МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖЕНО
Голова Приймальної комісії,
Голова комісії з реорганізації НАУ,
в.о. ректора
_____Ксенія СЕМЕНОВА

«15» 04 2024 року.

ПРОГРАМА
ВСТУПНОГО ВИПРОБУВАННЯ ДО АСПІРАНТУРИ

зі спеціальності 125 Кібербезпека та захист інформації

на здобуття наукового ступеня доктора філософії

(третій (освітньо-науковий) рівень вищої освіти)

Галузь знань 12 Інформаційні технології

Освітньо-наукова програма «Кібербезпека»

Київ – 2024

ЗМІСТ

ВСТУП

Програма фахового вступного випробування до аспірантури за галуззю знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека та захист інформації» відображає кваліфікаційні вимоги до теоретичних знань претендентів для вступу до аспірантури.

Програма є основою для формування переліку питань вступного випробування й складання екзаменаційних білетів.

Метою складання вступного випробування є перевірка й оцінювання фундаментальних знань вступників із організаційно-технічних та правових основ забезпечення захисту людини, суспільства, держави; забезпечення безпеки інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах; управління інформаційною безпекою, що є передумовою оцінки можливостей для проведення наукових досліджень з обраної галузі науки.

Фахове випробування проводиться з метою виявлення знань, вмінь, компетентної здатності щодо здійснення наукових досліджень, якими повинен володіти фахівець за галуззю знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека та захист інформації».

1. ОРІЄНТОВНИЙ ПЕРЕЛІК ПИТАНЬ ДЛЯ ПІДГОТОВКИ ДО ВСТУПНОГО ВИПРОБУВАННЯ

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

1.6. Поняття інформаційної війни, інформаційно-психологічного впливу, інформаційної зброї, психотропної зброї. Типи інформаційних війн, основи їх ведення. Типові тактики та стратегії. Канали маніпулятивного впливу на людей, суспільство та державу. Рекомендації щодо захисту.

1.7. Кібертероризм та сучасні загрози в цій сфері. Основні поняття (кіберпростір, кіберзагроза, кібератака тощо). Загальний огляд сучасних проблем кіберзлочинності. Класифікація кіберзлочинів відповідно до чинного вітчизняного та міжнародного законодавства.

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

1.9. 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.

1.10. 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.

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

1.12. 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.

1.13. 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.

1.14. 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 інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах

2.1. Основні поняття безпеки інформаційно-телекомунікаційних систем. Актуальні проблеми безпеки інформаційних ресурсів у мережі Інтернет: загальна характеристика та сучасні методи їх вирішення. Аналіз загроз безпеці інформаційно-телекомунікаційних систем. Побудова моделі загроз та порушника безпеки.

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

2.3. Захищені віртуальні канали. Канальний рівень моделі OSI (протоколи PPTP, L2F, L2TP тощо). Мережевий та сеансовий рівні моделі OSI (протоколи SSL, Socks, S/Key тощо).

2.4. Протокол IPSec. Архітектура засобів безпеки протоколу IPSec. Протоколи заголовку аутентифікації та інкапсульованого захисту.

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

2.6. 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.

2.7. 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.

2.8. Основні терміни та поняття криптографічного захисту інформаційних ресурсів. Класифікація шифрів та основні вимоги до них. Режими шифрування.

Поняття обчислювальної, практичної та теоретико-інформаційної стійкості.

2.9. 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.).

2.10. 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.

2.11. 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.

2.12. 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.

2.13. 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.

2.14. 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).

2.15. 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.

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.

