МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ЛИПЕЦКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ П.П. СЕМЕНОВА-ТЯН-ШАНСКОГО»
(ЛГПУ имени П.П. Семенова-Тян-Шанского)

УТВЕРЖДАЮ
Врио ректора ФГБОУ ВО
«ЛГПУ имени П.П. Семенова-Тян-Шанского»
_____ Д.В. КРЕТОВ
«27» октября 2022 г.

ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ ПРИ ПРИЕМЕ НА ОБУЧЕНИЕ ПО ПРОГРАММАМ МАГИСТРАТУРЫ

Направление подготовки

10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Магистерская программа

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ ПРИ РАССЛЕДОВАНИИ ИНЦИДЕНТОВ

Липецк – 2022

I ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа вступительных испытаний составлена в соответствии с примерными программами, разработанными на основе обязательного минимума требования владения компетенций по информатике, вычислительной технике и сетям передачи данных (для естественнонаучных, технических и технологических направлений подготовки).

В содержание программы входят основные разделы по дисциплине, вынесенные на вступительное испытание.

Цель программы – выявление уровня знаний, умений, навыков лиц, поступающих в ФГБОУ ВО «Липецкий государственный педагогический университет имени П.П. Семенова-Тян-Шанского» (ЛГПУ имени П.П. Семенова-Тян-Шанского). На базе перечисляемых в разделах программы дидактических единиц осуществляется подбор экзаменационных заданий.

Экзамен по информатике и методике преподавания информатики в ЛГПУ имени П.П. Семенова-Тян-Шанского, является вступительным испытанием, направленным на выявление уровня форсированности мышления кандидатов и владения соответствующими умениями и навыками, которые необходимы для успешного освоения различных курсов, включенных в программы подготовки профильной магистратуры в ЛГПУ имени П.П. Семенова-Тян-Шанского. Вступительный экзамен проводится в письменной форме.

Объем знаний и степень владения материалом, описанным в программе, соответствуют базовым вузовским курам информатики и методики преподавания информатики. Для ответа по экзаменационным вопросам кандидату достаточно уверенно владеть теоретическим материалом тем, перечисленных в настоящей программе. Поступающие могут использовать материал, не изучаемый в высших учебных заведениях, но при условии, что они способны его пояснять и применять на практике.

Экзамен проводятся для граждан, имеющих высшее образование (диплом бакалавра, специалиста, магистра), соответствующее профилю магистерской программы, или меняющих профиль предыдущего образования.

I. СОДЕРЖАНИЕ ПРОГРАММЫ

Содержание программы представлено в виде перечисленных ниже вопросов из следующих дисциплин: информатика и информационные технологии, алгебра логики, операционные системы, методика преподавания информатики и другим дисциплинам.

Экзамен проводится письменно. Письменный экзамен проводится в виде тестирования. Для определения качества знаний, используются тестовые задания как закрытого (предлагается выбрать правильный ответ из нескольких возможных), так и открытого типа (написать свой вариант ответа).

Тест содержит 25 заданий и оценивается по стобалльной шкале. Таким образом, каждое правильно выполненное задание позволяет получить до 4 баллов. Минимальный положительный балл –40.

Программа письменного экзамена

1. Информация. Источники информации и ее носители. Количество информации и энтропия. Формулы Хартли и Шеннона. Информация как основа прогресса. Информация как товар. Информация как предмет защиты.
2. Сообщения, сигналы. Типы сигналов, спектральный анализ сигналов. Дискретизация и восстановление сигналов. Частота Найквиста, теорема Котельникова.
3. Характеристики процесса передачи информации. Математические модели каналов связи и их классификация. Помехоустойчивость передачи информации. Пропускная способность каналов связи. Теорема Шеннона для каналов без помех и с ними.
4. Сущность и понятие информационной безопасности. Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества. Структура информационной безопасности. Определение понятия «информационная безопасность».
5. Сущность и понятие защиты информации. Виды защиты информации. Понятие угрозы безопасности информации. Уязвимость информационной системы. Политика информационной безопасности.
6. Государственная система органов РФ для обеспечения информационной безопасности и защиты информации. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации.
7. Современные подходы к составу защищаемой информации. Основа для отнесения информации к защищаемой, категории информации, подпадающие под эту основу. Понятия «конфиденциальная информация», «секретная информация», «открытая информация».
8. Критерии, условия и принципы отнесения информации к защищаемой. Состав и классификация носителей защищаемой информации. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.
9. Становление и развитие системы защиты информации в Российском государстве в XV-середине XX вв. Эволюция органов защиты информации в этот период. Изменение состава и классификации защищаемой информации.
10. Становление и развитие систем защиты информации в ведущих зарубежных странах. Государственная политика в области защиты информации в США. Организация защиты информации в Великобритании.
11. Информация как объект права. Отрасли права, обеспечивающие правовое регулирование в сфере защиты информации и охраны интеллектуальной собственности. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации»: основные положения.
12. Правовые основы защиты государственной тайны. Законодательные и иные нормативно-правовые акты РФ, регулирующие защиту государственной тайны. Закон РФ «О государственной тайне»: основные положения.

