Перелік програмних питань
з дисциплін, які виносяться на фахове вступне випробування

" ПРИКЛАДНА КРИПТОЛОГІЯ "

1. Шифрування та кодування.
2. Стеганографія та криптографія.
3. Алгоритми та протоколи.
4. Шифрування методом Цезаря.
5. Зламування методу Цезаря.
6. Криптостійкість шифрів
7. Шифрування методом простої підстановки.
8. Статистичні властивості мови. Зламування методу простої підстановки.
9. Поліалфавітні шифри (Гронсфельда, Тритеніуса, Віженера).
10. Зламування методу Віженера.
11. Криптостійкість ключів.
12. Перестановочні шифри. Статистичні властивості криптограм перестановок.
13. Шифри збивання. Лінійні перетворення.
14. Одноразові блокноти. Формування випадкової псевдопослідовності.
15. Комбінація шифрів. Стандарт шифрування DES
16. Асиметрична криптографія.
17. Метод Райвеста-Шамира-Адлемана (RSA).
18. Методи генерації простих чисел
19. Перевірка чисел на взаємну простоту (розширений алгоритм Евкліда).
20. Знаходження секретного ключа (рівняння Діофанта).
21. Шифрування методом RSA (дискретне піднесення до степеня).
22. Розшифровування криптограм RSA.
23. Дискретне логарифмування.
24. Метод ель-Гамаля.
25. Розшифровування криптограм ель-Гамаля.
26. Аутентифікація користувача. Цифровий підпис
27. Забезпечення цілісності інформації. Алгоритми Хешування .
28. Забезпечення доступності інформації. Протоколи обміну паролями.
29. Класифікація криптографічних методів.
30. Практичне застосування криптографічних методів. Відомі програмні та апартні продукти криптографічного захисту інформації.

" ТЕОРІЯ ІНФОРМАЦІЇ ТА КОДУВАННЯ "

1. Визначення інформації. Інформація і дані.
2. Кількісна міра інформації.
3. Ефективне або статистичне кодування.
4. Загальні відомості про технологію кодування. Технологія кодування чисел.
5. Технологія кодування інформаційних об’єктів.
6. Вимірювання інформації.

7. Задачі забезпечення цілісності і доступності інформаційних об’єктів у обчислювальних мережах.

8. Механізми контролю і відновлення цілісності в базових кодових словах при дії природних впливів.

9. Механізми контролю і відновлення цілісності в базових кодових словах при дії штучних впливів.

10. Методи захисту від помилок.

11. Принципи побудови завадостійких кодів.

12. Принципи побудови коду Хеммінга.

13. Алгоритми кодування-декодування з використанням коду Хеммінга.

14. Узагальнені завадостійкі коди.

15. Контрольне підсумовування.

16. Принципи побудови згорточного коду.

17. Принципи виявлення групових викривлень при застосуванні згорточного коду.

18. Методи захисту від викривлень з використанням передачі із зворотним зв’язком.

19. СПД із ВЗЗ з очікуванням (стартостопний метод передачі).

20. СПД із ВЗЗ з послідовним (потоковим) методом передачі.

21. СПД із ВЗЗ з адресним перезапитом комбінацій (вибіркова передача).

22. Порівняння СПД із ВЗЗ і систем передачі з використанням корегуючих кодів. Порівняння по відносній швидкості передачі.

23. Порівняння систем передачі із ВЗЗ і систем передачі з використанням корегуючих кодів. Порівняння систем передачі по вірності передачі даних.

24. Метод перемежування, виграш від кодування.

25. Типова система передачі даних.

26. Основні відомості про телекомунікаційні системи. Канали, що комутуються, і виділені канали зв’язку.

27. Комутація в мережах. Комутація ланцюгів.

28. Комутація в мережах. Комутація каналів на основі частотного мультиплексування.

29. Комутація в мережах. Комутація каналів на основі розподілу часу.

30. Комутація в мережах. Принципи кодового поділу каналів зв’язку.

"ОСНОВИ ТЕОРІЇ КІЛ, СИГНАЛІВ ТА ПРОЦЕСІВ В ЕЛЕКТРОНІЦІ"

1. Спектральний аналіз періодичних сигналів. Періодичні сигнали і ряди Фур’є. Спектри амплітуд і фаз.

