МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование ф-та полностью)
М.О. Таныгин
(подпись, инициалы, фамилия)
« *29* » *августа* 2022 г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Криптографические методы защиты информации
(наименование учебной дисциплины)

10.05.01 Информационная безопасность телекоммуникационных систем (профиль) «Защита информации в системах связи и управления»
(код и наименование ОПОП ВО)

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ СБЕСЕДОВАНИЯ.

Тема 1. Введение в криптологию.

1. Как были устроены первые криптосистемы?
2. Что такое криптоанализ?
3. Чем криптография отличается от криптоанализа?
4. Какое понятие шире криптография или криптология.
5. Назовите основные этапы истории развития криптологии как науки.
6. Каковы основные задачи криптологии как науки?
7. Назовите основные термины, используемые в криптографии.
8. Исторические сведения о системах и способах составления шифрованных писем.

Тема 2. Классификация криптоалгоритмов.

1. Сравнение систем шифрования относительно друг друга.
2. Как происходит использование открытого ключа.
3. Основы симметричного шифрования.
4. Блочные и поточные системы шифрования.
5. Классификация систем шифрования.
6. Симметричное шифрование, достоинства и недостатки.
7. Асимметричное шифрование, достоинства и недостатки
8. Преимущества использования блочных и поточных систем шифрования
9. Недостатки использования блочных и поточных систем шифрования.
10. Достоинства и недостатки симметричного шифрования.

Тема 3. Потоковые шифраторы.

1. Поточные шифры.
2. Современные поточные шифры.
3. Комбинирование РСЛОС.
4. Регистр сдвига с линейной обратной связью.
5. Ассоциированный многочлен.
6. Наиболее распространенные поточные шифры.
7. Приведите примеры поточных шифрови

Тема 4. Блочные криптоалгоритмы.

1. Как устроены режимы шифрования ECB и CBC, в чем их отличие.
2. Какой режим шифрования блочных шифров более стойкий

к атакам удаления и вставки.

3. Сделайте обзор наиболее распространенных блочных шифров.
4. Алгоритмы многократного кодирования.
5. Что такое блочные криптоалгоритмы?
6. Как устроено блочное шифрование?
7. Какие режимы блочного шифрования вы знаете.
8. Раунды шифрования.
9. Что такое сеть Фейштеля.
10. Как устроен шифр DES.

Тема 5. Ассиметричные криптоалгоритмы.

1. Сколько раундов шифрования в шифре DES?
2. Как устроен алгоритм разворачивания ключа в шифре DES.
3. Что такое секретный ключ.
4. Что такое ассиметричные криптоалгоритмы?
5. Математические основы шифрования с открытым ключом.
6. Как используется открытый ключ.
7. Системы распределения ключей.
8. Достоинства и недостатки систем с открытым ключом.

Тема 6. Алгоритмы обмена ключами.

1. Протокол Диффи-Хеллмана распределения ключей с тремя и более участниками.
2. Система управления ассиметричными ключами.
3. Цифровые сертификаты.
4. Центры сертификации.
5. Система управления симметричными ключами с предварительной частичной установкой.
6. Система управления симметричными ключами без предварительной частичной установки.
7. Схема Диффи-Хеллмана.
8. Схема Шамира.
9. Депонирование ключей. Encrypted File System (EFS).
10. Схема Шамира разделения секрета.

Тема 7. Применение программных систем шифрования.

1. Приведите примеры программных симметричных систем шифрования отечественного производства.
2. Программная реализация асимметричные системы шифрования.
3. Обзор основных программных продуктов на базе асимметричных систем шифрования.
4. Программный продукт PGP.
5. Применение программных криптосистем шифрования.
6. Программная реализация симметричные системы шифрования.
7. Обзор основных программных продуктов на базе симметричных систем шифрования.

8. Приведите примеры программных асимметричных систем шифрования отечественного производства

Тема 8. Стеганография.

1. Компьютерная стеганография.
2. Использование избыточности цифровой информации изображений.
3. Использование избыточности цифрового звука.
4. Использование избыточности цифрового видео.
5. Что такое стеганография.
6. Дайте основные понятия стеганографии.
7. Что такое тайнопись.
8. Использование компьютерных форматов данных.
9. Применение компьютерной стеганографии.
10. Классическая стеганография.
11. Практическое использование стеганографии.
12. Обзор основных методов использования классической стеганографии.

Тема 9. Криптоанализ и криптостойкость.

1. Основные методы криптоанализа.
2. Оценка предельных мощностей взлома.
3. Понятие стойкости шифров.
4. На чем основана безопасность криптографических протоколов.
5. Что такое доказуемая стойкость.
6. Что такое криптоанализ.
7. Что такое криптостойкость.
8. На чем основана проблема факторизации целых чисел.
9. В чем заключается проблема дискретного логарифма.
10. Теоретико-информационные оценки стойкости криптосистем.
11. Линейный криптоанализ.
12. Дифференциальный криптоанализ.

Критерии оценки:

2 балла выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

1 балл выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ К ЛАБОРАТОРНЫМ РАБОТАМ

Контрольные вопросы к лабораторной работе №1

1. Что такое частотные характеристики символов?
2. Какова криптостойкость шифра моноалфавитной подстановки?
3. Какие подстановочные шифры вам известны, назовите их?
4. Что такое шифр Виженера?
5. Что понимается под моноалфавитными подстановками?
6. Приведите примеры моноалфавитных подстановок.
7. Что такое коэффициент сдвига?
8. Что такое мощность алфавита?
9. Возможно ли применение статистических методов криптоанализа к полиалфавитным шифрам?
10. Что такое индекс соответствия криптограммы?

Контрольные вопросы к лабораторной работе №2

1. В чем особенности применения метода Метод Ф. Казиски?
2. Как узнать длину первичных ключей?
3. Какие подстановочные шифры вам известны, назовите их?
4. Какими методами возможно определение периода шифра?
5. Какую длину имеют первичные ключи, если длинна составного ключа равна 48, 60?
6. В чем отличие шифра Виженера от многопетлевых подстановок, какой метод более криптостойкий?

Контрольные вопросы к лабораторной работе №3

1. Для каких целей используют скремблеры и дескремблеры?
2. Какие типы скремблеров и дескремблеров вам известны?
3. Какие бывают алгоритмы шифрования?
4. Что такое потоковый шифр?
5. Что такое скремблер?
6. Что такое дескремблер?
7. Какие преимущества и недостатки самосинхронизирующихся скремблеров и дескремблеров вам известны?
8. Какие преимущества и недостатки аддитивных скремблеров и дескремблеров вам известны?

Контрольные вопросы к лабораторной работе №4

1. В чем отличие блочных от поточных шифров?
2. От чего зависит криптостойкость выбранного метода?
3. К каким шифрам относятся шифры перестановки?
4. Что такое сдвиговый регистр?
5. Дайте определение шифрованию и расшифрованию сообщений.
6. Суть алгоритма Берлекэмпа-Месси.
7. Алгоритм отыскания начального заполнения.
8. Сколько всевозможных ключей может быть бля блока длинной 8, 10 символов?
9. В чем отличие простых перестановок от путей Гамильтона, где больше ключей шифрования?

