011
14	З	111100
15	Т	111101
16	Ь	111110
17	Н	111111

Закодируйте слово СИМВОЛ. Рассчитайте полученную степень сжатия. Раскодируйте слово 11101011000000010100101100110000 10.

Задание 5. Смысловое кодирование – это кодирование, в котором в качестве исходного алфавита используются не только отдельные символы (буквы), но и слова и даже наиболее часто встречающиеся фразы.

Рассмотрим пример одноалфавитного и многоалфавитного смыслового кодирования.

Пример. Открытый текст: "19.9.1992 ГОДА". Таблица кодирования представлена в таблице:

Элементы открытого текста	Коды
1	089 146 214 417
2	187 226 145 361
_	_
9	289 023 194 635
ГОД	031 155 217 473
_	786 432 319 157

Закодированное сообщение при одноалфавитном кодировании:

"089 289 786 289 786 089 289 289 187 031".

Закодированное сообщение при многоалфавитном кодировании:

"089 289 786 023 432 146 194 635 187 031" (при многоалфавитном кодировании одинаковыесимволы заменяются кодами из следующего столбца).

Разработайте и примените свой вариант смыслового кодирования информации.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 27-28

Программная реализация классических шифров

Цель: изучение способов кодирования информации.

Теоретические вопросы

1. Основные понятия криптографии.
2. Основные понятия криптоанализа.
3. Методы шифрования и кодирования информации.

Задание 1

Вариант 1

В Средние века для шифрования перестановкой применялись и магические квадраты. Магическими квадратами называют квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.

Шифруемый текст вписывали в магические квадраты в соответствии с нумерацией их клеток. Если затем выписать содержимое такой таблицы по строкам, то получится шифртекст, сформированный благодаря перестановке букв исходного сообщения. В те времена считалось, чтосозданные с помощью магических квадратов шифртексты охраняет не только ключ, но и магическая сила.

Пример магического квадрата и его заполнения сообщением «Прилетаю восьмого» показан ниже (рисунок 3).

Шифртекст, получаемый при считывании содержимого правой таблицы по строкам, имеет вполне загадочный вид

ОИРМ ЕОСЮ ВТАЬ ЛГОП.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

О	И	Р	М
Е	О	С	Ю
В	Т	А	Ь
Л	Г	О	П

Рисунок 3

Число магических квадратов быстро возрастает с увеличением размера квадрата. Существует только один магический квадрат размером 3 × 3 (если не учитывать его повороты). Количество

магических квадратов 4 × 4 составляет уже 880, а количество магических квадратов 5 × 5 – около 250000.

Пользуясь изложенным способом создать программу, которая:

а) зашифрует введенный текст и сохранит его в файл;

б) считает зашифрованный текст из файла и расшифрует данный текст.

Вариант 2

Для обеспечения дополнительной скрытности можно повторно зашифровать сообщение, которое уже прошло шифрование. Такой метод шифрования называется двойной перестановкой. В случае двойной перестановки столбцов и строк таблицы перестановки определяются отдельно для столбцов и отдельно для строк. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровании порядок перестановок должен быть обратным.

Пример выполнения шифрования методом двойной перестановки показан на рисунке 4. Если считывать шифртекст из правой таблицы построчно блоками по четыре буквы, то получится следующее: ТЮАЕ ООГМ РЛИП ОЬСВ.

	4	1	3	2
3	П	Р	И	Л
1	Е	Т	А	Ю
4	В	О	С	Ь
2	М	О	Г	О

Исходная таблица

	1	2	3	4
3	Р	Л	И	П
1	Т	Ю	А	Е
4	О	Ь	С	В
2	О	О	Г	М

Перестановка столбцов

	1	2	3	4
1	Т	Ю	А	Е
2	О	О	Г	М
3	Р	Л	И	П
4	О	Ь	С	В

Перестановка строк

Рисунок 4

Ключом к шифру двойной перестановки служит последовательность номеров столбцов и номеров строк исходной таблицы (в нашем примере последовательности 4132 и 3142 соответственно).