2. КРИТЕРІЇ ОЦІНЮВАННЯ ПІДГОТОВЛЕНОСТІ ВСТУПНИКІВ

Вступне випробування має кваліфікаційний характер
Шкала оцінювання: національна та ECTS

РЕЙТИНГОВІ ОЦІНКИ
Виконання окремих завдань вступного випробування

Вид навчальної роботи	Максимальна величина рейтингової оцінки (бали)
Виконання завдання №1	60
Виконання завдання №2	70
Виконання завдання №3	70
Усього	200

Значення рейтингових оцінок за виконання завдань вступного іспиту та їх критерії

Оцінка	Виконання завдання №1	Виконання завдання №2,3
Відмінно	54-60	63-70
Добре	45-53	53-62
Задовільно	36-44	42-52
Незадовільно	0-35	0-41

Відповідність рейтингових оцінок у балах оцінкам за національною шкалою

Оцінка в балах		Пояснення	
120-200	**190-200**	**Відмінно** (відмінне виконання лише з незначною кількістю помилок)	**Вступне випробування складено**
	175-189	**Добре** (в загальному вірне виконання з певною кількістю суттєвих помилок)	
	101-174	**Задовільно** (непогано, але зі значною кількістю недоліків та задовольняє мінімальним критеріям)	
0-100		**Вступне випробування не складено**	

3. СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

Основна:

1. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення: підручник. К. : НАУ, 2011. 620 с.
2. Корченко О.Г., Дрейс Ю.О. Нормативно-правове забезпечення інформаційної безпеки: Збірник нормативно-правових документів. Житомир : ЖВІ НАУ, 2010. 280 с.
3. Богуш В.М., О.К. Юдін. Інформаційна безпека держави. К. : «МК-Пресс», 2005. 432 с.
4. Ліпкан В.А. Національна безпека України: Навчальний посібник. К. : Кондор, 2008. 552 с.
5. Ворожко В.П., Мастяниця Й.У., Шиманський Л.Є., Олійник О.В. Охорона державних секретів незалежної України. К.: Інститут законодавства Верховної Ради України, 2010. 128 с.
6. Ворожко В.П., Шлапаченко В.М., Пашков А.С., Макаренко В.В. Система охорони державної таємниці як складова національної безпеки України. К. : НА СБУ, 2008. 364 с.
7. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних: підручник. К. : Вид-во DIRECTLINE, 2009. 714 с.
8. В.О Хорошко, В.С. Чередніченко, М.Є. Шелест. Основи інформаційної безпеки. К. : ДУІКТ, 2008. 186 с.
9. О.А. Смірнов, Л.Г. Віхрова, С.І. Осадчій, Є.В. Мелешко, В.Ю. Ковтун. Основи захисту інформації: навчальний посібник. Кіровоград : РВЛ КНТУ, 2011. 322 с.
10. Корченко О.Г. Побудова систем захисту інформації на нечітких множинах. Теорія та практичні рішення. К. : НАУ, 2005. 336 с.
11. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г. Захист інформації в телекомунікаційних системах. К. : «МК-Пресс», 2005. 288 с.
12. О.М. Новиков, М.В. Грайворонський. Безпека інформаційно-комунікаційних систем: підручник. К. : Вид-во BHV, 2009. 608 с.
13. І.Д. Горбенко, Ю.І. Горбенко. Прикладна криптологія. Теорія. Практика. Застосування. Х. : Видавництво «Форт», 2012. 870 с.
14. І.Д. Горбенко, Ю.І. Горбенко. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: Монографія. Х.: Видавництво «Форт», 2010. 608 с.
15. Г.В. Кузнецов, В.В. Фомичов, С.О. Сушко, Л.Я. Фомичова. Математичні основи криптографії: навчальний посібник Д.: Національний гірничий університет, 2004. 391 с.

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

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

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

19. Покрокове керівництво по створенню CSIRT (ENISA) в рамках програми WP-2006), 2006. 86 с.

20. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методи та засоби захисту інформції. В 2-х томах. Том 1. Несанкціоноване отримання інформації. К.: Арий, 2008. 464 с.

21. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методи та засоби захисту інформції. В 2-х томах. Том 2. Інформаційна безпека К. : Арий, 2008. 344 с.

22. O. Korchenko, P. Vorobiyenko, M. Lutskiy, Ye. Vasiliu, S. Gnatyuk Telecommunications Networks – Current Status and Future Trends. Rijeka : InTech, 2012. 446 p.