13. Порядок распоряжения сведениями, составляющими государственную тайну. Обеспечение защиты государственной тайны, органы защиты. Закон РФ «О безопасности». Уголовно-правовая ответственность за разглашение информации, составляющей государственную тайну.
14. Правовые основы защиты коммерческой тайны. Федеральный закон РФ «О коммерческой тайне». Гражданский кодекс РФ и иные источники права о порядке защиты коммерческой тайны. Охрана коммерческой тайны в трудовых отношениях.
15. Правовые основы защиты банковской тайны. Источники права о банковской тайне. Объекты и субъекты права на банковскую тайну. Способы защиты владельцем банковской тайны своих прав.
16. Правовые основы защиты персональных данных в РФ. Федеральный закон РФ «О персональных данных». Подзаконные документы, определяющие меры защиты персональных данных в РФ. Общий регламент по защите данных (General Data Protection Regulation) от 25 мая 2016 года..
17. Правовые основы защиты информации в государственных информационных системах. Признаки отнесения информационных систем к государственным. Ведомственные нормативно-правовые акты, определяющие меры обеспечения защиты информации в государственных информационных системах.
18. Правовые основы лицензирования и сертификации в области защиты информации в РФ. Органы, уполномоченные на ведение лицензионной деятельности и их полномочия.
19. Институт правовой защиты авторских и смежных прав в РФ. Участие России в международных соглашениях по защите авторских и смежных прав. Развитие патентного права в России. Характеристика объектов патентного права. Оформление патентных прав.
20. Безопасность критической информационной инфраструктуры Российской Федерации. Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры. Принципы обеспечения безопасности критической информационной инфраструктуры.
21. Преступления, связанные с компьютерной информацией. Природа контрафакции программного обеспечения. Судебная практика рассмотрения дел о преступлениях в области информационно-телекоммуникационных систем и сетей связи.
22. Формирование структурного подразделения по защите информации в организации. Основные задачи и функции. Состав и структура подразделения. Обязанности сотрудников структурного подразделения по защите информации.
23. Порядок отнесения сведений, составляющих государственную тайну, к различным степеням секретности. Присвоение грифа секретности работам, документам и изделиям. Понятие «рассекречивание сведений».
24. Понятие «допуск к секретной информации». Формы допусков, их назначение и классификация. Процедура допуска, подлежащего согласованию с органами государственной безопасности.