Число вариантов двойной перестановки быстро возрастает при увеличении размера таблицы:

- для таблицы 3 × 3 – 36 вариантов;
- для таблицы 4 × 4 – 576 вариантов;
- для таблицы 5 ×5 – 14400 вариантов.

Пользуясь изложенным способом создать программу, которая: а) зашифрует введенный текст и сохранит его в файл;

б) считает зашифрованный текст из файла и расшифрует данный текст.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 29-30

***Изучение реализации классических шифров замены и перестановки в программе* CrypTool или аналоге.**

Цель: ознакомиться с меню, возможностями программы CrypTool.

Теоретические вопросы

1. Основные понятия криптографии.
2. Основные понятия криптоанализа.
3. Методы шифрования и кодирования информации.

Задание 1. Ознакомиться с меню, возможностями программы CrypTool.

Задание 2. Перечислите классические алгоритмы шифрования, которые описаны и реализованы в программе CrypTool.

Задание 3. Зашифровать и расшифровать сообщение с помощью одного из имеющегося в программе CrypTool классического шифра замены и шифра перестановки.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 31-34

Изучение программной реализации современных симметричных шифров

Цель: ознакомиться с современными симметричными шифрами.

Теоретические вопросы

1. Понятие криптографической системы.
2. Классификация криптографических систем.
3. Симметричные шифры.
4. Блочные алгоритмы шифрования.

Задание 1. Представьте алгоритм работы российского стандарта шифрования ГОСТ 28147-89.

Задание 2. Представьте алгоритм работы американского стандарта шифрования DES. Сравните алгоритмы шифрования ГОСТ 28147-89 и DES.

Задание 3. Выполнить ручное шифрование исходного текста с помощью алгоритма DES, алгоритма ГОСТ 28147-89.

Задание 4. Опишите особенности алгоритма AES. Сравните алгоритмы шифрования ГОСТ 28147-89 и AES.

Задание 5. Охарактеризуйте программы симметричного шифрования сообщений. Результаты представьте в виде таблицы.

Программа	Характеристики
Бесплатное ПО	
AES Free	
FineCrypt	
Dpcrypto	

Платное ПО	
EasyCrypto Deluxe	
Crypto-Lock	
Iron Key	
SafeGuard PrivateCrypto	

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 35-38

Применение различных асимметричных алгоритмов

Цель: ознакомиться с асимметричными алгоритмами.

Теоретические вопросы

1. Понятие криптографической системы.
2. Классификация криптографических систем.
3. Проблема распределения ключей.
4. Асимметричные алгоритмы шифрования.
5. Типы односторонних преобразований.

Задание 1. Опишите асимметричные алгоритмы шифрования.

Тип	Описание
RSA	
ECC (криптосистема на основе эллиптических кривых)	
Эль-Гамаль.	

Задание 2. Изучите процедуру создания ключей в алгоритме шифрования RSA на примере.

№ п/п	Описание операции	Пример
1	Выбираются два простых числа[1] **p** и **q**.	p=7, q=13
2	Вычисляется произведение **n** = p * q.	n=91
3	Вычисляется **функция Эйлера**[2] **φ(n)**.	φ(n)=(7-1)(13-1)= 91-7-13+1 = 72
4	Выбирается открытый ключ **e**, как произвольное число (0<e<n), взаимно простое[3] с результатом функции Эйлера (e ⊥ φ(n)).	e=5
5	Вычисляется секретный ключ **d**, как обратное число[4] к **e** по модулю **φ(n)**, из соотношения (d*e) mod φ(n) = 1.	(d*5) mod 72 = 1, d = 29
6	Публикуются открытый ключ (**e**, **n**) в специальном хранилище, где исключается возможность его подмены (**общедоступном сертифицированном справочнике**).	

Создайте открытый и секретный ключи для любой другой пары простых чисел.

Задание 4. Разработать алгоритм шифрования RSA.

Изучение программнойреализации асимметричного алгоритма RSA

Цель: ознакомиться с асимметричными алгоритмами.

Теоретические вопросы

1. Понятие криптографической системы.
2. Классификация криптографических систем.
3. Проблема распределения ключей.
4. Асимметричные алгоритмы шифрования.
5. Типы односторонних преобразований.

