Перелік програмних питань
з дисциплін, які виносяться на фахове вступне випробування
"Комплексні системи захисту інформації"

1. Визначення головних понять пов’язаних з КСЗІ.
2. Система законодавства у сфері інформаційних відносин.
3. Історичні аспекти формування поняття систем захисту інформації.
4. Критерії оцінки інформаційної безпеки за національними стандартами.
5. Класи автоматизованих систем.
6. Профілі захисту інформації.
7. Визначення області та межі дії КСЗІ.
8. Місце і роль КСЗІ в управлінні діяльністю організацій.
9. Загальні принципи внутрішньої та зовнішньої політики держави у сфері інформаційних відносин.
10. Організаційні та інженерно-технічні заходи.
11. Об’єкти інформаційних відносин.
12. Суб’єкти інформаційних відносин, основні права й обов’язки учасників зазначених відносин.
13. Нормативно-правове забезпечення КСЗІ.
14. Технічні канали витоку, нав’язування, знищення та блокування інформації в інформаційно-телекомунікаційних системах (ІТС).
15. Методи та засоби інженерно-технічних заходів безпеки.
16. Структура КСЗІ.
17. Обґрунтування створення КСЗІ.
18. Етапи побудови КСЗІ.
19. Ресурси як основні об'єкти КСЗІ.
20. Методика впровадження КСЗІ.
21. Розробка організаційно-розпорядчої документації на КСЗІ.
22. Документація КСЗІ.
23. Оцінка рівня загроз та вразливостей.
24. Системний підхід в управлінні КСЗІ.
25. Вимоги до проведення випробувань КСЗІ.
26. Програма, тривалість і область діяльності випробувань КСЗІ.
27. Експертиза КСЗІ.
28. Атестація КСЗІ.
29. Сертифікація КСЗІ.
30. Супроводження КСЗІ.

Список літератури
для самостійної підготовки вступника до
фахового вступного випробування з дисципліни
" КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ "

Основна література

1. Конституція України.
2. Концепція національної безпеки.
3. Закон України „Про національну програму інформатизації"" Київ-2001.

4. закон України „Про інформацію" Київ-1992.
5. Закон України "Про державну таємницю" Київ-1999.
6. Закон України "Про науково-технічну інформацію" Київ-1995.
7. Закон України "Про оперативно-розшукову діяльність" Київ-1992.
8. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" Київ-2003.
9. Закон України "Про електронні документи та електронний документообіг" Київ-2003.
10. Закон України "Про електронний цифровий підпис" Київ-2003.
11. Кримінальний Кодекс України. Київ-2001.
12. Закони України „ Про банки і банківську діяльність", „ Про національний банк України", Про платіжні системи та переказ грошей в Україні". Київ-2000.
13. Хорошко В.О. та ін. „Захист інформації*" КМУГА-2000.
14. Н.Ворожко В.П., Корченко О.Г. „Захист інформації з обмеженим доступом" КМУГА-1999.

Додаткова література

1. ДСТУ 3396.0-96 та ДСТУ 3396.1-96. Захист інформації. ТЗІ.
2. www.rada.gov.ua – офіційний сайт Верховної Ради України.
3. www.dstszi.gov.ua/dstszi - офіційний сайт ДСТЗІ.

"КРИПТОГРАФІЯ ТА СТЕГАНОГРАФІЯ"

1. Основні характеристики захисту інформації та криптографічні методи їх забезпечення.
2. Шифрування та кодування.
3. Криптографія та стеганографія.
4. Забезпечення цілісності інформації. Однонаправлені криптографічні функції.
5. Аутентифікація користувача. Цифровий підпис.
6. Забезпечення доступності інформації. Протоколи обміну ключами.
7. Криптостійкість шифрів та ключів.
8. Основні вимоги до криптографічних алгоритмів.
9. Шифрування метом Цезаря та його зламування.
10. Шифрування методом простої підстановки та його зламування.
11. Поліалфавітні шифри. Шифрування методом Віженера та його зламування.
12. Шифрування методом простої перестановки та його зламування.
13. Лінійні перетворення. Шифри збивання.
14. Одноразові блокноти. Формування випадкової послідовності.
15. Комбінація шифрів. Алгоритм шифрування DES.
16. Асиметрична криптографія (криптографія з відкритими ключами).
17. Прості та складені числа та їх властивості.
18. Взаємно прості числа. Алгоритм Евкліда знаходження найбільшого спільного дільника.
19. Рівняння Діофанта. Знаходження секретного ключа.

