КИЇВСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

ЗАТВЕРДЖЕНО
Приймальною комісією
Протокол № 2 від «24» 04. 2023 р.
Голова Приймальної комісії
_____Олександр ТУРУНЦЕВ

ПРОГРАМА

вступного випробування (іспиту) до аспірантури
зі спеціальності 125 Кібербезпека та захист інформації

Рівень вищої освіти: третій (освітньо-науковий)

Галузь знань: 12 Інформаційні технології

Спеціальність: 125 Кібербезпека та захист інформації

Освітньо-наукова програма: «Інформаційна безпека держави»

На основі: освітнього ступеня магістра
(освітньо-кваліфікаційного рівня спеціаліста)

ПОГОДЖЕНО
Проректор з наукової роботи
_____Наталія ВІННІКОВА

РОЗГЛЯНУТО І ЗАТВЕРДЖЕНО
на засіданні Вченої ради
Факультету інформаційних технологій та математики
Протокол № 2 від «15» березня 2023 р.
Голова Вченої ради
_____Оксана ЛИТВИН

Київ – 2023

1. Пояснювальна записка

Програма вступного випробування для здобувачів третього (освітньо-наукового) рівня вищої освіти за спеціальністю 125 Кібербезпека та захист інформації складена відповідно до програм підготовки фахівців в галузі знань 12 Інформаційні технології, відповідає вимогам якісної підготовки та атестації здобувачів відповідного рівня вищої освіти та є нормативним документом Київського університету імені Бориса Грінченка.

Головною метою іспиту є визначення рівня осмислення, усвідомлення здобувачем основ та головних положень спеціальності, стану готовності до дослідницької діяльності у сфері інформаційної та кібербезпеки й захисту інформації.

Програма включає сукупність питань з інформаційних технологій, які окреслюють основні явища та процеси інформаційної і кібербезпеки та захисту інформації, визначають термінологічне поле науки.

Вступник на іспиті має розкрити основний зміст питань білета та додаткових запитань, продемонструвати:

- знання першоджерел, уміння застосовувати їх зміст та основні ідеї;
- володіння змістом принципів захисту інформації та забезпечення безпеки інформаційно-комунікаційних систем, уміння оперувати ними;
- здатність виявити суть проблеми щодо забезпечення інформаційної/кібернетичної безпеки;
- уміння аргументувати власну позицію щодо вирішення завдань забезпечення інформаційної і кібербезпеки та захисту інформації на об’єктах інформаційної діяльності;
- спроможність до проведення самостійних наукових досліджень в обраній галузі.

Прийом вступного іспиту проводиться відповідно до вимог чинного законодавства, нормативних документів Міністерства освіти та науки України.

2. Методичні рекомендації до проведення вступного випробування

Вступне випробування проводиться у формі іспиту та передбачає відповідь вступника за трьома питаннями обраного білету.

Час підготовки відповіді – 30 хвилин.

3. Критерії оцінювання вступного іспиту

Вступне випробування оцінюється за принципом накопичувальної системи. Оцінка вступного випробування складається з балів, отриманих у

результаті відповіді на запитання білету. Критерії оцінювання відповідей на питання білету подано у табл.1.

Таблиця 1

Загальні критерії оцінювання відповідей на запитання білету

№ з/п	Критерії оцінювання	Оцінка (у балах)
1	Виставляється за ґрунтовні, систематизовані знання програмного матеріалу; вміння аналізувати явища, які вивчаються, у їхньому взаємозв'язку і розвитку, чітко і лаконічно; логічно і послідовно відповідати на поставлені запитання; вміння застосовувати теоретичні положення під час розв'язання практичних задач; вияв креативності у розумінні і творчому використанні набутих знань та умінь.	90 – 100
2	Виставляється за міцні, систематизовані знання навчального програмного матеріалу, аргументовані відповіді на поставлені запитання; вміння застосовувати теоретичні положення під час розв'язування практичних задач.	82 – 89
3	Виставляється за міцні знання програмного матеріалу, аргументовані відповіді на поставлені запитання, які, однак, містять певні (несуттєві) неточності; вміння застосовувати теоретичні положення під час розв'язання практичних задач.	75 – 81
4	Виставляється за посередні знання програмного матеріалу, мало аргументовані відповіді, слабке застосування теоретичних положень при розв’язанні практичних задач.	69 – 74
5	Виставляється за слабкі знання програмного матеріалу, неточні або мало аргументовані відповіді, з порушенням послідовності його викладання, за слабке застосування теоретичних положень при розв’язанні практичних задач.	60 – 68
6	Виставляється за незнання значної частини програмного матеріалу, істотні помилки у відповідях на запитання, невміння орієнтуватися під час розв'язання практичних задач, незнання основних фундаментальних положень.	1 – 59

4. Типовий перелік питань вступного випробування

Основні положення

Поняття «національна безпека». Види безпеки: державна, економічна, суспільна, військова, екологічна, інформаційна. Основні види загроз національній безпеці: загрози інформаційній інфраструктурі, загрози безпеці інформації, загрози духовному життю суспільства, загрози правам і свободам громадян.