2. Спектр періодичної послідовності прямокутних відео імпульсів.

3. Спектральний аналіз періодичних сигналів. Комплексна форма ряду Фур’є. Поняття негативної частоти.

4. Спектральний аналіз періодичної послідовності радіоімпульсів.

5. Спектральний аналіз неперіодичних сигналів. Спектральна щільність аналогових сигналів. Пари перетворень Фур’є.

6. Спектральний аналіз неперіодичних сигналів. Умови існування спектральної щільності сигналу.

7. Спектральний аналіз неперіодичних сигналів. Основні властивості перетворення Фур'є.

8. Спектральна щільність одиночних (уніполярних) сигналів. Зв'язок між тривалістю імпульсу і шириною його спектра.

9. Спектральна щільність одиночних (уніполярних) сигналів. Спектральна щільність сигналів, що неінтегруються.

10. Спектральна щільність одиночних (уніполярних) сигналів. Спектральна щільність постійного в часі сигналу.

11. Модульовані сигнали. Амплітудна модуляція. Спектр однотональних АМ коливань.

12. Модульовані сигнали. Багатотональна АМ.

13. Модульовані сигнали. Фазова модуляція.

14. Модульовані сигнали. Частотна модуляція.

15. Спектральний аналіз дискретних сигналів. Базис речовинний мнимих функцій (ВМФ).

16. Спектральний аналіз дискретних сигналів. Фільтруючі властивості дискретного перетворення Фур'є.

17. Спектральний аналіз дискретних сигналів. Амплитудно -фазові характеристики частотних каналів процесора дискретного перетворення Фур'є.

18. Сигнали з обмеженим спектром. Ідеальний низькочастотний сигнал. Ортогональні сигнали з обмеженим спектром.

19. Теорема Котєльнікова. Побудова ортонормованого базису.

20. Ряд Котєльнікова. Принципова важливість ряду Котєльнікова.

21. Автокореляційна функція сигналу. Автокореляційна функція прямокутного відео імпульсу.

22. Автокореляційна функція сигналу. Автокореляційна функція прямокутного радіо імпульсу.

23. Зв'язок між енергетичним спектром сигналу і його автокореляційною характеристикою.

24. Фізичні системи і їхні математичні моделі. Системні оператори. Стаціонарні і нестаціонарні системи. Лінійні і нелінійні системи.

25. Імпульсні і частотні характеристики лінійних стаціонарних систем.

26. Імпульсна перехідна характеристика. Інтеграл Дюамеля.

27. Умови фізичної реализуємості імпульсної характеристики лінійної системи.

28. Частотний коефіцієнт передавання (КП) лінійної системи.

29. Проходження сигналу через лінійні кола. Спектральний метод аналізу електричного кола. Основний принцип спектрального методу.

30. Проходження сигналу через лінійні кола. Алгоритм розрахунку реакції кола для періодичних сигналів.

" ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ "

1. Назвіть основні типи протоколів.
2. Опишіть принципи роботи мостів.

3. Назвіть основні етапи віддаленого доступу.
4. Опишіть принцип роботи мостів з прозорою комутацією.
5. Назвіть основні рівні моделі OSI.
6. Опишіть принципи роботи мостів з комутацією від джерела.
7. Назвіть основні властивості локальних мереж.
8. Накресліть і опишіть топологію «шина».
9. Назвіть основні властивості глобальних мереж.
10. Накресліть і опишіть топологію «зірка».
11. Назвіть основні алгоритми маршрутизації.
12. Опишіть технологію Frame Relay.
13. Назвіть основні протоколи мережного рівня.
14. Опишіть принципи роботи маршрутизатора.
15. Назвіть основні види фізичного кодування.
16. Опишіть принципи роботи комутаторів.
17. Назвіть основні види логічного кодування.
18. Опишіть принципи роботи комутаторів 3-го рівня.
19. Назвіть основні протоколи прикладного рівня.
20. Опишіть переваги цифрового зв'язку.
21. Назвіть основні протоколи транспортного рівня.
22. Опишіть набір протоколів X.25.
23. Назвіть основні рівні TCP/IP .
24. Назвіть основні характеристики Token Ring.
25. Назвіть основні характеристики Fast Ethernet.
26. Опишіть основні властивості коаксіального кабелю.
27. Назвіть основні характеристики Gigabit Ethernet.
28. Опишіть основні властивості витої пари.
29. Назвіть основні режими роботи плати мережного адаптера.
30. Опишіть принципи роботи повторювачів.