Контрольные вопросы к лабораторной работе №5

1. Что необходимо для оценки вероятности следования строк друг за другом?
2. Какую задачу необходимо решить для расшифровки криптограммы в общем случае?
3. К какому виду шифров относится шифр табличной перестановки?
4. С помощью какой формулы можно вычислить вероятности следования друг за другом всех возможных пар строк?
5. Дайте определение термину «диграмма».
6. Какую роль выполняет таблица вероятностей?
7. Что необходимо предпринять, если использование таблицы вероятностей не дает результата?

Контрольные вопросы к лабораторной работе №6

1. Оценка стойкости и безопасных размеров параметров криптосхемы;
2. Вывод формул для вычисления параметров к и g;
3. Анализ схемы на наличие слабостей и поиск вариантов усиления с минимальным модифицированием;
4. Общая характеристика и обоснование схемы ЭЦП, построенной на основе заданного проверочного уравнения
5. Описание процедуры генерации подписи и формулирование требований к ней;

Контрольные вопросы к лабораторной работе №7

1. Назовите схемы разделения секрета.
2. Достоинства схемы разделения секрета.
3. Недостатки схемы разделения секрета.
4. Что такое «разделение секрета»?
5. Что такое «тени» и как их вычислить?

6. Какие программные криптосистемы шифрования вы знаете, назовите
7. Назовите основные функциональные возможности Kremlin?
8. Перечислите исполняемые файлы Kremlin?
9. С помощью каких процедур осуществляется безвозвратное удаление файлов?
10. Какими методами возможна очистка истории работы на компьютере при помощи Kremlin?
11. Какие функции КМИЗ выполняет Kremlin?
12. Как осуществляется шифрование файлов?
13. Как происходит отправка зашифрованных сообщений?

Контрольные вопросы к лабораторной работе №8

1. Каким образом шифруется сообщение?
2. Какие типы файлов можно использовать для скрытия данных?
3. Какие операции над секретами вам доступны в начале работы?
4. Какие типы секретов доступны в программе?
5. Какие типы контейнеров для помещения туда секретов реализуются в программе?
6. Как создать хранилище RSA ключей?
7.
8. Что такое стеганография?
9. Что такое компьютерная стеганография?
10. Какие виды компьютерной стеганографии вы знаете?
11. Что такое файл-контейнер?
12. Какие файлы можно скрывать с помощью компьютерной стеганографии?
13. Какие программные продукты для реализации методов стеганографии вы знаете?
14. Какие алгоритмы лежат в основе работы Fox Secret?

Контрольные вопросы к лабораторной работе №9

1. Кто может расшифровать сообщение?
2. Каковы преимущества используемого способа шифрования?
3. Можно ли расшифровать сообщение с помощью ключа шифрования?
4. Что такое парольная фраза?
5. Каким образом строится таблица Виженера?
6. Опишите суть метода вероятных слов.
7. К какому типу криптосистем относится шифр Виженера?
8. Сколько существуют способов шифрования с помощью шифра Виженера?

Критерии оценки:

3 балла (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

2 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

1 балл (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1	Преобразование открытого текста сообщения в закрытый называется:
	алгоритм шифрования
	обеспечение аутентификации
	цифровая запись
	процедура шифрования
2	Входные параметры процесса шифрования
	Ключ
	зашифрованный текст
	Алгоритм
	открытый текст
3	Какие из сервисов реализуются при использовании криптографических преобразований
	Алгоритм
	контроль целостности
	Аутентификация
	Шифрование
4	Что позволяет предотвратить использование криптографических преобразований:
	отказ от информации
	использование алгоритмов асимметричного шифрования
	обеспечение аутентификации
	утечку информации
5	Знание ключа позволяет:
	выполнить обратное преобразование
	предотвратить утечку информации
	обеспечить аутентификацию
	использовать криптографические сервисы безопасности
6	Какой алгоритм не используется при симметричном шифровании:
	побитовое шифрование
	блочное шифрование
	алгоритм Эль-Гамаля
	поточное шифрование
7	Какой из режимов алгоритма DES используется для построения шифров гаммирования?

	обратная связь по выходу
	обратная связь по шифротексту
	сцепление блоков шифра
	электронная кодовая книга
8	Какова длина блока алгоритма шифрования DES:
	64 бита
	5 байт
	56 бит
	16 бит
	18 бит
9	Чем определяется уровень надежности применяемых криптографических преобразований:
	значением допустимой вероятности неисправностей или сбоев, приводящих к получению злоумышленником дополнительной информации о криптографических преобразованиях
	отношением количества дешифрованной информации к общему количеству шифрованной информации, подлежащей дешифрованию.
	использованием большого числа ключей для шифрования;
	сложностью комбинации символов, выбранных случайным образом;
10	Ниже перечислены механизмы защиты информационных систем от несанкционированного доступа. Что здесь лишнее:
	обеспечения целостности
	идентификация и аутентификация пользователей и субъектов доступа
	управление доступом
	регистрация и учет
	обеспечение постоянного числа пользователей сети
11	Как иначе называется симметричное шифрование:
	шифрование методом Бейтса
	шифрование с переменным ключом.
	шифрование с закрытым ключом
	шифрование с открытым ключом
12	Какое из этих утверждений является верным:
	у S-блоков ГОСТ 8-битовые входы и 4-битовые выходы.
	у S-блоков ГОСТ 4-битовые входы и выходы
	у S-блоков ГОСТ 4-битовые входы и 8-битовые выходы
	нет S-блоков
13	Что означает «многократное шифрование» применительно к блочным шифрам:
	повторное применение алгоритма шифрования к шифротек- сту с другими ключами
	увеличение числа этапов шифрования открытого текста

	повторное применение алгоритма шифрования к шифротек- сту с теми же ключами
	шифрование одного и того же блока открытого текста несколько раз с несколькими ключами
14	Шифрование – это:
	раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства анализа криптосистемы или её входных и выходных сигналов с целью извлечения конфиденциальных параметров, включая открытый текст
	система, реализованная программно, аппаратно или программно - аппаратно и осуществляющая криптографическое преобразование информации
	раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства преобразования информации (шифрования) в целях сокрытия её содержания, предотвращения или несанкционированного использования
	способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого
15	Криптоанализ – это:
	раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства анализа криптосистемы или её входных и выходных сигналов с целью извлечения конфиденциальных параметров, включая открытый текст
	система, реализованная программно, аппаратно или программно - аппаратно и осуществляющая криптографическое преобразование информации
	раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства преобразования информации (шифрования) в целях сокрытия её содержания, предотвращения или несанкционированного использования
	способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого
16	Криптосистема – это:
	раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства анализа криптосистемы или её входных и выходных сигналов с целью
	извлечения конфиденциальных параметров, включая открытый текст
	система, реализованная программно, аппаратно или программно - аппаратно и осуществляющая криптографическое преобразование информации

	раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства преобразования информации (шифрования) в целях сокрытия её содержания, предотвращения или несанкционированного использования
	способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого
17	Что такое алфавит?
	Буквы и символы
	конечное множество используемых для кодирования информации знаков
	Множество знаков одного из языков
	Набор букв русского алфавита
18	Пусть пользователь А хочет передать пользователю Б сообщение m=10, зашифрованное с помощью алгоритма RSA Пользователь Б имеет следующие параметры: P=7, Q=11, d=47 Вычислите значение C зашифрованного сообщения
	C=53
	C=54
	C=55
19	Что в переводе с греческого языка означает слово «криптография»?
	Шифр
	Дешифрование
	Тайнопись
	Тайный шифр
20	Выберите вариант ответа, содержащий только простые числа
	2, 5, 10, 19, 37, 212
	2, 3, 7, 9, 11, 13, 15
	2, 5, 19, 37, 59, 101
	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
21	Для чего предназначен центр сертификации ключей? Выберите *неверный* вариант ответа:
	для регистрации абонентов
	для выделения специальных каналов связи абонентам
	для поддержания в актуальном состоянии справочника действующих сертификатов
	для выпуска списка досрочно отозванных сертификатов
	для изготовления сертификатов открытых ключей
22	Кем было выполнено доказательство существования абсолютно стойких криптографических алгоритмов:
	К. Шенноном
	Б. Паскалем
	Г. Вернамом
	Б. Шнайером

23	Что является целью криптографического преобразования информации:
	защита информации от всех случайных или преднамеренных изменений
	защита информации от случайных помех при передаче и хранении
	сжатие информации
	защита информации от несанкционированного доступа, аутентификация и защита от преднамеренных изменений
24	Как называется шифр, в котором каждый символ открытого текста заменяется некоторым, фиксированным при данном ключе, символом другого алфавита?
	шифром Цезаря
	шифром замены
	шифром одноалфавитной подстановки
	шифром многоалфавитной подстановки
25	Что общего имеют все методы шифрования с закрытым ключом?
	в них для шифрования и расшифрования информации используется один и тот же ключ
	в них производится сложение символов исходного текста и ключа по модулю, равному числу букв в алфавите
	в них для шифрования информации используется один ключ, а для расшифрования – другой ключ
	в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов
26	Алгоритм DES является:
	блочным алгоритмом асимметричного шифрования
	алгоритмом формирования электронной цифровой подписи
	блочным алгоритмом симметричного шифрования
	алгоритмом вычисления функции хеширования
27	Какие операции применяются обычно в современных блочных алгоритмах симметричного шифрования?
	возведение в степень
	замена бит по таблице замен
	перестановка бит
	сложение по модулю 2
	нахождение остатка от деления на большое простое число
28	Как называется однозначное преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины?
	Хеширование
	Гаммирование
	Коллизия
	Сложение по модулю 2
	Перестановка

29	В системе связи, применяющей шифр Эль-Гамаля известны следующие параметры P = 11, A = 3, X1 = 4 Вычислите открытый ключ Y1 В качестве ответа укажите его числовое значение
	12
	4
	8
	3
	2
30	Абоненты некоторой сети применяют цифровую подпись по стандарту ГОСТ Р3410-94 с общими параметрами p = 23, q = 11, a = 9 Найдите открытый ключ абонента Петрова для X = 10 В качестве ответа укажите числовое значение Y
	18
	20
	16
	14
31	Что такое «код»?
	совокупность знаков, а также система правил, позволяющая представлять информацию в виде набора таких знаков
	любой ряд допустимых знаков в соответствии с используемой системой правил
	система записи знаков, позволяющая обнаруживать и корректировать ошибки при хранении и передаче сообщений
	совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты
32	Пусть исходный алфавит содержит следующие символы: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ Зашифруйте с помощью шифра Вижинера и ключа ЯБЛОКО слово ПЕРЕСТАНОВКА
	ОЁЬУЬБЯОЖРХО
	КЕНТЛБЗОЕРЪХЭ
	ОЁЬУЬБЯОЪРХО
	ОЁКИНБЯОЪХРОТ
33	Какова длина хеш-кода, создаваемого алгоритмом ГОСТ 3411-94?
	256 байт
	256 бит
	64 байта
	64 бита
	128 бит
34	Какие существуют алгоритмы генерации псевдослучайных чисел?
	ГОСТ 28147-89
	RC4
	алгоритм с использованием сдвиговых регистров с обратной связью
	DES

35	С помощью обобщенного алгоритма Евклида найдите числа x и y, удовлетворяющие уравнению 21x +12y = НОД(21,12) В качестве ответа запишите через запятую сначала значение x, а затем без пробела – значение y Например, если при вычислениях получилось, что x=-5, а y=2, то ответ надо записать так: -5,2
	-1,2
	1,2
	1,3
	-1,-2
	2, -1
36	Расшифруйте сообщение ЕВВФМШБЫШ, зашифрованное шифром Цезаря, если известно, что исходное сообщение составлено из алфавита АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯОтвет запишите заглавными русскими буквами без пробелов
	СООБЩЕНИЕ
	СООБЩЕСТВО
	ОСВЕЩЕНИЕ
	СОВЕЩАНИЕ
	ПОСВЯЩЕНИЕ
37	Каков размер входного блока обрабатываемой информации при использовании стандарта шифрования AES?
	48 байт
	48 бит
	56 бит
	64 бита
	128 бит
38	Какие факторы влияют на стойкость блочного алгоритма шифрования?
	длина ключа
	количество раундов
	год разработки
	длина сообщения
	используемые операции
39	Алгоритм Диффи-Хеллмана основан на трудности
	решения задачи факторизации
	возведения целых чисел в степень по модулю
	вычисления дискретных логарифмов
	разложения больших чисел на множители
40	Каким требованиям должна удовлетворять электронная цифровая подпись?
	подпись не связывается с конкретным сообщением и может быть перенесена на другой документ

	подпись неразрывно связывается с данным сообщением и не может быть перенесена на другой документ
	подпись воспроизводится только одним лицом, а подлинность ее может быть удостоверена многими
	подпись воспроизводится многими лицами, а ее подлинность может быть удостоверена только одним лицом
41	Выберите верные утверждения
	алгоритм RC4 можно использовать для генерации псевдослучайной ключевой последовательности при поточном шифровании информации
	линейные конгруэнтные генераторы псевдослучайных чисел не рекомендуется использовать для генерации ключевых последовательностей при поточном шифровании
	поточные шифры применяются для формирования электронной цифровой подписи
	алгоритм RC4 можно использовать для формирования хеш-кода
42	Вычислите 39 по модулю 10
	13
	3
	1
	10
	39
	9
43	Определите ключи шифра Цезаря, если известны следующая пара открытый текст – шифротекст: АБРИКОС – ЛМЬФЦЪЭ (исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ)
	11
	12
	10
	9
	8
	7
44	Какие ключи и как должны применяться при использовании асимметричных криптографических алгоритмов для шифрования передаваемых данных?
	отправитель шифрует сообщение своим открытым ключом, а получатель расшифровывает сообщение закрытым ключом отправителя
	отправитель шифрует сообщение открытым ключом получателя, а получатель расшифровывает сообщение своим закрытым ключом
	отправитель шифрует сообщение своим закрытым ключом, а получатель расшифровывает сообщение открытым ключом отправителя
	отправитель шифрует сообщение закрытым ключом получателя, а получатель расшифровывает сообщение своим открытым ключом