25. Понятие «допуск к конфиденциальной информации». Условия правомерного доступа. Особенности доступа к конфиденциальной информации различных категорий персонала. Обязанности лиц, допущенных к защищаемым сведениям.
26. Понятие «пропускной режим». Цели и задачи пропускного режима. Организация пропускного режима. Порядок оформления и выдачи пропусков. Понятие «внутриобъектовый режим».
27. Физические поля как носители информации об объектах. Физические параметры полей. Измерение характеристик физических полей.
28. Элементы акустики речи и акустики помещений. Частотно-динамический диапазон восприятия звука ухом. Уровень громкости, логарифмические единицы. Особенности акустики закрытых помещений. Звукоизоляция помещений.
29. Распространение радиоволн в земной атмосфере. Пространственные и поверхностные радиоволны. Диапазоны радиоволн. Законодательство в области использования радиочастотного диапазона.
30. Виды носителей информации. Способы записи информации на различные виды носителей. Виды модуляции сигналов. Характеристики модулированных сигналов.
31. Принципы и средства радиосвязи. Антенны и их характеристики. Фидеры: назначение, основные характеристики. Передающие устройства, принципы их построения и основные характеристики. Приемные устройства.
32. Системы двухпроводной телефонной связи. Телефонная сеть. Офисные АТС. Радиотелефоны, их частотные диапазоны. Системы сотовой связи. Спутниковая связь. Качественные показатели каналов спутниковой связи.
33. Радиорелейные линии. Принципы радиорелейной связи. Приемопередающая аппаратура. Волоконно-оптическая связь, ее преимущества и недостатки. Космическая связь. Лазерная связь.
34. Цифровые системы связи, особенности их построения. Иерархия цифровых систем связи. Синхронная цифровая иерархия.
35. Понятие об опасных сигналах и их источниках. Основные и вспомогательные технические средства и системы. Принципы высокочастотного навязывания. Паразитная генерация усилителей.
36. Оптические системы и приборы. Основные понятия оптоэлектроники. Фотодиоды и фототранзисторы. Оптроны. Интегральная оптика. ИК-техника.
37. Способы и средства наблюдения. Структура и основные характеристики средств наблюдения. Добывание информации с помощью визуально-оптических и фотографических средств. Принципы конструкции и работы, виды и характеристики фотоаппаратуры.
38. Оптические каналы утечки информации. Основные принципы оптико-электронной разведки. Характеристика телевизионной и инфракрасной разведок. Структура средств телевизионного наблюдения и регистрации.
39. Радиоэлектронные каналы утечки информации. Классификация и характеристики помех в радиоэлектронных каналах утечки информации. Способы и

средства предотвращения утечки информации с помощью радиозакладных устройств.

40. Акустоэлектрические приборы (микрофоны). Электроакустические преобразователи (динамики), свойство обратимости. Усилители: основные виды и характеристики. Принципы построения.
41. Побочные электромагнитные излучения и наводки (ПЭМИН). Способы и средства предотвращения утечки информации через ПЭМИН. Средства активного линейного и пространственного зашумления.
42. Источники питания электронной аппаратуры. Выпрямители. Принципы построения. Стабилизаторы. Утечка информации по цепям заземления. Требования к заземлению и конструкция заземлителей.
43. Генераторы. Генераторы синусоидальных сигналов. Стабилизация частоты. Побочные гармоники. Импульсные генераторы. Утечка информации через генераторы.
44. Акустические каналы утечки информации. Структура акустического канала утечки информации. Способы и средства информационного и энергетического скрытия акустических сигналов и речевой информации. Скремблеры. Вокодеры.
45. Материально-вещественные каналы утечки информации. Способы утечки демаскирующих веществ в твердом, жидком и газообразном виде. Принципы ведения радиационной и химической разведок.
46. Концепция охраны объектов. Типовая структура системы охраны. Системы автономной и централизованной охраны. Работа бюро пропусков на предприятии. Контрольно-пропускные пункты.
47. Способы и средства инженерной защиты объектов. Типовые инженерные конструкции. Естественные и искусственные преграды. Металлические шкафы, сейфы и хранилища.
48. Системы сбора, обработки и отображения информации (ССОИ). Классификация ССОИ. Радиоволновые и радиолучевые средства обнаружения. Оптические, сейсмические, магнитометрические и комбинированные средства обнаружения.
49. Требования к проектированию систем пожарной сигнализации. Пожарные приемно-контрольные приборы, приборы управления и извещатели. Требования к монтажу и приемо-сдаточным испытаниям систем охранно-пожарной сигнализации.
50. Системы и средства контроля и управления доступом (СКУД). Периферийное оборудование и носители информации СКУД. Средства идентификации и аутентификации. Функциональные возможности СКУД.
51. Способы и средства видеоконтроля. Телевизионные камеры, их классификация, принципы работы и основные характеристики. Мониторы, коммутаторы, квадраторы, мультиплексоры, регистраторы. Принципы построения систем видеоконтроля.
52. Теоретико-числовые основы криптографии. Множество. Бинарные отношения. Множество натуральных чисел. Упорядоченные и частично упорядоченные множества.

