МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ПРОГРАМА

вступного іспиту до аспірантури зі спеціальності
21.05.01 – Інформаційна безпека держави

Затверджено на засіданні Вченої ради
Інституту комп'ютерних інформаційних технологій
протокол № 3 від «15» квітня 2013 р.
Голова Вченої ради ІКІТ
_____ О.К. Юдін

Київ – 2013

Програму вступного іспиту до аспірантури зі спеціальності 21.05.01 – «Інформаційна безпека держави» розробили д.т.н., професор О.Г. Корченко, д.т.н., професор О.К. Юдін, д.т.н., професор Г.Ф. Конахович, к.т.н., доцент С.О. Гнатюк.

У програмі відображені такі розділи теоретичних та практичних основ забезпечення захисту інформаційних ресурсів держави:

– організаційно-технічні та правові основи забезпечення захисту людини, суспільства, держави;

– забезпечення безпеки державних інформаційних ресурсів інформаційно-комунікаційних систем;

– управління інформаційною безпекою;

– основи криптографічного, стеганографічного та технічного захисту інформаційних ресурсів держави.

1. Організаційно-технічні та правові основи забезпечення захисту людини, суспільства, держави

1.1. Поняття «національна безпека». Види безпеки: державна, економічна, суспільна, військова, екологічна, інформаційна. Основні види загроз національній безпеці: загрози інформаційній інфраструктурі, загрози безпеці державних інформаційних ресурсів, загрози духовному життю суспільства, загрози правам і свободам громадян. Інформаційна безпека як складова національної безпеки. Співвідношення і взаємозв'язок інформаційної та інших видів безпеки.

1.2. Визначення та загальні властивості інформації. Види та форми представлення інформації. Поняття інформаційного ресурсу, інформаційного простору та інформаційного суверенітету. Види інформаційних ресурсів: національні, державні, особисті тощо. Категорії інформації за режимом доступу.

1.3. Методологічні, технологічні, технічні та організаційні основи розвитку інфраструктури єдиного інформаційного простору держави. Сучасні проблеми. Принципи побудови та функціонування інформаційних, інформаційно-аналітичних, пошукових систем і мереж. Моделі доступу до інформації.

1.4. Інформаційні технології та інформаційна безпека в сфері державного управління, освіти, економіки, фінансів, промисловості тощо. Поняття критичних інфраструктур, критичних інформаційних інфраструктур. Основні загрози критичним інформаційним ресурсам, методи їх виявлення та нейтралізації.

1.5. Питання інформаційної безпеки при створенні систем інформаційно-аналітичної підтримки державних органів. Проблеми та світовий досвід.

1.6. Основні види інформаційно-технічного впливу в контексті єдиного інформаційного простору та сучасних інформаційних війн. Основні методи, засоби та технології його здійснення.

1.7. Інформаційні технології як засіб інформаційного впливу. Поняття інформаційної війни, інформаційного впливу, інформаційної зброї, психотронної зброї. Типи інформаційних війн, основи їх ведення. Типові тактики та стратегії.

1.8. Кібертероризм та сучасні загрози в цій сфері. Основні поняття (кіберпростір, кіберзагроза, кібератака тощо). Загальний огляд сучасних проблем комп'ютерної злочинності. Класифікація комп'ютерних злочинів відповідно до чинного законодавства.

1.9. Закон України «Про основи національної безпеки України». Поняття інформаційної сфери та національної безпеки. Загрози національним інтересам України в інформаційній сфері.

1.10. 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.

1.11. 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.

1.12. Кримінальний кодекс України. Розголошення державної таємниці. Втрата документів, що містять державну таємницю. Передача або збирання відомостей, що становлять конфіденційну інформацію, яка є власністю держави.

1.13. Закон України «Про доступ до публічної інформації». Мета і сфера дії закону. Поняття публічної інформації. Право на доступ до публічної інформації та принципи його забезпечення. Контроль за забезпеченням доступу до публічної інформації. Суб'єкти відносин у сфері доступу до публічної інформації. Розпорядники інформації та їх обов'язки. Доступ до інформації про особу.