45	Для чего используются в криптографии сдвиговые регистры с обратной связью?
	для формирования открытых ключей
	для формирования хеш-кода
	для сжатия информации
	для генерации псевдослучайных чисел
46	На сколько блоков будет разбито сообщение размером 512 байт для шифрования алгоритмом DES? Ответ запишите в виде одного числа
	64
	256
	128
47	Чему равна сумма по модулю 28 двоичных чисел 01011001 и 11111010? Варианты ответов представлены в двоичной системе счисления
	11101100
	01000001
	01010011
	10111010
48	Пусть исходный алфавит состоит из следующих знаков (символ «_» (подчеркивание) будем использовать для пробела): АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_ Расшифруйте сообщение ПРЖВДЪЕ, зашифрованное с помощью таблицы Вижинера и ключа ОРЕХ
	БАБОЧКА
	ЛАСТОЧКА
	БАБУШКА
	БОЧКА
49	Два источника генерируют по два символа Первый источник генерирует символы с равными вероятностями, второй – с различными. Для какого источника количество информации по Шеннону, приходящееся на один символ, будет больше?
	количество информации для рассматриваемых источников одинаково
	недостаточно данных для точного ответа
	для первого
	для второго
50	Определите ключи шифра Цезаря, если известны следующая пара открытый текст – шифротекст: ЯБЛОКО – ЗЙФЧУЧ (исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ)
	11
	7
	9
	3
51	Укажите требования к алгоритмам шифрования с открытым ключом

	вычислительно легко создавать пару (открытый ключ, закрытый ключ)
	вычислительно легко зашифровать сообщение открытым ключом
	вычислительно легко, зная только открытый ключ и зашифрованное сообщение, восстановить исходное сообщение
	вычислительно легко, зная открытый ключ, определить соответствующий закрытый ключ
52	Вычислите 38 по модулю 10
	2
	3
	9
	1
53	Расшифруйте сообщение ИБЛКНАКУ, зашифрованное методом перестановки с фиксированным периодом d=8 с ключом 64275813
	ГЛУБИНКА
	КЛУБНИКА
	БЛАНК
	БУЛКА
54	Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства?
	шифр Цезаря
	шифр Бэбиджа
	шифр Шеннона
	шифр Вижинера
55	Выберите вариант ответа, содержащий только простые числа
	2, 9, 23, 43, 59, 89, 101
	3, 13, 23, 43, 83, 113
	2, 5, 19, 37, 59, 133
	2, 5, 19, 39, 59, 101
56	Пусть пользователь А хочет передать пользователю Б сообщение m=10, зашифрованное с помощью алгоритма RSA Пользователь Б имеет следующие параметры: P=7, Q=17, d=53 Вычислите значение с зашифрованного сообщения:
	c=43
	c=39
	c=41
	c=40
57	Как называется структура в составе большой сети связи, занимающаяся генерированием ключей, их хранением и архивированием, заменой или изъятием из обращения старых и ненужных ключей?
	центр открытого шифрования
	устройство распределения ключей
	центр распределения ключей

	центр закрытого шифрования
58	Как называется функция, которая для строки произвольной длины вычисляет некоторое целое значение или некоторую другую строку фиксированной длины?
	хеш-функция
	функция Эйлера
	односторонняя функция
	функция гаммирования
59	Как называется сообщение, полученное после преобразования с использованием любого шифра?
	Имитовставкой
	Ключом
	закрытым текстом
	открытым текстом
60	Как называется натуральное число, которое делится, помимо самого себя и единицы, еще хотя бы на одно число?
	простое число
	каноническое число
	составное число
	криптографическое число
61	Может ли шифр с конечным ключом быть совершенным?
	Да
	в зависимости от параметров шифра
	Нет
	да, если это алгоритм шифрования с открытым ключом
62	Как называется метод шифрования, в котором входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов?
	шифр замены
	шифр многоалфавитной подстановки
	шифр асимметричного преобразования
	шифр перестановки
63	Какие требования предъявляются в настоящее время к блочным шифрам?
	алгоритм шифрования должен допускать как программную, так и аппаратную реализацию
	в пространстве возможных ключей шифра должно быть не менее 210 «надежных» ключей
	алгоритм шифрования должен содержать не более четырех простейших операций
	знание алгоритма шифрования не должно влиять на надежность защиты

64	Какие операции применяются в шифре, определяемом ГОСТ 28147-89?
	нахождение остатка от деления на большое простое число
	сложение по модулю 2
	циклический сдвиг
	возведение в степень
	замена бит по таблице замен
65	Чем определяется разрядность сдвигового регистра с обратной связью?
	количеством бит, которое может одновременно храниться в регистре сдвига
	температурой окружающей среды
	скоростью работы регистра
	количеством входов в устройстве генерации функции обратной связи
66	Односторонние функции, то есть функции, которые относительно легко вычислить, но практически невозможно найти по значению функции соответствующее значение аргумента, можно использовать для
	формирования хеш-кодов
	контроля и исправления ошибок при передаче информации
	шифрования сообщений
	формирования цифровой подписи
67	Алгоритм основан RSA на трудности
	деления больших целых чисел
	разложения больших чисел на множители
	вычисления дискретных логарифмов
	возведения целых чисел в степень по модулю
68	Зашифруйте методом перестановки с фиксированным периодом d=6 с ключом 436215 сообщение ПЕРЕСТАНОВКА
	КОЛЮЧКА
	ЕРТЕПСВОАНАК
	БАНЕКГШЛОХЪ
	РНГШЛОПАИЛИ
69	Чему равен результат выполнения операции циклического сдвига влево на 5 разрядов для шестнадцатеричного числа 0B5? Варианты ответов представлены в двоичной системе счисления
	10110110
	11101001
	10011011
	01010101
70	Выберите верные утверждения:
	чем больше период последовательности, порождаемой генератором псевдослучайных чисел, тем лучше