53. Теоретико-числовые основы криптографии. Кольца: идеалы колец, прямые суммы колец. Кольцо целых чисел. Кольцо матриц над полем, определитель и ранг матрицы.
54. Теоретико-числовые основы криптографии. Простые числа. «Основная» теорема арифметики. Свойства простых чисел. Теорема Эйлера. Асимптотический закон распределения простых чисел. Взаимно простые числа.
55. История развития криптографии. Основные понятия криптографии. Определение шифра, понятие криптографической стойкости. Основные требования к шифрам.
56. Шифры перестановки. Шифры простой замены. Система шифрования Цезаря. Шифрующая таблица Трисемуса. Шифры сложной замены. Система шифрования Гронсфельда. Система шифрования Вижинера.
57. Криптосистемы с открытым ключом. Шифр Эль-Гамаля. Шифр Мак-Элиса.
58. Математические вычисления, используемые в ассиметричных алгоритмах. Стандарт ассиметричного шифрования RSA. Стойкость алгоритма RSA.
59. Понятие электронной цифровой подписи. Стандарты на электронную цифровую подпись. Электронная подпись на базе шифра Эль-Гамаля. Закон РФ «Об электронной цифровой подписи». Процессы формирования и проверки электронной цифровой подписи по ГОСТ Р 34.10-2001.
60. Хэш-функции. Хэш-функция по Secure Hash Algorithm (SHA-1). Отечественный стандарт хеш-функции ГОСТ Р 34.11-94. Стойкость хэш-функций.
61. Блочные системы шифрования. Американский стандарт шифрования данных DES, его свойства и режимы использования. Стандарт шифрования данных AES.
62. Блочные системы шифрования. Стандарт шифрования данных ГОСТ 28147-89.
63. Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов.
64. Протоколы распределения ключей. Протоколы передачи ключей с использованием симметричного и ассиметричного шифрования. Открытое и предварительное распределение ключей. Протокол «Station-To-Station». Протокол «Керберос». Протокол обмена зашифрованными ключами EKE.
65. Протоколы идентификации. Парольная идентификация. Криптографические протоколы идентификации. Протоколы с нулевым разглашением.
66. Угрозы и задачи информационной безопасности для локальных рабочих станций. Методы и средства защиты современных операционных систем на локальных рабочих станциях. Дискреционная и мандатная политика безопасности.
67. Защита информации в UNIX-системах. Протоколы локальной и сетевой аутентификации, избирательное разграничение доступа на основе векторов, децентрализованный аудит.
68. Защита информации в Windows NT/2000/XP/7/8/8.1/10. Протоколы локальной и сетевой аутентификации, избирательное разграничение доступа на основе списков, централизованный аудит в пределах компьютера.

69. Защита информации в сетях ЭВМ. Классификация сетевых атак. Атаки, направленные на отказ в обслуживании. Несанкционированный перехват и навязывание сетевого трафика, несанкционированное изменение путей маршрутизации.
70. Безопасность локальных компьютерных сетей: основные протоколы, службы, функционирование, средства обеспечения безопасности, управления и контроля. Утечка конфиденциальной информации через Интернет.
71. Туннелирование сетевого трафика и виртуальные частные сети (VPN). Политики безопасности в VPN. Стандартные протоколы создания VPN.
72. Требования к продуктам построения виртуальных частных сетей. VPN-решения компании «Инфотекс». Администрирование системы защиты информации ViPNet.
73. Межсетевые экраны, их достоинства и недостатки. Пакетные фильтры. Шлюзы сеансового уровня и уровня приложений. Использование межсетевых экранов.
74. История вредоносных программ. Понятие компьютерных вирусов, их классификация. Средства борьбы с вирусными атаками. Антивирусные программы.
75. Защита электронной почты: принципы, средства, протоколы. Настройка защиты электронной почты. Защита в архитектуре X.400. Защита от спама.
76. Социальная инженерия как сфера научно-практической деятельности: возможности и границы применения. Методики социальной инженерии. Примеры взломов с помощью методов социальной инженерии.
77. Средства защиты информации от несанкционированного доступа. Виды, классы, сертификация средств защиты информации от НСД. Принципы функционирования СЗИ от НСД. Условия применения.

III. ПРИМЕРЫ ТЕСТОВЫХ ЗАДАНИЙ

1. Что не относится к сведениям конфиденциального характера?

1. Персональные данные
2. Сведения о сущности изобретения
3. Сведения, составляющие тайну следствия
4. Сведения о задолженности работодателей по выплате заработной платы и социальным выплатам

2. Какое средство защиты информации создано для осуществления контроля и фильтрации проходящего через него сетевого трафика?

1. Антивирус
2. Межсетевой экран
3. Система обнаружения вторжений
4. Система мониторинга событий информационной безопасности

3. Какие три основные свойства информации достигаются с помощью защиты информации?