20. Лишки та їх властивості.
21. Шифрування методом Рівеста-Шаміра-Адлемана.
22. Багаторівнева система ключів. Метод шифрування ель-Гамаля.
23. Еліптичні криві. Додавання точок на еліптичних кривих.
24. Алгоритм формування ключів на еліптичних кривих.
25. Алгоритм формування цифрового підпису на еліптичних кривих.
26. Алгоритм перевірки цифрового підпису на еліптичних кривих.
27. Стеганографічний захист інформації. Прихована інформація. Контейнер.
28. Пропускна спроможність стеганографічного каналу.
29. Криптографічні алгоритми та протоколи.
30. Довірчі криптографічні протоколи. Протоколи з арбітражем та судівством.

Список літератури
для самостійної підготовки вступника до
фахового вступного випробування з дисципліни
" **КРИПТОГРАФІЯ ТА СТЕГАНОГРАФІЯ** "

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.
7. Вербицький О.В. Вступ до криптології. - Лв.:ВНТЛ, 1998. - 247 с.

«СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

1. Історичні аспекти формування поняття системи менеджменту.
2. Визначення області та межі дії систем менеджменту інформаційної безпеки.
3. Структура систем менеджменту.
4. Місце і роль системи менеджменту інформаційної безпеки в управлінні діяльністю організацій.
5. Критерії оцінки інформаційної безпеки за національними стандартами.
6. Критерії оцінки інформаційної безпеки міжнародними стандартами.
7. Канадські критерії оцінки безпеки надійних комп'ютерних систем.
8. Міжнародний стандарт ISO / IEC 15408.
9. Федеральні критерії оцінки інформаційної безпеки.
10. Історія серії стандартів ISO/IEC 27000.
11. Історія стандарту ISO/IEC 27001.
12. Обґрунтування створення СМІБ.
13. Структура та вимоги стандарту ISO/IEC 27001.
14. Стуктура стандарту ISO/IEC 27002.
15. Система управління ризиками на вимогу стандарту ISO/IEC 27001:2005.
16. Додаток А стандарту ISO/IEC 27001:2005. Реалізація вимог стандарту.
17. Методики впровадження системи менеджменту інформаційної безпеки.
18. Принципи QECD.
19. Модель PDCA.
20. Додаток В стандарту ISO/IEC 27001:2005.
21. Додаток С стандарту ISO/IEC 27001:2005.
22. Технології оцінки інформаційних ризиків.
23. Технології аналізу інформаційних ризиків.
24. Інтеграція системи менеджменту інформаційної безпеки за вимогами ISO/IEC 27001:2005 та системи менеджменту якості за вимогами ISO 9001:2000.
25. Вимоги стандарту ISO 19011:2002 до проведення аудитів.
26. Аудит систем менеджменту інформаційної безпеки.

27.Види аудиту.
28.Етапи внутрішнього аудиту систем менеджменту інформаційної безпеки.
29.Проведення коригувальних та попереджувальних дій.
30.Вимоги до аудиторів..

Список літератури
для самостійної підготовки вступника до
фахового вступного випробування з дисципліни
"СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ "

Основна література

1. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навчальний посібник. / МОН. – К.: Кондор, 2008. – 383 с.

2. Інформаційна безпека та сучасні мережеві технології: Англо-українсько-російський словник термінів / В.П. Бабак, О.Г. Корченко. – К.: НАУ, 2003. – 670с.

3. Захист інформації в мережах передачі даних / О.І. Юдін, О.Г. Корченко, Г.Ф. Конахович – К.: Вид-во ТОВ «НВП»Інтерсервіс», 2009. – 716 с.

4. Корченко О.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: «МК-Пресс», 2006. – 320с.

