МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ПРОГРАМА

вступного іспиту до аспірантури зі спеціальності
05.13.21 – Системи захисту інформації

Затверджено на засіданні Вченої ради
Інституту інформаційно-діагностичних систем
протокол № ___ від «___» _____ 2011 р.
Голова Вченої ради ІІДС
_____ С.Ф. Філоненко

Київ – 2011

Програму вступного іспиту до аспірантури зі спеціальності 05.13.21 – «Системи захисту інформації» розробили д.т.н., професор Г.Ф. Конахович, д.т.н., професор О.Г. Корченко, д.т.н., професор О.К. Юдін, к.т.н., доцент В.А. Швець.

У програмі відображені такі розділи теоретичних та практичних основ захисту інформації:

- безпека інформаційних та комунікаційних систем;
- управління інформаційною безпекою;
- захист програмного забезпечення;
- основи криптографічного захисту інформації;
- основи технічного захисту інформації.

1. Безпека інформаційних та комунікаційних систем:

1.1. Проблеми безпеки в Інтернет. Характеристика та сучасні методи їх вирішення.

1.2. Основні поняття інформаційної безпеки комп'ютерних систем та мереж.

1.3. Стандартні стеки комунікаційних протоколів.

1.4. Аналіз загроз безпеки інформаційних систем та мереж. Модель загроз безпеці. Модель протидії загрозам безпеці.

1.5. Протидія несанкціонованому міжмережевому доступу.

1.6. Еталонна модель OSI. Порівняння моделі OSI і стеку протоколів TCP/IP.

1.7. Модель комп`ютерної мережі.

1.8. Розробка концепції і політики інформаційної безпеки.

1.9. Побудова захищених віртуальних мереж VPN.

1.10. Захищені віртуальні канали. Канальний рівень моделі OSI.

1.11. Побудова захищених віртуальних мереж на базі маршрутизаторів.

1.12. Захищені віртуальні канали. Мережевий рівень моделі OSI.

1.13. Захищені віртуальні канали. Сеансовий рівень моделі OSI.

1.14. Побудова захищених віртуальних мереж за допомогою міжмережевих екранів.

1.15. Побудова захищених віртуальних мереж на основі спеціалізованого програмного забезпечення. Побудова захищених віртуальних мереж на основі спеціалізованих апаратних засобів.

1.16. Сервери віддаленого доступу.

1.17. Архітектура засобів безпеки IPSec.

1.18. Централізований контроль віддаленого доступу.

1.19. Безпека віддаленого доступу до комп`ютерної мережі.

1.20. Наведіть основні характеристики прикладного шлюзу.

1.21. Порівняння Інтернет-банкінгу, -трейдингу та -страхування.

1.22. Порівняльний аналіз IPv4 та IPv6.

1.23. Яким чином здійснюється фільтрація трафіку.

1.24. Вкажіть основні характеристики екранного маршрутизатору. Опишіть шлюз сеансового рівня.

1.25. Опишіть процес налаштування базових параметрів функціонування брандмауера у різних операційних системах.

1.26. Назвіть критерії оцінки міжмережевих екранів.

1.27. Сучасні системи FireWall. Переваги і недоліки.

1.28. Опишіть детально яким чином здійснюється тунелювання на канальному

рівні. Протокол PPTP.

1.29. Побудова захищених віртуальних каналів на сеансовому рівні. Протокол Socks.

1.30. Сучасні системи FireWall. Підтримка різних платформ і режимів роботи.

1.31. Яким чином здійснюється тунелювання на канальному рівні? Протокол L2F. Яким чином здійснюється тунелювання на канальному рівні? Протокол L2TP.

1.32. IPSec. Опишіть протокол заголовку аутентифікації. Опишіть протокол інкапсульованого захисту. Опишіть управління захищеним тунелем.

1.33. Сучасні системи FireWall. FireWall-1. Black Hole. Підтримка функцій захисту.