	линейные конгруэнтные генераторы псевдослучайных чисел рекомендуется использовать для генерации ключевых последовательностей при поточном шифровании
	поточные шифры применяются для проверки целостности сообщения
	поточные шифры не применяются для формирования электронной цифровой подписи
71	Для решения каких задач может использоваться алгоритм Диффи-Хеллмана?
	формирования общих секретных ключей
	шифрования сообщений
	формирования электронной цифровой подписи
	формирования хеш-значений
72	Расшифруйте сообщение ИЫЛРУДХРТ, зашифрованное шифром Цезаря, если известно, что исходное сообщение составлено из алфавита АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ. Ответ запишите заглавными русскими буквами без пробелов
	БУДИЛЬНИК
	АТМОСФЕРА
	ЛУКОМОРЬЕ
	ВЕДОМОСТЬ
73	Определите ключ в системе шифрования, использующей перестановку с фиксированным периодом d=5 по паре открытых и зашифрованных сообщений: ИНФОРМАЦИЯ – НРФИОАЯЦМИ Ответ запишите в виде последовательности цифр без пробелов
	35214
	25314
	43125
	54213
74	Под целостностью понимают (выберите продолжение)
	гарантирование невозможности несанкционированного изменения порядка следования информации
	гарантирование невозможности несанкционированного изменения переносов в текстовой информации
	гарантирование невозможности несанкционированного изменения объема информации
	гарантирование невозможности несанкционированного изменения информации
75	Выберите вариант ответа, содержащий только взаимно простые числа
	7, 27, 77, 147
	4, 7, 15, 60
	5, 19, 32, 49
	5, 9, 27, 54

76	Как расшифровывается аббревиатура AES?
	Analytic Encryption Standard
	Advanced Encryption Standard
	American Extended Standard
	Advanced Extended Standard
77	Какая наука разрабатывает методы «вскрытия» шифров?
	линейная алгебра
	Криптоанализ
	Криптография
	теория чисел
78	Что такое «избыточность» помехоустойчивого кода?
	число информационных разрядов в кодовом слове
	число разрядов двух кодовых слов, в которых они различны
	характеристика помехоустойчивого кода, показывающая, насколько увеличена длина кодового слова по сравнению с обычным непомехоустойчивым кодом
	наименьшее из всех расстояний по Хэммингу для любых пар различных кодовых слов, образующих код
79	Как называется режим использования блочного шифра, в котором каждый блок исходных данных шифруется независимо от остальных блоков с применением одного и того же ключа шифрования?
	режим формирования электронной цифровой подписи
	режим создания хеш-кода
	режим простой поблочной замены
	режим сцепления блоков шифра
80	Как называется распределенный алгоритм, определяющий последовательность действий каждой из сторон?
	Протокол
	электронная цифровая подпись
	процесс шифрования
	хэш-функция
81	Определите наибольший общий делитель чисел 187 и 264
	13
	11
	9
	7
82	Определите наибольший общий делитель чисел 146 и 182
	6
	4
	2
	12
83	Определите наибольший общий делитель чисел 293 и 47
	47
	1

	13
	7
84	Определите наибольший общий делитель чисел 139 и 278
	1
	2
	139
	278
85	Под конфиденциальностью понимают (выберите продолжение):
	решение проблемы защиты информации от ее изменения со стороны лиц, не имеющих права доступа к ней
	решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, имеющих права доступа к ней
	решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней
	решение проблемы запуска программ со стороны лиц, не имеющих права доступа к ним
86	В чем заключается общая идея эффективного кодирования методом Хаффмана?
	из всех возможных кодовых слов считаются допустимыми не все, а лишь некоторые
	символам с меньшей вероятностью присваиваются более короткие коды, тогда как чаще встречающимся символам – более длинные
	символам с большей вероятностью присваиваются более короткие коды, тогда как реже встречающимся символам – более длинные
	производится замена цепочек или серий повторяющихся байтов на один кодирующий байт-заполнитель и счетчик числа их повторений
87	Какой способ реализации криптографических методов обладает максимальной скоростью обработки данных?
	Программный
	Электромеханический
	Аппаратный
	Ручной
88	Для решения каких задач можно использовать алгоритмы шифрования с открытым ключом?
	для распределения секретных ключей, используемых потом при шифровании документов симметричными методами
	для формирования цифровой подписи под электронными документами
	для помехоустойчивого кодирования передаваемых сообщений
	для шифрования передаваемых и хранимых данных в целях их защиты от несанкционированного доступа
89	Определите число натуральных чисел, не превосходящих 33 и взаимно простых с 33
	15

	14
	20
	1
90	Известно, что для некоторого источника сообщений количество информации по Хартли, приходящееся на 1 символ, равно 5 битам Чему равно количество символов в алфавите источника сообщений?
	32
	64
	128
	256
91	Что такое «минимальное кодовое расстояние»?
	число контрольных разрядов в кодовом слове
	число разрядов двух кодовых слов, в которых они различны
	наименьшее из всех расстояний по Хэммингу для любых пар различных кодовых слов, образующих код
	характеристика помехоустойчивого кода, показывающая, насколько увеличена длина кодового слова по сравнению с обычным непомехоустойчивым кодом
92	Что называют открытым ключом в асимметричных методах шифрования?
	ключ, который не обязательно хранить в секрете
	ключ, который должен храниться в секрете
	ключ, который используется для выработки имитовставки
	любой ключ, используемый для шифрования или расшифрования
93	Определите число натуральных чисел, не превосходящих 59 и, взаимно простых с 59
	27
	16
	58
	3
94	Определите наибольший общий делитель чисел 64 и 89
	1
	2
	32
	4
	12
95	Определите наибольший общий делитель чисел 325 и 208
	2

	11
	13
	55
96	С точки зрения криптографии, энтропия сообщения определяет …
	длину сообщения
	максимальное количество бит информации, которое может быть передано одним символом рассматриваемого языка, при условии, что все последовательности символов равновероятны
	количество символов, которые необходимо раскрыть, чтобы узнать содержание сообщения
	количество информации, приходящееся на один символ сообщения
97	Какой язык обладает минимальной избыточностью сообщений?
	Язык, в котором все символы равновероятны и могут встречаться в сообщениях независимо друг от друга в любом порядке
	Язык, в котором только два символа
	Язык, в котором как можно больше символов
	Язык, в котором некоторые символы гораздо вероятнее других
98	Длина ключа в алгоритме AES составляет
	64 байта
	56 байт
	Длина ключа может быть переменной в зависимости от используемого количества раундов
	256 бит
99	Какая операция наиболее быстро выполняется при программной реализации алгоритмов шифрования?
	возведения в степень
	нахождения остатка от деления на большое простое число
	вычисления дискретных логарифмов
	сложения по модулю 2
100	Расшифруйте сообщение ЖКИЛШЪОБМ, зашифрованное шифром Цезаря, если известно, что исходное сообщение составлено из алфавита АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ. Ответ запишите заглавными русскими буквами без пробелов
	КРИПТОГРАФИЯ
	КОМПЬЮТЕР
	КЛАВИАТУРА
	ОСВЕЩЕНИЕ

Задания в открытой форме

1) … - раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства преобразования информации (шифрования) в целях сокрытия её содержания, предотвращения или несанкционированного использования.