Задание 1. Разработать и отладить приложение, реализующее алгоритм асимметричного

шифрования RSA.

Предлагаемый интерфейс приложения (рисунок 5).

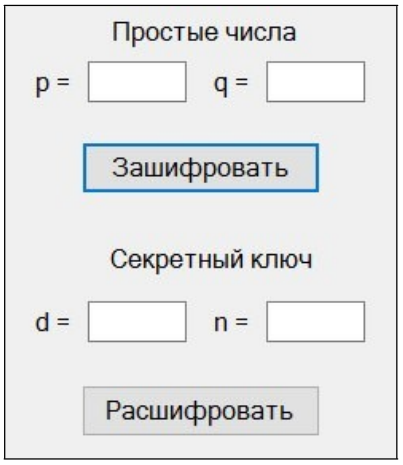

Рисунок 5

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 39-41

Применение различных функций хеширования, анализ особенностей хешей

Цель: ознакомиться с различными функциями хеширования.

Теоретические вопросы

1. Понятие хеширования.
2. Хеш-функции.
3. Анализ особенностей хешей.
4. Свойства хеш-функций.

Задание 1. Опишите функции хеширования.

Тип	Описание
MD2	
MD4	
MD5	
SHA (Secure Hash Algorithm)	

Задание 2. Опишите свойства хеш-функций.

Задание 3. Ознакомьтесь с алгоритмом работы хеш-функции MD5.

Задание 4. Программно реализовать алгоритм MD4 хеширования символьной строки. Хеш- код представить в виде 16-ричного числа.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 42-43

Применение криптографических атак на хеш-функции.

Цель: научиться применять криптографические атаки на хеш-функции.

Теоретические вопросы

1. Понятие хеширования.
2. Хеш-функции.
3. Анализ особенностей хешей.
4. Свойства хеш-функций.
5. Атаки на функции хеширования.

Задание 1. Приведите примеры атак на функции хеширования.

Задание 2. Противник перехватил хеш H = H (M1). Длина хеша *n* битов. Он хочет найти любое сообщение M2 , для которого H (M1) = H (M2), для чего генерирует *k* сообщений и вычисляет их хеши. Какова вероятность успеха?

Задание 3. Противник перехватил определенное число хешей разных сообщений. Длина хеша *n* битов. Сколько новых сообщений и их хешей надо сгенерировать, чтобы найти коллизию для 50 % перехваченных хешей?

Задание 4. Хэш-функция дает хеш длиной 64 бита. Сколько хешей надо сгенерировать, чтобы найти коллизию двух любых сообщений?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 44-45

Изучение программно-аппаратных средств, реализующих основные функции ЭП

Цель: изучить программно-аппаратные средства, реализующие основные функции ЭП.

Теоретические вопросы

1. Понятие электронной цифровой подписи.
2. Свойства электронной цифровой подписи.
3. Схемы электронной цифровой подписи.
4. Алгоритмы цифровой подписи.

Задание 1. Разработать алгоритм реализации цифровой подписи RSA.

Задание 2. В чем отличие подписи RSA от алгоритма шифрования RSA?

Задание 3. Приведите примеры программно-аппаратных средств, реализующих основные функции электронной цифровой подписи.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 46-48

Применение протокола Диффи-Хеллмана для обмена ключами шифрования

Цель: изучить протокол Диффи-Хеллмана для обмена ключами шифрования.

Теоретические вопросы

1. Управление ключами.

2. Алгоритм обмена ключами по схеме Диффи-Хеллмана.
3. Формирование общего ключа.
4. Алгоритмы цифровой подписи.

Задание 1. Для каких целей может применяться алгоритм Диффи-Хеллмана?

Задание 2. Опишите последовательность действий при использовании алгоритма Диффи-Хеллмана.

Задание 3. На чём основывается безопасность обмена ключа по схеме Диффи-Хеллмана?

Задание 4. Доказать, что в схеме Диффи-Хеллмана $K_A = K_B$.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 49-51

Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.

Цель: изучить принципы работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.