1. Актуальность, достоверность, защищенность
2. Отчуждаемость, правильность, упругость
3. Конфиденциальность, целостность, доступность

4. Нет правильного ответа

4. Когда применяются алгоритмы шифрования информации

1. Когда мы не доверяем месту, где храним информацию
2. Когда мы не доверяем каналам связи, по которым передаем информацию
3. Когда нам требуется подтверждения подлинности отправителя
4. Во всех перечисленных случаях

5. Тебе пришло письмо от неизвестного отправителя с неизвестным содержимым. Что будешь делать с ним?

1. Открою и посмотрю содержимое
2. Перешлю системному администратору
3. Посмотрю и сразу удалю
4. Передам ответственному специалисту за защиту информации

6. Основными видами электронных подписей, которые регулируются федеральным законом, являются …

1. простая электронная подпись;
2. неквалифицированная электронная подпись;
3. квалифицированная электронная подпись.
4. Усложненная электронная подпись

7. Электронные и механические устройства, предназначенные для инженерно-технической защиты информации и противодействия шпионажу, относятся к _____ средствам защиты.

1. Аппаратным
2. Программным
3. Программно-аппаратным
4. Организационным

8. В соответствии с Указом Президента Российской Федерации № 212 от 19.02.99 г., межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную и служебную тайну, осуществляет

1. ФСБ России
2. УМВД России
3. ФСТЭК России
4. Правительство России

9. Установите соответствие между способами перехвата информации и их сущностью.

1. Активный перехват
2. Аудиоперехват
3. Пассивный перехват

А - подключение к телекоммуникационному оборудованию компьютера, например линии принтера или телефонному проводу канала связи, либо непосредственно через соответствующий порт персонального компьютера

Б - фиксация электромагнитных излучений, возникающих при функционировании многих средств компьютерной техники, включая и средства коммуникации

В - установка подслушивающего устройства в аппаратуру средств обработки информации

10 Разработчик первого алгоритма с открытыми ключами:

1. Ади Шамир
2. Росс Андерсон
3. Брюс Шнайер
4. Мартин Хеллман

11. Алгоритм, основанный на сложности разложения больших чисел на два исходных простых сомножителя:

1. ECC
2. RSA
3. DES
4. Диффи-Хеллман

12. Выберите то, как связаны ключи друг с другом в системе с открытым ключом:

1. математически
2. логически
3. алгоритмически
4. геометрически

13. Злоумышленнику Ивану стал известен хэш-образ пароля пользователя для входа секретную систему. Для того, чтобы узнать правильный пароль он решил перебрать все возможные пароли, вычислить от них хэш и сравнить с известным. Сколько потребуется времени Ивану, если известно, что время проверки одного пароля – 10 секунд, максимальная длина пароля составляет 7 символов и используется алфавит, состоящий из 20 букв.

14. Какой из перечисленных простейших криптографических или математических алгоритмов реализован в коде ниже?