2) … - система, реализованная программно, аппаратно или программно - аппаратно и осуществляющая криптографическое преобразование информации.

3) … - раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства анализа криптосистемы или её входных и выходных сигналов с целью извлечения конфиденциальных параметров, включая открытый текст.

4) Если группа состоит из конечного числа элементов, то она называется ...

5) Если в качестве групповой операции используется операция сложения, то группа называется ...

6) Два цикла называются …, если перемещаемые ими элементы попарно различны.

7) Кольцо называется …, если оно является коммутативным кольцом с единицей и без делителей нуля.

8) Свойство устойчивости криптосистемы к криптоанализу называется ...

9) Симметричная криптосистема называется …, если апостериорное распределение вероятностей исходного случайного сообщения X при регистрации случайного шивротекста $Y=f(X;\theta(0))$ совпадает с априорным распределением вероятностей.

10) Всякое иррациональное a разлагается в бесконечную цепную …

11) Поле называется алгебраически …, если любой многочлен в разлагается на линейные множители.

12) … — множество, элементами которого являются все возможные упорядоченные пары элементов исходных множеств.

13) … — мультипликативная арифметическая функция, значение которой равно количеству натуральных чисел, не превышающих n и взаимно простых с ним.

14) … позволяет определить, является ли данное целое число квадратичным вычетом по модулю простого числа.

15) … – это мера хаоса в какой-либо системе.

16) ... двух множеств — множество, элементами которого являются все возможные упорядоченные пары элементов исходных множеств.

17) … — эффективный алгоритм для нахождения наибольшего общего делителя двух целых чисел (или общей меры двух отрезков). Алгоритм назван в честь греческого математика.

18) Представление любого множества A в виде объединения непустых и попарно непересекающихся подмножеств называется ....

19) нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре.… — документ, содержащий требования безопасности для конкретной разработки, выполнение которых обеспечивает достижение поставленных целей безопасности.

20) … шифрование –один из способов защиты отчастотной криптоатаки.

Задание на установление соответствия

1. Установить соответствие:

1) Криптосистема	a) Раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства анализа криптосистемы или её входных и выходных сигналов с целью извлечения конфиденциальных параметров, включая открытый текст;
2) Криптоанализ	b) Система, реализованная программно, аппаратно или программно - аппаратно и осуществляющая криптографическое преобразование информации;
3) Криптография	c) Раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства преобразования информации (шифрования) в целях сокрытия её содержания, предотвращения или несанкционированного использования.

2. Установить соответствие длины ключа:

1) AES	a) 256 бит
2) DES	b) Переменная
3) ГОСТ 28147-89	c) 56 бит

3. Установить соответствие:

1) Чему равен результат выполнения побитовой операции «сумма по модулю 2» для двоичных чисел 10101100 и 11001010?	a) 01000101
2) Чему равен результат выполнения	b) 10100011

побитовой операции «сумма по модулю 2» для десятичных чисел 250 и 191?	
3) Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 9E и 0A3?	c) 00111101

4. Установить соответствие:

1) Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 0B5 и 37?	a) 10000010
2) Чему равна сумма по модулю 28 двоичных чисел 10101100 и 11001010?	b) 01110110
3) Чему равна сумма по модулю 28 двоичных чисел 01011001 и 11111010?	c) 01010011

5. Установить соответствие:

1) Чему равна сумма по модулю 28 десятичных чисел 250 и 191?	a) 10111001
2) Чему равна сумма по модулю 28 шестнадцатеричных чисел 9E и 0A3?	b) 01000001
3) Чему равна сумма по модулю 28 шестнадцатеричных чисел 0B5 и 37?	c) 11101100

6. Установить соответствие:

1) Чему равен результат выполнения операции циклического сдвига влево на 5 разрядов для двоичного числа 10101100?	a) 10010101
2) Чему равен результат выполнения операции циклического сдвига вправо на 5 разрядов для двоичного числа 01011001?	b) 11001010
3) Чему равен результат выполнения операции циклического сдвига влево на 5 разрядов для	c) 10110110

шестнадцатеричного числа 0B5?	

7. Установить соответствие:

1) Чему равен результат выполнения операции циклического сдвига влево на 7 разрядов для одного байта, хранящего шестнадцатеричное значение 37?	a) 10011011
2) Чему равен результат выполнения операции циклического сдвига вправо на 2 разряда для одного байта, хранящего шестнадцатеричное значение 55?	b) 01010101
3) 11) Чему равна сумма по модулю 28 шестнадцатеричных чисел 9E и 0A3?	c) 01000001

8. Установить соответствие:

1) Угроза безопасности	a) Это некая неудачная характеристика системы, которая делает возможным возникновение угрозы.
2) Уязвимость	b) Это угроза раскрытия информации.
3) Атака	c) Это потенциально возможное происшествие, которое может оказать воздействие на информацию в системе.
4) Угроза конфиденциальности	d) Это действие по использованию уязвимости; реализация угрозы.

9. Установить соответствие:

1) Линейная структура процесса вычислений	a) Предполагает, что для получения результата некоторые действия необходимо выполнить несколько раз.
2) Разветвленная структура процесса вычислений	b) Предполагает, что конкретная последовательность операций зависит от значений одной или нескольких переменных.
3) Циклическая структура	c) Предполагает, что для получения результата необходимо выполнить

процесса вычислений	некоторые операции в определенной последовательности.

10. Установить соответствие:

1) Правильность	a) Возможность проверки получаемых результатов;
2) Универсальность	b) Обеспечение полной повторяемости результатов, т. Е. Обеспечение их правильности при наличии различного рода сбоев;
3) Надежность	c) Обеспечение правильной работы при любых допустимых данных и защиты от неправильных данных;
4) Проверяемость	d) Функционирование в соответствии с техническим заданием;

11. Установить соответствие:

1) Точность результатов	a) Возможность совместного функционирования с некоторым оборудованием
2) Защищенность	b) Возможность совместного функционирования с другим программным обеспечением
3) Программная совместимость	c) Обеспечение конфиденциальности инф ормации;
4) Аппаратная совместимость	d) Обеспечение погрешности результатов не выше заданной;

12. Установить соответствие средства обеспечения информационной безопасности:

1) Организационные	a) Сюда входит весь перечень программного обеспечения, который поможет обеспечить должную информационную безопасность ресурса
2) Программные	b) Сюда входят сами приборы и устройства, которые обеспечивают защиту информации.

3) Аппаратные	c) Сюда входят: обеспечение качественного помещения для размещения серверов, качественное оборудование, продуманная кабельная система, организация правового статуса ресурса или компании и др.

13. Установить соответствие:

1) Угроза целостности	a) Это вероятный ущерб, который зависит от защищенности системы.
2) Угроза доступности	b) Это стоимость потерь, которые понесет компания в случае реализации угрозы конфиденциальности, целостности или доступности по каждому виду ценной информации.
3) Ущерб	c) Это угроза нарушения работоспособности системы при доступе к информации.
4) Риск	d) Это угроза изменения информации.