Теоретические вопросы

1. Схема протокола Kerberos.
2. Аутентификация и авторизация клиента.
3. Недостатки и ограничения протокола Kerberos.
4. Политика протокола Kerberos.

Задание 1. Опишите схему протокола Kerberos (рисунок 6).

Рисунок 6

Задание 2. Объясните механизм работы протокола Kerberos.

Задание 3. Реализация Kerberos в ОС Windows Server.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 52-54

Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей

Цель: ознакомиться с механизмом аутентификации по одноразовым паролям.

Теоретические вопросы

1. Понятие аутентификации.
2. Механизмы аутентификации.
3. Аутентификация, основанная на паролях.
4. Среднее время безопасности пароля.
5. Концепция одноразовых паролей в системе аутентификации
6. Способы реализации принципа одноразовых паролей.

Задание 1. Приведите примеры устройств, используемых для генерации одноразовых паролей. Опишите алгоритм генерации одноразовых паролей.

Задание 2. Опишите способы защиты от атак на одноразовые пароли.

Описание атаки	Защита от данной атаки
Атака «Человек посередине» Злоумышленник перехватывает одноразовый пароль, посланный законным пользователем при аутентификации, блокирует законного пользователя и использует перехваченный пароль для входа в систему	
Кража аутентификационного токена Злоумышленник похищает аутентификационный токен законного пользователя и использует его для входа всистему	
Подбор PIN-кода аутентификационного токена Злоумышленник вручную производит перебор всех возможных значений PIN-кода похищенного им аутентификационного токена законного пользователя	
Извлечение значения секретного ключа из программного аутентификационного токена Злоумышленник копирует программный аутентификационный токен (программное обеспечение), пытается найти в нем хранимый секретный ключ, чтобы потом его использовать для аутентификации под видом законного пользователя	

Подбор PIN-кода аутентификационного токена с помощью известных OTP Злоумышленник перехватывает несколько правильных OTP, использованных для входа в систему, копирует программный аутентификационныи токен (программное обеспечение), и тем самым он пытается подобрать PIN-код путем перебора его возможных значений, для тестирования пробного значения PIN-кода используются перехваченные OTP	
Нечестный администратор аутентификационных токенов Злоумышленник является доверенным лицом либо является посредником доверенного лица, производящего инициализацию аутентификационного устройства до передачи его владельцу. Он может создать дубликат токена и, используя его, выдавать себя за владельца	

Задание 3. Разработать приложение, реализующее генерацию одноразовых паролей.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 55-56

Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ

Цель: изучить программное обеспечение, используемое для встраивания цифровых водяных знаков.

Теоретические вопросы

1. Понятие цифрового водяного знака. Его преимущества перед печатным водяным знаком.
2. Виды цифровых водяных знаков.
3. Методы защиты с помощью цифровых водяных знаков.
4. Программы для создания цифровых водяных знаков.

Задание 1. Приведите примеры устройств, используемых для генерации одноразовых паролей. Опишите алгоритм генерации одноразовых паролей.

Задание 2. Проведите сравнительный анализ программ, используемых для создания цифровых водяных знаков: PhotoWatermark Professional, Image Tuner, EasyWatermark, CryptoFoto.

Задание 3. Опишите процесс создания печатного водяного знака в программе Image Tuner.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 57-58

Реализация простейших стеганографических алгоритмов

Цель: изучить простейшие стеганографические алгоритмы.

Теоретические вопросы

1. Понятие стеганографии.
2. Назначение стеганографической системы.
3. Обобщенная модель стеганографической системы.
4. Классификация стеганографических систем.
5. Методы сокрытия информации.
6. Области применения стеганографии.

Задание 1. Рассмотреть работу двух программ, позволяющих проводитьстеганографические преобразования.

Задание 2. Выбрать контейнер и выполнить внедрение в него некоторой информации.

Задание 3. Попробовать извлечь информацию из стегоконтейнера, созданного другойпрограммой.

Задание 4. От чего зависит криптостойкость стеганографических систем?

ПЕРЕЧЕНЬ РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основная учебная литература:

Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/476997

Дополнительная учебная литература:

Сети и телекоммуникации : учебник и практикум для среднего профессионального образования /К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2021. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/475704