1.14. Закон України «Про науково-технічну інформацію». Визначення, склад та завдання національної системи науково-технічної інформації. Інформаційні ресурси національної системи науково-технічної інформації. Умови надання інформаційної продукції та послуг. Державна політика у сфері науково-технічної інформації: державна підтримка науково-інформаційної діяльності. Забезпечення суверенітету України у цій сфері.

1.15. Закон України «Про захист персональних даних». Поняття персональних даних, їх обробки. Суб’єкт персональних даних. Об’єкти захисту. Загальні та особливі вимоги до обробки персональних даних. Державна служба України з питань захисту персональних даних, структура та функції.

2. Забезпечення безпеки державних інформаційних ресурсів інформаційно-комунікаційних систем

2.1. Основні поняття безпеки інформаційно-комунікаційних систем (маска, шлюз, метрика, класи та топології мереж).

2.2. Актуальні проблеми безпеки державних інформаційних ресурсів у мережі Інтернет: загальна характеристика та сучасні методи їх вирішення.

2.3. Аналіз загроз безпеці державних інформаційно-комунікаційних систем. Побудова моделі загроз та порушника безпеки.

2.4. Розробка концепції і політики інформаційної безпеки державних інформаційно-комунікаційних систем. Еталонна модель OSI. Співвідношення відповідних рівнів моделі OSI і стеку протоколів TCP/IP.

2.5. Захищені віртуальні канали. Канальний рівень моделі OSI. Протоколи PPTP, L2F, L2TP та ін.

2.6. Захищені віртуальні канали. Мережевий та сеансовий рівні моделі OSI. Протоколи SSL, Socks, S/Key тощо.

2.7. Протокол IPSec. Архітектура засобів безпеки протоколу IPSec. Протоколи

заголовку аутентифікації та інкапсульованого захисту.

2.8. Особливості налаштування базових параметрів функціонування брандмауера у різних операційних системах. Функціональні особливості та критерії оцінки міжмережевих екранів.

2.9. Поняття віртуальної приватної мережі. Класифікація та основні функції. Особливості їх застосування для безпеки державних інформаційних ресурсів.

2.10. Побудова захищених VPN: на базі спеціалізованих апаратних засобів, міжмережевих екранів та маршрутизаторів.

2.11. Класи мереж за IP-адресацією. Порівняльний аналіз версій протоколів IPv4 та IPv6.

2.12. Поняття та класифікація бездротових технологій захисту інформаційних ресурсів. Види атак на бездротові інформаційно-комунікаційні системи.

2.13. Порівняльний аналіз технологій бездротового зв'язку IEEE 802.11 та 802.16 з точки зору ефективності захисту інформаційних ресурсів.

2.14. Технології захисту бездротових систем зв'язку (WEP, WPA, WPA2).

2.15. Методи випробування стійкості інформаційно-комунікаційних систем на основі технологій WEP та WPA.

3. Управління інформаційною безпекою

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

3.2. Характеристики захищеності інформаційних ресурсів. Модель CIA.

3.3. Загрози безпеці державних інформаційних ресурсів. Типові уразливості інформаційних та комунікаційних систем, причини їх появи. Класифікація атак на державні ресурси.

3.4. Поняття та категоризація державних інформаційних ресурсів. Принципи та рівні захисту державних інформаційних ресурсів інформаційно-комунікаційних систем.

3.5. Комплексні системи захисту інформації. Етапи побудови. Види випробувань та вимоги до проведення випробувань комплексних систем захисту інформації (державних інформаційних ресурсів).

3.6. Критерії оцінки рівня інформаційної безпеки за національними та міжнародними стандартами. Нормативні документи з оцінювання захищеності інформаційних ресурсів.

3.7. Системи менеджменту інформаційної безпеки. Аудит систем менеджменту інформаційної безпеки.

3.8. Стандарти серії 27К. Основні принципи та завдання. Основні положення та структура стандарту ISO/IEC 27001:2005. Додаток А стандарту ISO/IEC 27001:2005. Реалізація вимог стандарту.

3.9. Класифікація ризиків інформаційної безпеки. Основні методи оцінки та аналізу інформаційних ризиків. Ризик-менеджмент стандарт NIST 800-30 та ISO 27002.

3.10. Соціотехнічна безпека. Основні алгоритми соціотехнічних атак на державні інформаційні ресурси та рекомендації щодо захисту від них.