14. Установить соответствие:

1) Шифр	a) Это любой знак, в том числе буква, цифра или знак препинания.
2) Символ	b) Совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты.
3) Алфавит	c) Конечное множество используемых для кодирования информации символов.

15. Установить соответствие:

1) Ключ	a) Можно использовать для обратимого изменения текста сообщения с целью сделать его непонятным для всех, кроме тех, кому оно предназначено.
2) Шифрсистема	b) Информация, необходимая для шифрования и расшифрования сообщений.
3) Криптостойкость	c) Характеристика шифра, определяющая его защиту к дешифрованию без знания ключа.

16. Установить соответствие:

1) Шифр замены	a) Группа методов шифрования подстановкой, в которых для замены символов исходного текста используется не один, а несколько алфавитов по определенному правилу.
2) Шифр многоалфавитной замены	b) Основан на том, что символы исходного текста, обычно разделенные на блоки и записанные в одном алфавите, заменяются одним или несколькими символами другого алфавита в соответствии с принятым правилом преобразования.
3) Шифр перестановки	c) Основан на том, что входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов.
4) Шифр простой (или одноалфавитной) замены	d) Группа методов шифрования, которые сводятся к созданию по определённому алгоритму таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква шифртекста.

17. Установить соответствие:

1) DES	a) Один из режимов использования блочного алгоритма шифрования.
2) ECB	b) Является блочным алгоритмом симметричного шифрования..
3) CBC	c) Режим сцепления блоков шифра.
4) BBS	d) Один из методов генерации псевдослучайных чисел.

18. Установить соответствие:

5) LFSR	a) Линейный сдвиговый регистр с обратной связью.
6) CTR	b) Режим работы блочного шифра, который позволяет генерировать ключи при поточном шифрования информации.
7) RC4	c) Алгоритм генерации псевдослучайных чисел.

19. Установить соответствие:

1) Шифр одноалфавитной подстановки	a) Каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите;
2) Шифр многоалфавитной подстановки	b) Метод шифрования, в котором входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов;
3) Шифр перестановки	c) Каждый символ открытого текста заменяется некоторым, фиксированным при данном ключе, символом другого алфавита.
4) Шифр Цезаря	d) Это совокупность шифров простой замены, которые используются для шифрования очередного символа открытого текста согласно некоторому правилу.

20. Установить соответствие:

1) Чему равен результат выполнения операции циклического сдвига влево на 5 разрядов для шестнадцатеричного числа 0B5?	a) 10011011
2) Чему равен результат выполнения операции циклического сдвига влево на 5 разрядов для двоичного числа 10101100?	b) 10010101
3) Чему равен результат выполнения операции циклического сдвига влево на 7 разрядов для одного байта, хранящего шестнадцатеричное значение 37?	c) 10110110

Задание на установление правильной последовательности

1. Установить этапы построения программы обеспечения безопасности:

1) Формирование политики безопасности организации
2) Проведение разъяснительных мероприятий и обучения персонала для поддержки требуемых мер безопасности
3) Регулярный контроль пошаговой реализации плана безопасности
4) Установление уровня безопасности
5) Определение ценности технологических и информационных активов организации

2. Выберите правильную последовательность этапов защиты информации:

1) Анализ рисков для активов организации, включающий в себя выявление ценных активов и оценку возможных последствий реализации атак с использованием скрытых каналов
2) Реализация защитных мер по противодействию скрытых каналов
3) Организация контроля за противодействием скрытых каналов.
4) Выявление скрытых каналов и оценка их опасности для активов организации

3. Выберите правильную последовательность этапов процесса управления рисками:

1) Идентификация активов и ценности ресурсов, нуждающихся в защите;
2) Анализ угроз и их последствий, определение слабостей в защите;

3) Классификация рисков, выбор методологии оценки рисков и проведение оценки;

4) Выбор, реализация и проверка защитных мер;

5) Оценка остаточного риска;

6) Выбор анализируемых объектов и степени детальности их рассмотрения;

4. Выберите последовательность проведения моделирования угроз:

1) Определение негативных последствий от угроз безопасности информации.

2) Определение объектов воздействия угроз безопасности информации.

3) Оценка возможности реализации угроз и их актуальности.

5. Установите этапы процессной модели:

1) Проверка.

2) Планирование.

3) Реализация

4) Действие.

6. Установите последовательность этапов:

1) Характеризуется внедрением электромеханических устройств в работу шифровальщиков. При этом продолжалось использование полиалфавитных шифров.

2) Период перехода к математической криптографии.

3) Характеризуется господством моноалфавитных шифров (основной принцип – замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами).

4) Ознаменовался введением в обиход полиалфавитных шифров.

5) Отличается зарождением и развитием нового направления – криптография с открытым ключом.

7. Установите последовательность этапов:

1) Наивная криптография..

2) Формальная криптография.

3) Научная криптография.

4) Компьютерная криптография.

8. Установите последовательность этапов шифрования текста методом «атбаш»:

1) Выделить каждую букву исходного текста;

2) Определить номер буквы, шифрующей каждую букву исходного текста, учитывая особенность метода;

3) Определить букву алфавита с номером;

4) Определить её номер в алфавите;

9. Установите последовательность этапов шифрования алгоритмом Цезаря:

1) Выделить каждую букву исходного текста;

2) Определить её номер в алфавите;

3) Определить номер буквы, шифрующей каждую букву исходного текста, учитывая величину сдвига;

4) Определить букву алфавита с номером, полученным на этапе..

10. Установите последовательность этапов шифрования алгоритмом Виженера:

1) Выделить каждую букву исходного текста;

2) Определить её номер в алфавите;

3) Выделить каждую букву ключа шифрования;

4) Сопоставить её соответствующей букве исходного текста;

11. Установите последовательность этапов шифрования алгоритмом Виженера:

1) Определить номер каждой буквы ключа шифрования в алфавите;

2) Определить номер буквы, шифрующей каждую букву исходного текста;

3) Определить букву алфавита с номером, полученным на этапе…

12. Установите последовательность этапов алгоритма шифрования с использованием кодов:

1) Выделяются отдельные буквы шифруемого текста;

2) Для каждой выделенной буквы:определяется её код;

3) Для каждой выделенной буквы:определяется код шифрующей её букву (учитывая правила шифрования);

4) Для каждой выделенной буквы:определяется буква с полученным кодом

13. Установите последовательность этапов:

1) Найти НОД для чисел 28 и 64.

2) Находим произведение одинаковых простых множителей и записываем ответ; Разложим на простые множители данные числа;

3) Подчеркиваем одинаковые простые множители в обоих числах.

14. Установите последовательность этапов:

1) Выбор ключа к длиной м символов.

2) Символы исходного текста последовательно замещаются символами, выбираемыми из тш по следующему правилу:

3) Определяется символ km ключа к, соответствующий замещаемому символу sor;

4) Находится строка i в тш, для которой выполняется условие km=bi1;

5) Определяется столбец j, для которого выполняется условие: sor=b1j;

6) Символ sor замещается символом bij.