1.34. Побудова захищених віртуальних каналів на сеансовому рівні. Протокол SSL. Опишіть протокол S/Key.

2. Управління інформаційною безпекою:

2.1. Концепція національної безпеки України. Загрози національній безпеці України в інформаційній сфері.

2.2. Характеристики захищеності інформаційних ресурсів.

2.3. Загрози безпеці інформаційних ресурсів.

2.4. Принципи побудови моделі порушника.

2.5. Базові принципи та рівні захисту інформаційних систем.

2.6. Типові уразливості інформаційних систем та причини їх появи.

2.7. Класифікація атак на ресурси інформаційних систем.

2.8. Комплексні системи захисту інформації. Етапи побудови.

2.9. Види випробувань та вимоги до проведення випробувань комплексних систем захисту інформації.

2.10. Критерії оцінки інформаційної безпеки за національними та міжнародними стандартами.

2.11. Аудит систем менеджменту інформаційної безпеки.

2.12. Стандарти серії 27000. Основні принципи та завдання.

2.13. Основні положення та структура стандарту ISO/IEC 27001:2005.

2.14. Додаток А стандарту ISO/IEC 27001:2005. Реалізація вимог стандарту.

2.15. Класифікація ризиків інформаційної безпеки.

2.16. Основні методи оцінки та аналізу інформаційних ризиків.

2.17. Ризик-менеджмент стандарт NIST 800-30 та ISO 27002.

2.18. Соціотехнічна безпека. Основні поняття та методи.

2.19. Міжнародний стандарт ISO/IEC 15408.

2.20. Нормативні документи з оцінювання захищеності інформації.

2.21. Законодавча і нормативна база захисту інформації в Україні.

2.22. Закон України «Про захист інформації в автоматизованих системах». Об'єкти захисту. Суб'єкти відносин. Компетенція органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці. Здійснення права власності на секретну інформацію та її матеріальні носії.

2.23. Закон України «Про державну таємницю». Обмеження на оприлюднення секретної інформації. Права режимно-секретних відділів. Інформація, що не може бути віднесена до державної таємниці. Завдання режимно-секретних органів.

2.24. Кримінальний кодекс України. Розголошення державної таємниці. Втрата документів, що містять державну таємницю. Передача або збирання відомостей, що

становлять конфіденційну інформацію, яка є власністю держави.

3. Захист програмного забезпечення:

3.1. Обмеження доступу до комп'ютера за допомогою пароля BIOS. Прийоми, застосовувані для розкриття і зняття пароля BIOS. Заходи для захисту комп'ютера від атак на пароль BIOS.

3.2. Підсистема безпеки ОС Windows. Методи і програмні засоби атак на файли парольного кеша ОС Windows. Заходи для захисту парольного кеша ОС Windows.

3.3. Підсистема безпеки ОС Windows. Методи і програмні засоби атак на базу даних SAM ОС Windows. Комплексні заходи для захисту ОС Windows від локальних атак.

3.4. Захист у ОС Windows бази даних SAM за допомогою утиліти SYSKEY.

3.5. Атака на базу даних SAM за допомогою утиліти L0phtCrack+.

3.6. Заходи для захисту парольного кеша ОС Windows.

3.7. Структура системного реєстру ОС Windows.

3.8. Ключі підсистеми безпеки в системному реєстрі ОС Windows.

3.9. Застосування шаблонів безпеки адміністратора ОС Windows.

3.10. Приховані мережеві адміністративні ресурси ОС Windows (IPC$, ADMIN$ C$ та інші).

3.11. Методи проведення хакерами сканування мереж при атаці через NetBiOS.

3.12. Захист ОС Windows від мережних атак і віддаленого вторгнення.

3.13. Підсистема безпеки ОС UNIX.

3.14. Методи шифрування, збереження і керування паролями в UNIX.

3.15. Об'єкти і методи атак на ОС UNIX.

3.16. Методи протидії комп'ютерним вірусам і троянським програмам.