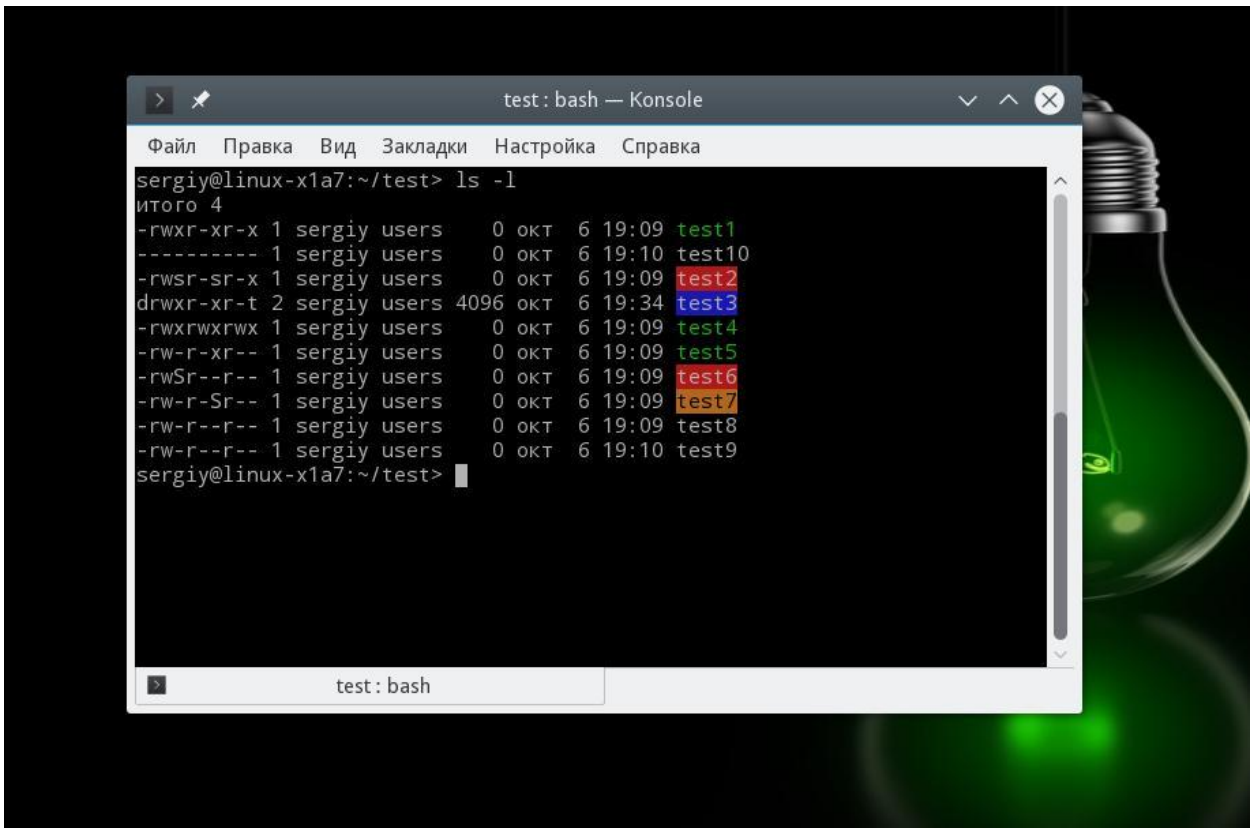
C

```c
#include <stdio.h>
int main(){
    int a, b, p=1, q=0, r=0, s=1, x, y;
    scanf("%d %d",&a,&b);
    while (a && b) {
        if (a>=b) {
            a = a - b;
            p = p - r;
            q = q - s;
```

```
            } else
            {
                b = b - a;
                r = r - p;
                s = s - q;
            }
        }
        if (a) {
            x = p;
            y = q;
        }else
        {
            x = r;
            y = s;
        }
        printf("%d %d\n",x,y);
        return 0;
}
```

1. Алгоритм Диффи-Хеллмана;
2. Побитовое XOR шифрование;
3. Аффинный шифр;
4. Расширенный алгоритм Евклида.

15 Выберите номера верных утверждений проанализировав следующее изображение.



Варианты ответов:

1. Объект test5 является папкой, групповым пользователям которой разрешена запись;
2. Объект test1 является файлом, владельцу которого разрешено чтение, запись и исполнение;
3. Объект test8 является папкой, которую разрешено читать всем остальным;
4. Объект test4 является файлом, который не разрешено редактировать ни одной из категорий.

16. «FeNix» - студенческая команда программистов, постоянные участники олимпиад и хакатонов. Однажды, на почту их капитана пришло письмо следующего содержания:

«Здравствуйте! Мы долго наблюдали за вашими успехами и решили предложить вам вступить в наше сообщество. Мы находим самых талантливых молодых людей, помогаем развить свои способности и использовать их во благо. Нам кажется, что вы могли бы стать членами нашего сообщества, но сначала вы должны доказать, что мы в вас не ошиблись.

«Ргкселхз тсорсз лпв тсонсесжщг, тусфогелеызёс ахсх ылчу»

Ответьте на вопрос, зашифрованный в данном сообщении. При формулировке ответа воспользуйтесь помощью нашего вдохновителя – Гронсфельда. Поговаривали, его любимое число было 1268»

Вопросы:

1. Какой вопрос зашифрован в сообщении?
2. В какой форме отправитель ждет ответа на свое сообщение?