7) Под каждым символом s0r исходного текста длиной i символов размещается символ ключа km. Ключ повторяется необходимое число раз.

8) Построение матрицы шифрования tш,=(bij) размерностью [(m+1), r] для выбранного ключа к.

9) Полученная зашифрованная последовательность разбивается на блоки определенной длины, например, по четыре символа. Последний блок дополняется, при необходимости, служебными символами до полного объема.

15. Установить последовательность этапов:

1) Доработка прототипа системы
2) Проверка системы
3) Получение законченной системы
4) Разработка прототипа системы
5) Разработка обобщённой спецификации
6) Использование прототипа системы

16. Установить порядок этапов компьютерного моделирования:

1) Постановка задачи.
2) Компьютерный эксперимент.
3) Анализ результатов моделирования.
4) Разработка модели.

17. Установить этапы разработки:

1) Проектирование
2) Реализация
3) Внедрение
4) Анализ и планирование требований пользователей

18. Установите последовательность процедуры создания ключей:

1) Вычисляется функция Эйлера;

Выбираются два простых числа;

2) Выбирается открытый ключ, как произволное число взаимно простое к функции Эйлера;

3) Вычисляется секретный ключ d, как обратное число к открытому ключу по модулю функции Эйлера;

4) Публикуется открытый ключ.

5) Вычисляется произведение простых чисел;

19. Установите последовательность этапов процедуры опознавания с использованием простого пароля:

1) система запрашивает пароль;

2) пользователь посылает запрос на доступ к компьютерной системе

и вводит свой идентификатор;

3) пользователь вводит пароль;

4) система сравнивает полученный пароль с паролем пользователя, хранящимся в базе эталонных данных системы защиты, и разрешает доступ, если пароли совпадают; в противном случае пользователь к ресурсам компьютерной системы не допускается.

20. Установите последовательность этапов стеганографии:

1) Выбор информационного файла;

2) Отправление сокрытого сообщения по электронной почте и его декодирование;

3) Выбор файла-контейнера

4) Кодирование файла;

5) Выбор стеганографической программы.

Шкала оценивания результатов тестирования: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 баллов (установлено положением П 02.016).

Максимальный балл за тестирование представляет собой разность двух чисел: максимального балла по промежуточной аттестации для данной формы обучения (36) и максимального балла за решение компетентностно-ориентированной задачи (6).

Балл, полученный обучающимся за тестирование, суммируется с баллом, выставленным ему за решение компетентностно-ориентированной задачи.

Общий балл по промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

2.2КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

1. Решить сравнение 2160x≡807(mod1317)
2. Решить систему сравнений:

x ≡ 13 mod (18)

x ≡ 19 mod (29)

x ≡ 12 mod (17)

3. Найти НОД 57824 и 2151 и его разложение.
4. Решить сравнение, используя подходящие дроби: 9x≡12(mod21)
5. Составить таблицу индексов по модулю 78.
6. Решить сравнение 1287x ≡ 447 (mod 516)
7. Решить сравнение: x^35= 17(mod67).
8. Пусть исходный алфавит содержит следующие символы:

АБВГДЕВЖЗИЙКЛМНОПРСТУФХИЧШЩЬЫЬЭЮЯ.

Зашифруйте с помощью шифра Вижинера и ключа ЯБЛОКО слово ПОДСТАНОВКА.

9. Решить сравнение 221x ≡ 111 (mod 360)
10. Решить сравнение 143x ≡ 41 (mod 221)

11. Определите ключи шифра Цезаря, если известны следующая пара

открытый текст — шифротекст: ВИНОГРАД — ШЯДЕЩЖЦЪ (исходный алфавит: АБВГДЕЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ)

12. Решить сравнение 113x ≡ 89 (mod 311)
13. Решить сравнение 37x ≡ 25 (mod 117)
14. Пусть исходный алфавит состоит из следующих знаков (символ

«_» (подчеркивание) будем использовать для пробела):

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦУЧШЩЪЫЬЭЮЯ_ Расшифруйте сообщение 'ЪРОЕШШОФФВП, зашифрованное с помощью таблицы Вижинера и ключа ОРЕХ.

15. Решить сравнение 85x ≡ 149 (mod 172)

16. Решить сравнение 255x ≡ 447 (mod 516)

17. Чему равна сумма по модулю 28 шестнадцатеричных чисел 9E и 0A3?

18. Решить сравнение 1287x ≡ 447 (mod 516)

19. Решить сравнение 14x≡7 (mod 101)

20. Пусть хеш-функция y=h(x1x2…xn) определяется как результат выполнения побитовой операции «сумма по модулю 2» для всех байтов сообщения, представленного в двоичном виде Длина хеш-кода равна 8 битам Для каждого из шести сообщений, записанных в левом столбце, найдите соответствующий результат вычисления хеш-функции из правого столбца Все сообщения и значения хеш-функции представлены в шестнадцатеричном формате

а) 34 0A9 0B6

б) 32 7F 0B3

в) 1A 0B4 96

г) 0D2 0C1 0B2

д) 0E4 36 29

е) 21 0AE 54

Шкала оценивания решения компетентностно-ориентированной задачи: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 (установлено положением П 02.016).

Максимальное количество баллов за решение компетентностно-ориентированной задачи – 6 баллов.

Балл, полученный обучающимся за решение компетентностно-ориентированной задачи, суммируется с баллом, выставленным ему по результатам тестирования. Общий балл промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

Критерии оценивания решения компетентностно-ориентированной задачи (нижеследующие критерии оценки являются примерными и могут корректироваться):

6-5 баллов выставляется обучающемуся, если решение задачи демонстрирует глубокое понимание обучающимся предложенной проблемы и разностороннее ее рассмотрение; свободно конструируемая работа представляет собой логичное, ясное и при этом краткое, точное описание хода решения задачи (последовательности (или выполнения) необходимых трудовых действий) и формулировку доказанного, правильного вывода (ответа); при этом обучающимся предложено несколько вариантов решения или оригинальное, нестандартное решение (или наиболее эффективное, или наиболее рациональное, или оптимальное, или единственно правильное решение); задача решена в установленное преподавателем время или с опережением времени.

4-3 балла выставляется обучающемуся, если решение задачи демонстрирует понимание обучающимся предложенной проблемы; задача решена типовым способом в установленное преподавателем время; имеют место общие фразы и (или) несущественные недочеты в описании хода решения и (или) вывода (ответа).

2-1 балла выставляется обучающемуся, если решение задачи демонстрирует поверхностное понимание обучающимся предложенной проблемы; осуществлена попытка шаблонного решения задачи, но при ее решении допущены ошибки и (или) превышено установленное преподавателем время.

0 баллов выставляется обучающемуся, если решение задачи демонстрирует непонимание обучающимся предложенной проблемы, и (или) значительное место занимают общие фразы и голословные рассуждения, и (или) задача не решена.