3.17. Атака на конфіденційну інформацію за допомогою програм «клавіатурних шпигунів».

3.18. Методи своєчасного виявлення і знешкодження програм, що атакують.

3.19. Вкажіть області адрес CMOS, що мають відношення до збереження пароля BIOS. Фрагмент програми атаки на пароль BIOS. Приклад розрахунку хеш-функції 01EAAh інструментального пароля BIOS.

3.20. Алгоритм шифрування паролів ОС Windows і вкажіть файли його реалізації. Відключення кешування паролів в ОС Windows.

3.21. Приведіть приклад фрагмента програми, що реалізує алгоритм потокового шифрування RC4 при формуванні пароля в ОС Windows.

3.22. Включення аудиту в ОС Windows.

3.23. Включення в ОС Windows режиму застосування тільки складних паролів.

3.24. Шифрування бази даних SAM за допомогою утиліти SYSKEY.

3.25. Наведіть приклад обходу заборони на копіювання бази даних SAM за допомогою утиліти NTFSDOS.EXE.

3.26. Наведіть приклади значень ідентифікаторів облікових записів RI (relative identifier) для користувачів «ADMINISTRATOR» і «GUEST» у LM-хеш ОС Windows.

3.27. Введення обмеження на доступ до системного реєстру ОС Windows.

3.28. Конструювання шаблону безпеки адміністратора ОС Windows..

3.29. Найбільш часто використовувані порти ОС Windows.

3.30. Атаки через NetBiOS за допомогою утиліт NET і NBSTAT.

3.31. Заборона «Null session» і відключення «NetBiOS over TCP/IP» у системному реєстрі ОС Windows.

3.32. Перелік найбільш часто використовуваних команд ОС UNIX.

3.33. Приведіть алгоритм послідовності дій при зломі паролів UNIX і вкажіть шляхи підвищення їх криптостійкості.

3.34. Перерахуйте основні типи комп'ютерних вірусів і розкрийте алгоритм їхнього пошуку.

4. Основи криптографічного захисту інформації:

4.1. Класифікація шифрів та основні вимоги до них.

4.2. Поняття обчислювальної та теоретико-інформаційної стійкості криптографічних систем.

4.3. Симетричні криптографічні алгоритми. Принципи побудови та особливості застосування.

4.4. Мережа Файстеля.

4.5. Принципи побудови блокових шифрів.

4.6. Класифікація потокових шифрів.

4.7. Типові криптоаналітичні атаки на блокові та потокові шифри.

4.8. Аналіз сучасних алгоритмів із секретним ключем (AES, ГОСТ 28147-89, RC6).

4.9. Режими шифрування (ECB, CBC та ін.).

4.10. Сутність проблеми розподілу ключів шифрування та сучасні способи її вирішення.

4.11. Асиметричні криптографічні алгоритми. Принципи побудови та особливості застосування.

4.12. Поняття та принципи використання NP-складних задач в асиметричній криптографії.

4.13. Криптосистема з відкритим ключем RSA.

4.14. Електронний цифровий підпис та його застосування.

4.15. Стандарти електронного цифрового підпису (ДСТУ 4145-2002, ISO/IEC 14888-3(15946-2), FIPS 186-3 та ін.).

4.16. Сутність асиметричних криптографічних перетворень у кільці цілих чисел.

4.17. Сутність асиметричних криптографічних перетворень у полях Галуа.

4.18. Сутність асиметричних криптографічних перетворень у групі точок еліптичних кривих.

4.19. Система електронного цифрового підпису України та її застосування.

4.20. Визначення та вимоги до функцій гешування.

4.21. Криптографічні протоколи аутентифікації. Аутентифікація на основі паролів та сертифікатів.

4.22. Сувора аутентифікація на базі симетричних і асиметричних алгоритмів.

4.23. Метод розподілу ключів Діфі-Хелмана. Особливості застосування.

4.24. Квантова криптографія. Принципи та основні протоколи.

4.25. Квантовий розподіл ключів шифрування. Основні поняття, принципи та протоколи.