3.11. Основи планування безперервності роботи державних інформаційно-

комунікаційних систем відповідно до ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. Розробка та тестування плану BCP.

3.12. Поняття та класифікація інцидентів інформаційної безпеки відповідно до міжнародних стандартів та рекомендацій (ISO 18044:2004, ISO/IEC 27002:2005, MOD, ITU-T E.409 тощо).

3.13. Система управління інцидентами інформаційної безпеки: фази життєвого циклу відповідно до моделі PDCA. Архітектура та функції типової системи управління інцидентами інформаційної безпеки.

3.14. Особливості організації та функціонування команд (груп) CERT/CSIRT. Організаційні структури та управлінські механізми. Документаційне забезпечення. Діяльність CERT/CSIRT в органах державної влади.

3.15. Порівняльний аналіз міжнародних стандартів та української нормативної бази в частині управління інцидентами інформаційної безпеки.

4. Основи криптографічного, стеганографічного та технічного захисту інформаційних ресурсів держави

4.1. Основні терміни та поняття криптографічного захисту державних інформаційних ресурсів. Класифікація шифрів та основні вимоги до них. Режими шифрування. Поняття обчислювальної та теоретико-інформаційної стійкості.

4.2. Симетричні криптографічні алгоритми, принципи побудови та особливості їх застосування. Класифікація блокових та потокових шифрів. Аналіз сучасних алгоритмів із секретним ключем (AES, ГОСТ 28147-89, RC6 та ін.).

4.3. Сутність проблеми розподілу ключів шифрування та сучасні способи її вирішення. Метод розподілу ключів Діфі-Хелмана (приклад). Інші методи розподілу ключів.

4.4. Асиметричні криптографічні алгоритми. Принципи побудови та особливості застосування. Поняття та принципи використання NP-складних задач в асиметричній криптографії. Криптосистема з відкритим ключем RSA (приклад).

4.5. Сутність асиметричних криптографічних перетворень у кільці цілих чисел, полях Галуа та у групі точок еліптичних кривих.

4.6. Електронний цифровий підпис та його застосування. Стандарти електронного цифрового підпису (ДСТУ 4145-2002, ISO/IEC 14888-3(15946-2), FIPS 186-3 та ін.). Система електронного цифрового підпису України та її застосування для захисту державних інформаційних ресурсів.

4.7. Криптографічні протоколи аутентифікації. Аутентифікація на основі паролів та сертифікатів. Сувора аутентифікація на базі симетричних і асиметричних алгоритмів.

4.8. Квантова криптографія. Принципи та основні протоколи. Квантовий розподіл ключів та квантовий прямий безпечний зв'язок. Основні поняття, принципи та протоколи. Принципи побудови та застосування квантових систем захисту державних інформаційних ресурсів.

4.9. Атаки на криптографічні системи. Поняття та класифікація. Криптоаналіз класичних шифрів. Криптоаналіз систем шифрування з відкритим ключем. Новітні технології криптоаналізу (квантові алгоритми, суперкомп’ютери та нейронні мережі).

4.10. Поняття та базові терміни стеганографічного захисту інформації. Критерії стеганографічної стійкості. Застосування стеганографічних методів для захисту державних інформаційних ресурсів. Цифрова та комп'ютерна стеганографія (принципи та застосування). Основні атаки на стеганографічні системи захисту інформації.

4.11. Класифікація каналів витоку інформації та методів технічного захисту державних інформаційних ресурсів. Моделі оцінки рівня електромагнітних випромінювань в каналах витоку інформації.

4.12. Акустичні канали витоку інформації. Види акустоелектричних перетворень. Використання телефонних ліній для прослуховування приміщень. Використання мікрофонного ефекту для прослуховування приміщень.

4.13. Електричні канали витоку інформації. Паразитні електромагнітні випромінювання та наводки. Витік інформації колами електроживлення та заземлення.

4.14. Візуально оптичні канали витоку інформації. Канали витоку інформації при експлуатації ПК. Оцінка рівня побічних електромагнітних випромінювань від ПК. Класифікація засобів несанкціонованого отримання інформації (державних інформаційних ресурсів).

