МІНІСТЕРСТВО ОСВІТИ УКРАЇНИ

ВИЩА АТЕСТАЦІЙНА КОМІСІЯ УКРАЇНИ

Затверджено
Атестаційною колегією
Міністерства освіти України
від 23.12.99 протокол
№ 5/9-12/5

"Узгоджено"
Заступник голови ВАК України
_____ С.В.Іванов
"09" 12 1999 р.

ПРОГРАМА

кандидатських іспитів зі спеціальності

05.13.21 - Системи захисту інформації

НАЦІОНАЛЬНА
АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ
МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ

203680,м.Київ-164,
вул.ГенералаНаумова,15,
Телефон:444-10-63
Телефакс:4440586

E-mail:svetlana@ipme.kiev.ua

НАЦИОНАЛЬНАЯ
АКАДЕМИЯ НАУК УКРАИНЫ

ИНСТИТУТ ПРОБЛЕМ
МОДЕЛИРОВАНИЯ В ЭНЕРГЕТИКЕ

'03680,г.Киев-164,
ул.ГенералаНаумова,15,
Телефон:444-10-63
Телефакс:4440586

E-mail:svetlana@ipme.kiev.ua

06.12.99 № 215/9-332

На № _____ от _____

Міністерство освіти України
Головне управління керівних і
науково-педагогічних кадрів
В.П.Погребняку

Направляємо Вам проект програми кандидатського іспиту зі спеціальності 05.13.21 - системи захисту інформації, складеної на ініціативній основі, для розгляду і затвердження науково-методичною комісією Міністерства освіти України.

Директор
чл. кор. НАН України В.Ф.Євдокимов

Програма розроблена д.т.н. В.В.Мохором, д.т.н., професором Ю.М.Коростіль, д.т.н., професором В.О.Хорошко, к.т.н. В.М.Горіцький, к.т.н. М.Е.Шелест.

Програма погоджена з науково-методичною комісією Міністерства освіти України " " N .

Програма кандидатського іспиту за спеціальністю 05.13.21 - системи захисту інформації.

В програмі відображені слідуючі розділи теоретичних та практичних основ захисту інформації:

- основи створення комплексних систем захисту інформації,
- організаційно-правове забезпечення захисту інформації,
- основи криптографічного захисту інформації,
- основи технічного захисту інформації,
- основні компоненти систем захисту інформації та засоби їх реалізації.

1. Системи захисту інформації:

а) загрози інформації, моделі оцінки загроз інформації,

б) системи показників вразливостей інформації,

в) аналітичні моделі визначення значень базових показників вразливостей,

г) статистичні моделі визначення значень базових показників вразливостей,

д) узагальнені показники вразливостей інформації,

е) визначення та обгрунтування повної множини функцій захисту інформації,

ж) методологія проектування систем захисту інформації,

з) обгрунтування складу засобів захисту у системі захисту

інформації,

к) технологія функціонування систем захисту інформації.

2. Організаційно-правове забезпечення захисту інформації:

а) загальний склад організаційно-правового забезпечення захисту інформації,

б) організаційно-технічні засоби захисту інформації,

в) рівні захисту, класифікація автоматизованих систем та вимоги до захисту інформації,

г) державні стандарти по захисту інформації.

3. Основи криптографії:

а) місце і роль криптографічних методів у загальній системі захисту інформації,

б) математичні моделі шифрів, їх властивості,

в) класифікація шифрів, основні вимоги до шифрів,

г) теоретична і практична стійкість шифрів, досконалі шифри і їх властивості,

д) типові криптосистеми і їх характеристики,

е) моделі і критерії відкритого тексту,

ж) функції криптографічних систем, методи забезпечення імітостійкості й автентифікації повідомлень,

з) управління ключами, формування ключів, протоколи розподілу ключів,

і) криптографічні протоколи в задачах ідентифікації, розмежування доступу, тощо,

к) стандарти криптографічних систем захисту інформації (DES, ГОСТ-28147, інші),

л) типові методи криптоаналізу й оцінювання криптог-

рафічної стійкості системи.

м) квантова криптографія, імовірнісна криптографія, концепція відвідного каналу.

н) основні поняття і методи стеганографічного захисту інформації.

4. Основи технічного захисту інформації:

а) характеристика технічної розвідки.

б) загальні питання організації протидії технічній розвідці

в) класифікація технічних каналів витоку інформації та їх моделі.

г) методи і засоби захисту об'єкту від витоку інформації по технічних каналах.

д) захист технічних засобів від витоку інформації по побічних електромагнітних випромінюваннях.

е) захист інформації від витоку по ланцюгах електроживлення.

ж) віброакустичний канал і захист інформації.

з) норми ефективності захисту інформації від витоку по технічних каналах.

і) умови створення технічних каналів витоку інформації.