Теоретический материал. Шифр Цезаря. «Шифр (от французского chiffre – «цифра» и арабского слова sifr – «ноль») представляет собой систему преобразования текста, обладающую некоторым секретом (ключом) для обеспечения секретности передаваемой информации. В основе данного шифра лежала замена каждой буквы исходного текста на другую букву того же алфавита, со сдвигом на фиксированное количество позиций.
Представляет собой модификацию шифра Цезаря числовым ключом. Для этого под буквами исходного сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифртекст получают примерно, как в шифре Цезаря, но отсчитывают по алфавиту не третью букву (как это делается в шифре Цезаря), а выбирают ту букву, которая смещена по алфавиту на соответствующую цифру ключа. Например, применяя в качестве ключа группу из четырех начальных цифр числа e (основания натуральных логарифмов), а именно 2718, получаем для исходного сообщения ВОСТОЧНЫЙ ЭКСПРЕСС следующий шифртекст

IV. ПОРЯДОК ПРОВЕДЕНИЯ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

В определенное расписанием время абитуриенты должны занять места в назначенной аудитории, для чего с собой необходимо иметь: паспорт, экзаменационный лист, 2 ручки (синие или черные), непрограммируемый калькулятор, линейку, карандаш. После размещения всех допущенных к вступительным испытаниям представитель экзаменационной комиссии объясняет правила оформления ответа и раздает листы с экзаменационными заданиями. С этого момента начинается отсчет времени. Продолжительность вступительных испытаний 2 астрономических часа (60 минут). По окончании отведенного времени абитуриенты должны начинать ответы представителям экзаменационной комиссии, после ответа выйти из аудитории.

V. СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

ОСНОВНАЯ

1. Алферов А.П. и др. Основы криптографии. – М.: Гелиос АРВ, 2001. – 480 с.
2. Белов Е.Б. и др. Основы информационной безопасности. – М.: Горячая линия – Телеком, 2006. – 544 с.
3. Буйневич М.В., Доценко С.М., Малыш В.Н. Информационная безопасность и защита информации в компьютерных системах: Учебное пособие. – Липецк: ЛГПУ, 2007. – 255 с.
4. Введение в криптографию [Электронный ресурс]: . — Электрон. дан. — М. : МЦНМО (Московский центр непрерывного математического образования), 2012. — 348 с. — Режим доступа: http://e.lanbook.com/ books/element.php?pl1_id=71813
5. Журавлева Л.В. Радиоэлектроника: Учебник. – М.: Академия, 2005.
6. Куприянов А.И. и др. Основы защиты информации: Учебное пособие. – М.: Академия, 2006. – 256 с.

7. Курило, А.П. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1 [Электронный ресурс] : учебное пособие / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов [и др.]. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 244 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5178
8. Лопатин В.Н. Правовые основы информационной безопасности: Курс лекций. – М.: МИФИ, 2000.
9. Малыш В.Н., Осинин В.Ф. Теория информации: Учебное пособие. – Липецк: ЛГПУ, 2004. – 73 с.
10. Малюк, А.А. Введение в информационную безопасность [Электронный ресурс] : учебное пособие / А.А. Малюк, В.С. Горбатов, В.И. Королев. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 288 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5171
11. Молдовян А.А. Криптография. – СПб.: Лань, 2001. – 224 с.
12. Основы информационной безопасности. Курс лекций: Учебное пособие. – М.: ИНТУИТ.РУ, 2006. – 208 с.
13. Рябко, Б.Я. Основы современной криптографии и стеганографии. [Электронный ресурс] : монография / Б.Я. Рябко, А.Н. Фионов. – Электрон. дан. – М. : Горячая линия-Телеком, 2011. — 232 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5192
14. Системы радиосвязи: Учебник / Под ред. Н.И.Калашникова. – М.: Радио и связь, 1988. – 352 с.
15. Скуднев Д.М. Сети и системы передачи информации. Защита информации в сетях связи : учебно- методическое - Липецк: ЛГПУ, 2015. - 176 с.
16. Торокин А.А. Инженерно-техническая защита информации. М.: Гелиос АРВ, 2005. – 960 с.
17. Ярочкин В.И. Информационная безопасность: Учебник. – М.: Трикста, 2005. – 544 с.

ДОПОЛНИТЕЛЬНАЯ

1. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие. – М.: Горячая линия – Телеком, 2004. – 280 с.
2. Бобровников Л.З. Радиотехника и электроника: Учебник. – М.: Недра, 1990. – 374 с.
3. Виноградов И.М. Основы теории чисел. – М.: Наука, 1981.
4. Виртуальные защищенные сети ViPNet. Курс лекций: Учебное пособие. – М.: Прометей, 2008. – 172 с.
5. Волков Л.Н., Немировский М.С., Шинаков Ю.С. Системы цифровой радиосвязи: базовые методы и характеристики. – М.: Эко-Трендз, 2005. – 390 с.
6. Жельников В. Криптография от папируса до компьютера. – М.: ABF, 1997. – 336с.