4.15. Методи та засоби прослуховування телефонних ліній. Спеціальні засоби прослуховування (направлені та лазерні мікрофони, стетоскопи і т.д.). Пристрої перехоплення інформації з кабельних та оптоволоконних ліній зв'язку. Системи прихованого відеоспостереження. Засоби захисту державних інформаційних ресурсів від радіозакладок.

Рекомендована література:

1. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення / О.К. Юдін // Підручник. — К. : НАУ, 2011. — 620 с.

2. Нормативно-правове забезпечення інформаційної безпеки: Збірник нормативно-правових документів / Уклад. О.Г. Корченко, Ю.О. Дрейс. — Житомир : ЖВІ НАУ, 2010. — 280 с.

3. Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. — К. : «МК-Пресс», 2005. — 432 с.

4. Ліпкан В.А. Національна безпека України / В.А. Ліпкан // Навчальний посібник. — К. : Кондор, 2008. — 552 с.

5. Охорона державних секретів незалежної України. / В.П. Ворожко, Й.У. Мастяниця, Л.Є. Шиманський, О.В. Олійник — К. : Інститут законодавства Верховної Ради України, 2010. — 128 с.

6. Система охорони державної таємниці як складова національної безпеки України [Ворожко В.П., Шлапаченко В.М., Пашков А.С., Макаренко В.В. та ін.]. — К. : НА СБУ, 2008. — 364 с.

7. Юдін О.К. Захист інформації в мережах передачі даних / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович // Підручник — К. : Вид-во DIRECTLINE, 2009. — 714 с.

8. Основи інформаційної безпеки / За ред. проф. В.О. Хорошка / В.О Хорошко, В.С. Чередніченко, М.Є. Шелест. — К. : ДУІКТ, 2008. — 186 с.

9. Смірнов О.А. Основи захисту інформації: навчальний посібник / О.А. Смірнов, Л.Г. Віхрова, С.І. Осадчій, Є.В. Мелешко, В.Ю. Ковтун. — Кіровоград : РВЛ КНТУ, 2011. — 322 с.

10. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / Корченко А.Г. — К. : НАУ, 2005. — 336 с.

11. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г. Защита информации в телекоммуникационных системах. — К. : «МК-Пресс», 2005. — 288 с.

12. Новиков О.М. Безпека інформаційно-комунікаційних систем / О.М. Новиков, М.В. Грайворонський // Підручник. — К. : Вид-во BHV, 2009. — 608 с.

13. Панасенко С.П. Алгоритмы шифрования. Специальный справочник / Панасенко С.П. — СПб. : БХВ-Петербург, 2009 — 576 с.

14. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування / І.Д. Горбенко, Ю.І. Горбенко. — Х. : Видавництво «Форт», 2012 — 870 с.

15. Горбенко І.Д. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: Монографія / І.Д. Горбенко, Ю.І. Горбенко. — Х.: Видавництво «Форт», 2010. — 608 с.

16. Математичні основи криптографії: навчальний посібник / Г.В. Кузнецов, В.В. Фомичов, С.О. Сушко, Л.Я. Фомичова. — Д.: Національний гірничий університет, 2004. — 391 с.

17. Математичні основи криптоаналізу: навчальний посібник / С.О. Сушко, Г.В. Кузнецов, Л.Я. Фомичова, А.В. Корабльов. — Д.: Національний гірничий університет, 2010. — 465 с.

18. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Конахович Г.Ф., Пузыренко А.Ю. — К. : «МК-Пресс», 2006. — 288 с.

19. Кононович В.Г. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. Ч. 4. Інформаційна безпека комунікаційних мереж та послуг. Реагування на атаки. Навчальний посібник / В.Г. Кононович, С.В. Гладиш. — Одеса : ОНАЗ ім. О.С. Попова, 2009. — 208 с.

20. Пошаговое руководство по созданию CSIRT (Европейское Агентство по Сетевой и Информационной Безопасности (ENISA) в рамках программы WP-2006), 2006. — 86 с.

21. 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.

22. 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.

23. Telecommunications Networks – Current Status and Future Trends / [O. Korchenko, P. Vorobiyenko, M. Lutskiy, Ye. Vasiliu, S. Gnatyuk et al.]; edited by J.H. Ortiz. — Rijeka : InTech, 2012. — 446 p.