к) методика виміру і розрахунку параметрів небезпечних сигналів.

л) принципи побудови засобів виявлення каналів витоку інформації.

5. Реалізація систем захисту інформації та їх фрагментів:

а) методи захисту програмного забезпечення від вірусів, несанкційованого використання, тощо.

б) реалізація методів захисту інформації в стандартних мережевих операційних системах,

в) стандартні системи захисту інформації в локальних та глобальних мережах, захист інформації в Internet,

г) програмна та апаратна реалізація шлюзів,

д) особливості використання методів захисту у банківських технологіях та віртуальній торгівлі.

Література.

1. Вакка Дж. Безопасность Интранет. М.: Book Media Publisher, 1998, 458 с.

2. Горфинкель С., Стеффорд Дж. Безопасность Web и электронная коммерция. М.: Book Media Publisher, 1999, 563 с.

3. Организация и современные методы защиты информации. М.: Концерн "Банковский Деловой Центр", 1998, 465 с.

4. Эдвардс М.Дж. Безопасность в Интернете на основе Windows NT. М.: Русская Редакция, 1999, 618 с.

5. Горфинкель С., Стеффорд Дж. Практическое руководство по безопасности UNIX и Интернет. М.: Book Media Publisher, 1999, 478 с.

6. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. М.: Яхтсмен, 1996, 187 с.

7. Мельников В.В. Защита информации в компьютерных системах. М.: Финансы и статистика, Электроинформ, 1997, 364 с.

8. Корченко А.Г. Несанкционированный доступ к компьютерным системам и методы защиты. Учебное пособие. Киев, 1998, КМУГА,115 с.

9. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа

к информации. Показатели защищенности от несанкционированного доступа к информации. Москва, 1992.

10. Коваленко М.М. Комп'ютернi вiруси i захист iнформацiї. Київ, Наукова думка, 1999.

11.Галатенко В.А. Информационная безопасность. /Открытые системы, NN4-6, 1995.

12. Задірака В.К., Олесюк О.С., Недашковський Н.О. Методи захисту банкiвської iнформацiї. Київ. Вища школа, 1999.

13. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему. Санкт-Петербург, НПО "Мир и семья - 95", 286 с.

14. Стенг Д., Мун С. Секреты безопасности сетей. Киев: Диалектика, 1996, 535 с.

15. Тайли Э. Безопасность персонального компьютера. Минск: Попурри, 1997, 477 с.

16. Петраков Защита и охрана личности, собственности, информации. М.: Радио и связь, 1997, 315 с.

17. Барсуков В.С. Обеспечение информационной безопасности. М.: Технология электронных коммуникаций. 1996, 94 с.

18.Спесивцев А.В., Вегнер В.А., Крутяков А.Ю. Защита информации в персональных ЭВМ. М.: Радио и связь, 1992, 192 с.

19. Хоффман Л.Д. Современные методы защиты информации. М.: Советское радио, 1980, 268 с.

20. Теория и практика обеспечения информационной безопасности./ Под ред. П.Д.Зегжды, М.: Яхтсмен, 1996, 297 с.

21. Зегжда Д., Мешков А., Семьянов П., Шведов Д. Как противостоять вирусной атаке. BHV - Санкт-Петербург, 1995, 318 с.

22. Саломаа А. Криптография с открытым ключом. М.: Мир, 1996.

23. Богуш В.М., Кудін А.М. Інформаційна безпека "від А до Я" 3000 термінів та понять. Київ, Техніка, 1999.

24. Феденко Б.А., Макаров И.В. Безопасность сетевых ОС. Москва, Эко-трендз, 1999.

25. Герасименко В.А., Размахин М.К. Криптографические методы в автоматизированных системах./ Зарубежная радиоэлектроника. 1982, N 8, с.97-123.

26. Смид М.Э., Бранстед Д.К. Стандарт шифрования данных: Прошлое и будущее. ТИИЭР, т. 76, N5, 1988, с. 43-54.

27. Малый тематический выпуск "Защита информации"/ ТИИЭР, т.76, N5, 1988.

28. Буч Г. Объектно-ориентированное проектирование с примерами применения. М.: Конкорд, 1992.

29. Балакшин Е.И., Хлупнов С.В. Опыт работы с межсетевым экраном Firewall-1 компании Check Point./ Защита информации "Кофидент, N2, 1998, с. 56- 59.

30.Галатенко В.А., Трифаленков И.А. Комплексные межсетевые экраны обеспечиваю безопасность систем Intarnet. / Защита информации "Конфидент", N2, 1997, с. 31-34.

31. Мафтик С. Механизмы защиты в сетях ЭВМ. М.: Мир, 1993, 216 с.

32. Барсуков В.С., Марущенко В.В., Шигин В.А. Интегральная безопасность. М.: "Газпром", 1994, 170 с.

Експертна рада з інформатики