" АРХІТЕКТУРА КОМП'ЮТЕРНИХ СИСТЕМ "

1. Визначення персонального комп'ютера і його основні складові частини. Конструктивний устрій ПК.
2. Системні ресурси персонального комп'ютера.
3. Адресний простір ПК. Модель розподілу пам'яті. Додаткова, відображувана і розширена пам'ять.
4. Прямий доступ до пам'яті. Канали прямого доступу до пам'яті і пряме керування шиною.
5. Розподіл системних ресурсів. Поняття Plug and Play.
6. Апаратні і програмні переривання. Джерела переривань і їхня обробка.
7. Системний порт IBM PC. Системний таймер. Канал керування звуком. Інтерфейс клавіатури. Батарейна пам'ять і годинник CM0S.
8. Процедура P0ST і базова система введення-виведення. Розширення базової системи введення-виведення.
9. Системна плата. Основні типи конструктива і порядок установки. Підключення компонентів до материнської плати.

10.Установка і конфігурування оперативної пам'яті і процесора.

11.Логіка керування системною платою. Поняття чипсета, його функції і структура.

12.Південний і північний міст. Розподіл функцій: керування системною платою; визначення характеристик пристроїв; організація інтерфейсу.

13.Вибір системної плати. Перелік основних характеристик. Основні елементи архітектури.

14.Поняття однокристального процесора. Основні типи корпусів. Способи установки процесора на плату.

15.Процесор i8086. Організація пам'яті, регістри процесора.

16.Процесор i80286. Реальний і захищений режим роботи.

17. Описати основні характеристики процесорів

18.Фізичні і логічні основи збереження інформації. Види пам'яті і їхні основні характеристики.

19.Статична і динамічна пам'ять. Синхронний і асинхронний режими роботи, основні типи пам'яті і їхніх характеристик.

20.Поняття шин розширення і їхня коротка характеристика.

21.Шина PCI-E, її параметри. Основні сигнали шини.

22.Шина PCI. Протокол обміну по шині PCI.

23.Описати архітектури системної плати

24.Інтерфейс AGP. Фактори підвищення продуктивності функціонування шини.

25.Відеосистема. Фізичні основи візуалізації інформації. Принципи виводу зображення.

26.Відеосистема. Графічний режим. Текстовий режим. 2-D і 3-D акселератори.

27.Відеосистема. Типи графічних адаптерів.

28.Принципи довгострокового збереження інформації. Типи накопичувачів інформації.

29.Фізична і логічна організація жорстких дисків.

30.Основні інтерфейси жорстких дисків та їх характеристики.

Список літератури
для самостійної підготовки вступника до
фахового вступного випробування з дисципліни
" ПРИКЛАДНА КРИПТОЛОГІЯ "

Основна література

1.Б. Шнайер Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: Изд-во ТРИУМФ.2002. - 816 с.

2.Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. - М.: Гелиос АРВ, 2001. - 480 с.

3.Анохин М. И., Варновский Н. П., Сидельников В. М., Ященко В. В. Криптография в банковском деле. - М.:МГУ, 1997.

4.Чмора АЛ. Современная прикладная криптография. - М.:Гелиос АРВ,

2001.-256 с.

5. Аграновский А.В., Хади Р.А. Практическая криптография: алгоритмы и их программирование. - М.:СОЛОН-Пресс, 2002. - 256 с.

6. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. - М.:КУДИЦ-ОБРАЗ, 2003.-240 с.

7. В.Г. Грибунин, Н.Н. Оков, И.В. Туринцев Цифровая стеганография. - М.: СОЛОН-Пресс, 2002. -272 с.

8. В.К. Задірака, О.С. Олексюк Комп'ютерна криптологія:підручник. - Київ:2002. - 504 с.

9. Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. Основи комп'ютерної стеганографії. Навчальний посібник. - Вінниця: ВДТУ, 2003. -143 с.