7. Запечников С.В. и др. Основы построения виртуальных частных сетей: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2003. – 249 с.
8. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. – М.: Гелиос АРВ, 2005. – 192 с.
9. Зюко А.Г., Кловский Д.Д., Коржик В.И., Назаров М.В. Теория электрической связи. – М.: Радио и связь, 1999.
10. Крис Касперски Компьютерные вирусы изнутри и снаружи. – СПб.: Питер, 2006.
11. Кузнецов М., Симдянов И. Социальная инженерия и социальные хакеры. – С-Пб.: БХВ-Петербург, 2007. – 358 с.
12. Курош А.Г. Лекции по общей алгебре: Учебник. – М.: Лань, 2007.
13. Магауенов Р.Г. Системы охранной сигнализации: основы теории и принципы построения. – М.: Горячая линия-Телеком, 2004. – 367 с.
14. Маховенко Е.Б. Теоретико-числовые методы в криптографии. – М.: Гелиос АРВ, 2006. – 320 с.
15. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки. – М.: РГГУ, 2002. – 399 с.
16. Методика информационной безопасности: Монография. – М.: Экзамен, 2004. – 544 с.
17. Палий А.И. Радиоэлектронная борьба. – М.: Воениздат, 1981.
18. Программно-аппаратные средства обеспечения информационнойц безопасности. Защита программ и данных: Учеб. пособие для вузов, П.Ю. Белкин, О.О.Михальский, А.С.Першаков и др. – М.: Радио и связь, 2000. – 168с.
19. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Защита в операционных системах: Учеб. пособие для вузов. – М.: Радио и связь, 2000. – 168с.
20. Разбирин С.А. Информационная безопасность фирмы. Организационно-правовой аспект. – Липецк: ЛЭГИ, 2000. – 180 с.
21. Романец Ю.В. и др. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001. – 376 с.
22. Савельев И.В. Курс общей физики. – М.: Наука, 1996-1999.
23. Соболев А.Н., Кириллов В.М. Физические основы технических средств обеспечения информационной безопасности: Учебное пособие. – М.: Гелиос АРВ, 2004. – 224 с.
24. Собурь С.В. Установки пожарной сигнализации. – М.: Спецтехника, 2002.–312с.
25. Технические средства разведки / Под ред. В.И.Мухина. – М.: РСВН, 1992.
26. Убайдулаев Р.Р. Волоконно-оптические сети. – М.: Эко-Трендз, 2000. – 270 с.

ДОПОЛНИТЕЛЬНАЯ

1. ГОСТ Р 50922 – 2006. Защита информации. Основные термины и определения.

2. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
3. ГОСТ Р 34.10-2001 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой под-писи.
4. ГОСТ Р 34.11-94 Информационная технология. Криптографическая защита ин-формации. Функция хэширования.
5. Гражданский кодекс Российской Федерации (ГК РФ) (части первая, вторая, тре-тья и четвертая) (с изменениями и дополнениями).
6. Закон РФ от 27.12.1991 N 2124-1 (ред. от 03.07.2016) "О средствах массовой информации" (с изм. и доп., вступ. в силу с 15.07.2016).
7. Закон РФ от 11.03.1992 N 2487-1 (ред. от 03.07.2016) "О частной детективной и охранной деятельности в Российской Федерации"
8. Федеральный закон от 28.12.2010 N 390-ФЗ (ред. от 05.10.2015) "О безопасно-сти"
9. Конституция РФ.
10. Постановление Правительства РФ от 07.05.2006 N 276 (ред. от 15.05.2010) "Об упорядочении функций федеральных органов исполнительной власти в области авторского права и смежных прав"
11. Уголовный кодекс Российской Федерации.
12. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г.
13. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 03.07.2016) "О персональ-ных данных"
14. Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 23.06.2016) "Об электронной подписи"
15. Федеральный закон от 22.10.2004 N 125-ФЗ (ред. от 23.05.2016) "Об архивном деле в Российской Федерации"
16. Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) "О коммерческой тайне"