Додаткова література

a. Риск-менеджмент. / В.Н. Вяткин, И.В. Вяткин, В.А. Гамза, Ю.Ю. Екатеринославский, Дж.Дж Хэмптон; И. Юргенс, ред. Учебник. - М: Дашков и К, 2003. - 494 с.

b. Информационная безопасность и защита информации: Учебное пособие. – 2-е изд., стер. / В. П. Мельников, С. А. Клейменов, А. М. Петраков; Клейменов С. А., ред. – М.: Академия, 2007. – 332 с.

c. Надійнісне проектування технічних систем і оцінка риску. / Хенлі Ернест Джон, Кумамото Хиромицу; пер. з англ. О.Ю. Зареніна, В.Ф.Хмеля; під ред. Ю.Г.Зареніна. - К: Вища школа, 1987. - 544 с.

"СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ".

1. Класифікація технічних каналів витоку за фізичними властивостями.
2. Які бувають методи захисту інформації? У чому полягає їх сутність?
3. Поняття основних технічних засобів і систем, які системи до них ставляться.
4. Логічні елементи І, АБО. НІ схемотехнічний пристрій і принципи функціонування.
5. Функціональні вузли ЦС. Схемотехнічний пристрій і принципи функціонування.
6. Поняття про мікропроцесори.
7. Програмовані логічні матриці.
8. Інтегральні схеми типу CPLD.
9. Інтегральні схеми типу FPGA.

10.Загальна характеристика схемотехнічних методів проектування.

11.Етапи створення схемотехнічного проекту ЦУ.

12.Проектування програмними методами.

13.Вимоги до мови проектування цифрової апаратури. Основні характеристики мови.

14.Представлення проектованої цифрової системи в мовному середовищі VHDL: Базові розділи проекту.

15.Лексичні елементи мови VHDL. Ключові слова і зарезервовані слова.

16.Лексичні елементи мови VHDL.

17.Літерали.

18.Вступні зауваження про програмні величини даних і їх оголошенні.

19.Інформаційні типи програмних величин.

20.Підпрограми в мові VHDL.

21.Бібліотеки та пакети мови VHDL, що містять конвертують функції.

22.Програмні об'єкти даних.

23.Етапи створення і апаратної реалізації VHDL проектів.

24.Оператори мови VHDL. Класифікація операторів мови VHDL.

25.Операція коментування. Математичні вирази мови VHDL

26.Явно заданий оператор процес (Process Statement (PS)) з явно вибраною групою чутливості, що розташовуються після ключового слова процес (Process (... ..)).

27.Оператори тіла оператора Process (). Підлеглі оператори оператори Process ().

28.Оператор умовної передачі управління if ... then ... end if і його модифікації.

29.Бібліотеки типів даних.

30.Класифікація масивів. Визначені типи масивів. Масиви користувача.

Список літератури
для самостійної підготовки вступника до
фахового вступного випробування з дисципліни
" СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ "

Основна література

1. Корченко А.Г., Тимошенко Н.П. и др., VHDL: Справочное пособие по основам языка. М: «Додэка XX1», 2008 – 224 с.: ил.

2. Гроувер Д., Сатер Р., Фипс Дж. Защита программного обеспечения// Пер. с англ.// Под редакцией Д. Гроувера - М.: Мир, 1992.- 285 с.

3. Соловьев В.В. VHDL'92. Новые свойства языка описания аппаратуры. /Пер. с англ./ - М: Радио и связь, 1995. – 256 с.

4. Угрюмов Е.П. Цифровая схемотехника. – СПб.: БХВ – Петербург, 2000. – 528 с.

5. Соломенчук В.Г., Соломенчук П.В. Железо ПК – СПб.: БХВ-Петербург, 2008. – 480с.

6. Вильям Столлингс Структура организация и архитектура компьютерных систем, 5-е изд. – М: Издательский дом «Вильямс», 2002. –

896с.

Додаткова література

1. Таненбаум Э, Архитектура компьютера. 5-е изд. – СПб.: Питер, 2007. – 844 с.
2. Жмакин А.П., Архитектура ЭВМ.- СПб.: БХВ-Петербург, 2008. – 320с.