10. Домашев А.В. и др. Программирование алгоритмов защиты информации. Учебное пособие. - М.: "Нолидж", 2000. - 288 с.

11. В.Мельников Защита информации в компьютерных системах. М.:"Финансы и статистика", 1997. – 368 с.

Додаткова література

1. Довідкова система операційної системи Windows 2000.

2. В.К. Задірака, О.С. Олексюк Комп'ютерна арифметика багаторозрядних чисел: Наукове видання. - Київ:2003. - 264 с.

3. Введение в криптографию / Под общ. ред. В.В. Ященко.- 2-е изд., испр. - М.:МЦНМО:"ЧеРо", 1999.-271 с.

4. В. Жельников Криптография от папируса до компьютера. - М.:АВР, 1996.-336 с.

5. Фаль О.М. Криптографія: основні ідеї та застосування: Преапринт. - К.: ІВЦ "Видавництво "Політехніка"", 2003. - 28 с.

6. Саломаа А. Криптография с открытым ключом / Пер. с англ. - М.: Мир, 1996.-318 с.

Список літератури
для самостійної підготовки вступника до
фахового вступного випробування з дисципліни
" ТЕОРІЯ ІНФОРМАЦІЇ ТА КОДУВАННЯ "

Основна література

1. Василенко В.С., Юдін О.К. Теорія інформації і кодування в захищених інформаційно − телекомунікаційних системах та мережах: -К., НАУ: Електронна версія конспекту лекцій з дисципліні „Теорія інформації”

2. Стратонович Р. Л.: - М.: “Сов. радио”, 1975, - 424с.

3. Файнштейн А. Основы теории информации. Пер. з англ.: - М.: “Наука”, 1997, - 317 с.: іл.

4. Колмогоров А.Н. Теория информации и алгоритмов: - М.: “Наука”, 1987. – 304 с.: іл.

5. Хемминг Р.В. Теория кодирования и теория информации. Пер. з англ.: - М.: “Наука”, 1983. – 240 с.

6. Тарасенко Ф.П. Введение в курс теории информации – Томск: Вид. ТДУ, 1963. – 397 с.
7. Дмитриев В.В. Прикладная теория информации: - М.: “Высш. школа”, 1998. − 320 с.

Додаткова література

8. Кузьмин И.В., Кедрус В.А. Основы теории информации и кодирования. Учебное пособие для вузов.: -К.: Вища школа, 1987.
9. Методичні рекомендації по виконанню курсової роботи з дисципліни Теорія інформації для студентів факультету Інформаційної безпеки за напрямом 1601 “Інформаційна безпека”, К., ДАУ, 2005

Список літератури
для самостійної підготовки вступника до
фахового вступного випробування з дисципліни
"ОСНОВИ ТЕОРІЇ КІЛ, СИГНАЛІВ ТА ПРОЦЕСІВ В ЕЛЕКТРОНІЦІ"

Основна література

1. Карташов Р.П., Медведев А.П. Теория электрорадиоцепей. Под ред. А. М.Широкова, М.: Воениздат МО СССР. 1980 г.
2. Лосев А.К, Теория линейных электрических цепей. Учебник для Вузов. – М. Высшая школа. 1987 г.
3. Белецкий А.Ф. Теория линейных электрических цепей. –М. „Радио и связь”, 1986 г.
4. Атабеков Г.И. Теоретические основы электротехники, ч.1. Линейные электрические цепи. – М.: Энергия, 1978 г.
5. Попов П.А. Расчет частотных электрических фильтров. – М. Энергия, 1966 г.
6. Гоноровский И.С. Радиотехнические цепи и сигналы. Учебник для Вузов. - М.: Радио и связь, 1986 г.
7. Баскаков С.І..- Радиотехнические цепи и сигналы. Учебник для Вузов М.: Высшая школа, 1983. г.
8. Зернов Н.В. Карпов В.Г. Теория радиотехнических цепей. – Л. „Энергия” 1972 г.

Додаткова література

9. Ланне А.А. Оптимальный синтез линейных электрических цепей . – М.: Связь, 1969 г.
10. Матханов П.Н. Основы анализа электрических цепей. Линейные цепи . -М.: Высшая школа, 1981г.
11. Зааль Р. Справочник по расчету фильтров / Перевод. Под ред. Слепова Н.Н. – М.: Радио и связь, 1983.

