МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Проректор
з навчальної роботи
_____ Анатолій ПОЛУХІН
«__» _____ 2023 р.

ПРОГРАМА

додаткового вступного іспиту до аспірантури (PhD докторантури)
зі спеціальності 125 «Кібербезпека та захист інформації»

Гарант освітньо-наукової програми
«Кібербезпека та захист інформації» Олександр КОРЧЕНКО

Розробник
к.т.н., доцент Юлія ХОХЛАЧОВА

Київ – 2023

Програма додаткового вступного іспиту до аспірантури (PhD докторантури) зі спеціальності 125 «Кібербезпека та захист інформації» відображає базові розділи теоретичних та практичних основ кібербезпеки.

Питання:

1. Захищені віртуальні канали. Канальний рівень моделі OSI (протоколи PPTP, L2F, L2TP тощо). Мережевий та сеансовий рівні моделі OSI (протоколи SSL, Socks, S/Key тощо).
2. Протокол IPSec. Архітектура засобів безпеки протоколу IPSec. Протоколи заголовку аутентифікації та інкапсульованого захисту.
3. Особливості налаштування базових параметрів функціонування брандмауера у різних операційних системах. Функціональні особливості та критерії оцінки міжмережевих екранів.
4. Поняття віртуальної приватної мережі. Класифікація та основні функції. Особливості їх застосування для безпеки державних інформаційних ресурсів. Побудова захищених VPN: на базі спеціалізованих апаратних засобів, міжмережевих екранів та маршрутизаторів.
5. Поняття та класифікація бездротових технологій захисту інформаційних ресурсів. Види атак на бездротові інформаційно-телекомунікаційні системи та методи випробування їх стійкості. Порівняльний аналіз технологій бездротового зв’язку IEEE 802.11 та 802.16 з точки зору інформаційної безпеки.
6. Основні терміни та поняття криптографічного захисту інформаційних ресурсів. Класифікація шифрів та основні вимоги до них. Режими шифрування. Поняття обчислювальної, практичної та теоретико-інформаційної стійкості.
7. Симетричні криптографічні алгоритми, принципи побудови та особливості їх застосування. Класифікація блокових та потокових шифрів. Аналіз сучасних алгоритмів із секретним ключем (AES, ДСТУ 7624-2014, RC6 та ін.).
8. Сутність проблеми розподілу ключів шифрування та сучасні способи її вирішення (асиметрична криптографія, квантовий розподіл ключів тощо). Метод розподілу ключів Діфі-Хелмана (приклад). Інші схеми розподілу ключів.
9. Асиметричні криптографічні алгоритми. Принципи побудови та особливості застосування. Поняття та принципи використання NP-складних задач в асиметричній криптографії. Криптосистема з відкритим ключем RSA (приклад). Сутність асиметричних криптографічних перетворень у кільці цілих чисел, полях Галуа та у групі точок еліптичних кривих.
10. 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.
11. 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 інформації.

12. 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).
13. Поняття та базові терміни стеганографічного захисту інформації. Критерії стеганографічної стійкості. Застосування стеганографічних методів для захисту інформаційних ресурсів. Цифрова та комп’ютерна стеганографія (принципи та застосування). Основні атаки на стеганографічні системи захисту інформації.
14. Концепція національної безпеки України. Загрози національній безпеці України в інформаційній сфері.
15. Характеристики захищеності інформаційних ресурсів. Модель CIA.
16. Загрози безпеці державних інформаційних ресурсів. Типові уразливості інформаційних та комунікаційних систем, причини їх появи. Класифікація атак на державні ресурси.
17. Поняття та категоризація державних інформаційних ресурсів. Принципи та рівні захисту державних інформаційних ресурсів інформаційно-комунікаційних систем.
18. Комплексні системи захисту інформації. Етапи побудови. Види випробувань та вимоги до проведення випробувань комплексних систем захисту інформації (державних інформаційних ресурсів).
19. Критерії оцінки рівня інформаційної безпеки за національними та міжнародними стандартами. Нормативні документи з оцінювання захищеності інформаційних ресурсів.
20. Системи менеджменту інформаційної безпеки. Аудит систем менеджменту інформаційної безпеки.
21. 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.
22. Класифікація ризиків інформаційної безпеки. Основні методи оцінки та аналізу інформаційних ризиків. Ризик-менеджмент стандарт NIST 800-30 та ISO 27002.
23. Соціотехнічна безпека. Основні алгоритми соціотехнічних атак на державні інформаційні ресурси та рекомендації щодо захисту від них.
24. Основи планування безперервності роботи державних інформаційно-комунікаційних систем відповідно до ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. Розробка та тестування плану BCP.
25. 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).

26. Особливості організації та функціонування команд (груп) CERT/CSIRT. Організаційні структури та управлінські механізми. Документаційне забезпечення. Діяльність CERT/CSIRT в органах державної влади.
27. Порівняльний аналіз міжнародних стандартів та української нормативної бази в частині управління інцидентами інформаційної безпеки.
28. Система управління інцидентами інформаційної безпеки: фази життєвого циклу відповідно до моделі PDCA. Архітектура та функції типової системи управління інцидентами інформаційної безпеки.

Рекомендована література:

1. Корченко А.Г. Побудова систем захисту інформації на нечітких множинах. Теорія та практичні рішення / Корченко О.Г. — К. : НАУ, 2005. — 336 с.
2. 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.
3. Основи інформаційної безпеки / За ред. проф. В.О. Хорошка / В.О Хорошко, В.С. Чередніченко, М.Є. Шелест. — К. : ДУІКТ, 2008. — 186 с.
4. 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.
5. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г. Захист інформації в телекомунікаційних системах. — К. : «МК-Пресс», 2005. — 288 с.
6. Новиков О.М. Безпека інформаційно-комунікаційних систем / О.М. Новиков, М.В. Грайворонський // Підручник. — К. : Вид-во BHV, 2009. — 608 с.
7. Панасенко С.П. Алгоритми шифрування. Спеціальний довідник / Панасенко С.П. — СПб.: БХВ, 2009 — 576 с.
8. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування / І.Д. Горбенко, Ю.І. Горбенко. — Х. : Видавництво «Форт», 2012 — 870 с.
9. 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.
10. Математичні основи криптографії: навчальний посібник / Г.В. Кузнецов, В.В. Фомичов, С.О. Сушко, Л.Я. Фомичова. — Д.: Національний гірничий університет, 2004. — 391 с.

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

12. Конахович Г.Ф. Комп'ютерна стеганографія. Теорія та практика / Конахович Г.Ф., Пузиренко А.Ю. — К. : «МК-Пресс», 2006. — 288 с.

13. Методи та засоби захисту інформації. В 2-х томах / Ленков С.В., Перегудов Д.О., Хорошко В.О., за ред. В.О. Хорошко. — К. : Арій, 2008. — Том 1. Несанкціоноване отримання інформації. — 464 с.

14. Методи та засоби захисту інформації. В 2-х томах / Ленков С.В., Перегудов Д.О., Хорошко В.О., за ред. В.О. Хорошко. — К. : Арій, 2008. — Том 2. Інформаційна безпека. — 344 с.