4.26. Квантовий прямий безпечний зв'язок. Основні поняття, принципи та

протоколи.

4.27. Принципи побудови квантових систем захисту інформації.

4.28. Атаки на криптографічні системи. Поняття та класифікація.

4.29. Криптоаналіз класичних шифроалгоритмів. Приклад.

4.30. Криптоаналіз систем шифрування з відкритим ключем. Приклад.

4.31. Новітні технології криптоаналізу. Квантові алгоритми, суперкомп'ютери та нейронні мережі.

4.32. Цифрова стеганографія. Принципи та застосування.

4.33. Комп'ютерна стеганографія. Принципи. Файлова система StegFS.

4.34. Основні поняття та методи стеганографії. Застосування стеганографії.

4.35. Основні атаки на стеганографічні системи захисту інформації.

4.36. Критерії стеганографічної стійкості.

4.37. Застосування стеганографічних методів в інформаційно-комунікаційних системах.

5. Основи технічного захисту інформації:

5.1. Класифікація каналів витоку інформації.

5.2. Утворення радіоканалів витоку інформації.

5.3. Моделі оцінки рівня електромагнітних випромінювань в каналах витоку інформації.

5.4. Акустичні канали витоку інформації.

5.5. Використання телефонних ліній для прослуховування приміщень.

5.6. Види акустоелектричних перетворень.

5.7. Використання мікрофонного ефекту для прослуховування приміщень.

5.8. Електричні канали витоку інформації.

5.9. Паразитні електромагнітні випромінювання та наводки.

5.10. Виток інформації колами електроживлення та заземлення.

5.11. Візуально оптичні канали витоку інформації.

5.12. Канали витоку інформації за рахунок взаємного впливу ліній зв'язку.

5.13. Канали витоку інформації при експлуатації ЕОМ.

5.14. Оцінка рівня побічних електромагнітних випромінювань від ЕОМ.

5.15. Класифікація засобів несанкціонованого отримання інформації.

5.16. Загальна характеристика радіомікрофонів.

5.17. Методи та засоби прослуховування телефонних ліній.

5.18. Спеціальні засоби прослуховування (направлені та лазерні мікрофони, стетоскопи і т.д.).

5.19. Пристрої перехоплення інформації з кабельних та оптоволоконних ліній зв'язку.

5.20. Системи прихованого відеонагляду.

5.21. Класифікація технічних засобів захисту інформації.

5.22. Засоби захисту акустичної інформації.

5.23. Засоби захисту від радіозакладок.

5.24. Радіомоніторинг побічних електромагнітних випромінювань.

Рекомендована література:

1. Юдін О.К. Захист інформації в мережах передачі даних / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович // Підручник. – К. : Видавництво DIRECTLINE, 2009. – 714 с.
2. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / Корченко А.Г. – К. : НАУ, 2005. – 336 с.
3. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г. Защита информации в телекоммуникационных системах. – К. : «МК-Пресс», 2005. – 288 с.
4. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Конахович Г.Ф., Пузыренко А.Ю. – К. : «МК-Пресс», 2006. – 288 с.
5. Нормативно-правове забезпечення інформаційної безпеки: Збірник нормативно-правових документів / Уклад. О.Г. Корченко, Ю.О. Дрейс. – Житомир : ЖВІ НАУ, 2010. – 280 с.
6. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А., под ред. В.А. Хорошко. – К. : Арий, 2008. – Том 1. Несанкционированное получение информации. – 464 с.
7. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А., под ред. В.А. Хорошко. – К. : Арий, 2008. – Том 2. Информационная безопасность. – 344 с.
8. Новиков О.М. Безпека інформаційно-комунікаційних систем / О.М. Новиков, М.В. Грайворонський // Підручник. – К. : Видавництво BHV, 2009. – 608 с.
9. Венбо Мао. Современная криптография. Теория и практика // Венбо Мао. – М. : Вильямс, 2005. – 786 с.