Список літератури
для самостійної підготовки вступника до
фахового вступного випробування з дисципліни
" ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ "

Основна література

1. Буров Є. Комп‘терні мережі. Львів: БаК, 1999. – 468 с., (004.7 Б91)
2. Майкл Дж. Мартин. Введение в сетевые технологии, издательство «Лори», 2002 – 659 с. (004.7 М29)
3. Олифер В.Г., Олифер Н.А.. Новые технологии IP-сетей. – СПб.: БХВ-Петербург, 2001. – 512 с. (004,7 О-54)
4. Microsoft Windows 2000 Prefessional. Учебный курс MCSE: Пер. с англ. – 2-е изд. перераб. – М.: Издательство-торговый дом «Русская Редакции», 2001. – 672 стр. (004.45 М59)
5. Microsoft Windows 2000 Server. Учебный курс MCSE: Пер. с англ. – 2-е изд. перераб. – М.: Издательство-торговый дом «Русская Редакции», 2001. – 912 стр. (004.45 М59)
6. Комп‘ютерні мережі:Навч. посіб. / Зайченко Ю.П. – К., Слово, 2003. – 286с.,
7. Комп‘ютерні мережі: Підруч. для ВНЗ / Кулаков Ю.О. – К., 2002. – 432с.,
8. Компьютерные коммуникации / Иванов В. – СПб.: ИД Питер, 2002., - 224 с.,
9. Компьютерные сети. – 4-е изд. / Таненбаум Э. – СПб.: ИД Питер, 2003. – 992 с.,
10. Компьютерные системы передачи данных. – 6-е изд. / Столингс В. – М.: Вильямс, 2002. – 928 с.
11. Сети TCP/IP – Т.1: Принципы, протоколы и структура. – 4-е изд., / Камер Дуглас. – М.: Вильямс, 2003, 880с.
12. Служба Active Directory Win2000: разработка и внедрение / Гэри Л. Олсен. – М., Вильямс, 2001., 624с..

Додаткова література

13. Современные компьютерные сети. – 2-изд. / Столлингс Вильям. – СПб.: ИД Питер, 2003. – 784с.
14. Основы построения виртуальных частных сетей. Уч. пос. для ВУЗов. / Запечников С.В. – М., 2003, 342с.
15. Управление сетями связи: принципы, протоколы, прикладные задачи / Дымарский Я. С. – М., 2003., 384 с.

Список літератури
для самостійної підготовки вступника до
фахового вступного випробування з дисципліни
" АРХІТЕКТУРА КОМП’ЮТЕРНИХ СИСТЕМ "

Основна література

1. Гук М. Архитектура и интерфейсы ПК. - СПб.: «Издательство «Питер», 2001.

2. Рудометов В., Рудометов Е. Материнские платы и чипсеты. - СПб.: «Издательство «Питер», 2001. - 352 с.
3. Гук М., Юров В. Процессоры Pentium VI, Athlon и DURON.-СПб.:- «Издательство «Питер», 2001. - 480 с.
4. Соломенчук В.Г., Соломенчук П.В. Железо ПК – СПб.: БХВ-Петербург, 2008. – 480с.
5. Вильям Столлингс Структура организация и архитектура компьютерных систем, 5-е изд. – М: Издательский дом «Вильямс», 2002. – 896с.
6. Гук М.Ю. Аппаратные средства IBM PC. 3-изд. - СПб.: Издательство «Питер», 2008. - 1072 с.

Додаткова література

7. Стивен Бигелоу, Устройство и ремонт пресонального компьютера. Аппаратная платформа и основные компоненты. – М.: ООО «Бином-Пресс», 2008. – 976с.
8. Таненбаум Э, Архитектура компьютера. 5-е изд. – СПб.: Питер, 2007. – 844 с.
9. Жмакин А.П., Архитектура ЭВМ.- СПб.: БХВ-Петербург, 2008. – 320с.

Голова фахової атестаційної комісії
Інституту комп'ютерних інформаційних технологій О.К.Юдін

Завідувач кафедри
комп'ютеризованих систем захисту інформації О.К.Юдін