Інформаційна безпека як складова національної безпеки. Взаємозв'язок інформаційної та інших видів безпеки.

Зовнішні і внутрішні загрози інформаційній безпеці: типи і класи загроз, джерела, засоби реалізації загроз та їхні наслідки.

Базові методи запобігання і ліквідації загроз інформаційній безпеці держави (правові, організаційно-технічні, економічні тощо). Поняття політики безпеки. Принципи побудови політики безпеки та її впровадження.

Визначення та загальні властивості інформації. Види та форми представлення інформації.

Поняття інформації, інформаційного ресурсу, інформаційного простору та інформаційного суверенітету. Види інформаційних ресурсів: національні, державні, особисті тощо. Категорії інформації за режимом доступу.

Системні принципи організації інформаційних ресурсів: чіткість, точність, доступність, швидкість, вичерпність, узгодженість, структурованість, цілісність, актуальність.

Принципи побудови та функціонування інформаційних, інформаційно-аналітичних, пошукових систем і телекомунікаційних мереж. Моделі доступу до інформації.

Світова мережа Інтернет: особливості побудови, можливі загрози.

Методологічні, технологічні, технічні та організаційні основи розвитку інфраструктури єдиного інформаційного простору держави. Сучасні проблеми.

Поняття надійності, живучості та відмовостійкості інформаційних систем і процесів. Базові методи реалізації цих принципів.

Інформаційні технології в системі державного управління

Поняття інфраструктури, інформаційної інфраструктури. Принципи побудови сучасних інформаційних інфраструктур (технічні аспекти).

Предметна область інформатики. Соціальні аспекти інформатизації суспільства.

Поняття інформаційної технології. Стан, проблеми розвитку і використання інформаційних технологій.

Методи людино-машинного спілкування. Програмні засоби людино-машинного спілкування. Діалогові системи. Інтелектуальний інтерфейс користувача. Мультимедійні системи як засоби людино-машинного інтерфейсу представлення та інтелектуалізації знань.

Методи і засоби розпізнавання і розуміння мовлення. Методи і засоби автоматичного витягування інформації з текстів на природній мові. Методи і засоби автоматичного синтезу мовлення. Методи і засоби розпізнавання

образів. Методи і засоби розпізнавання і синтезу зображень. Системи і засоби віртуальної реальності.

Експертні системи. Основні принципи побудови експертних систем. Мови логічного програмування. Інженерія знань. Здобуття, представлення і формування знань. Організація процесів управління і прийняття рішень на основі логіко-лінгвістичних моделей. Експертні системи в задачах планування і управління.

Задачі і функції систем підтримки прийняття рішень (СППР). Базові функціональні підсистеми СППР та їх задачі. Розподілені системи підтримки прийняття рішень у корпоративних системах.

Інформаційні технології та інформаційна безпека у сфері управління, економіки, фінансів, промисловості тощо. Поняття критичних інфраструктур, критичних інформаційних інфраструктур (КІІ). Основні загрози КІІ, методи їх виявлення та запобігання.

Стан розвитку та захищеності КІІ провідних країн світу та країн, що розвиваються. Типові політики безпеки та заходи їх забезпечення (огляд).

Питання інформаційної безпеки при створенні систем інформаційно-аналітичної підтримки державних органів.

Загальні відомості щодо методів дослідження складних систем

Основи експертного аналізу. Методологія, сутність, вимоги, сфери застосування експертного аналізу та прогнозування.

Основи технічного аналізу. Методологія, сутність, вимоги, сфери застосування технічного аналізу та прогнозування.

Побудова інформаційних моделей об'єктів, визначення критичних місць в інформаційних системах.

Аналіз і оцінка рівня захищеності інформації у СЗІ. Методологія, сутність, вимоги до проведення аналізу ризиків.

Математичні методи аналізу проблем інформаційної безпеки. Доказовий метод в теорії ЗІ.

Елементи теорії прийняття рішень. Формалізація процесу прийняття рішень. Прийняття рішень в умовах визначеності. Прийняття рішень в умовах ризику і невизначеності.

Елементи теорії систем масового обслуговування (СМО). Основні компоненти і характеристики СМО. Вихідний потік вимог. Процеси загибелі і розмноження. Основні типи СМО, які описуються процесами загибелі і розмноження. Мережі масового обслуговування.

Елементи лінійного програмування. Постановка задачі. Графічні методи рішень. Симплекс-метод. Транспортна задача. Подвійна задача. Задачі оптимізації на мережах.

Комп'ютерні системи та їх вплив на інформаційну безпеку держави

Методи організації безпечної взаємодії інформації в комп'ютерних системах.

Роль та місце комп’ютерних систем в державному управлінні та управлінні роботою критично важливих об'єктів держави.

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

Основні загрози комп’ютерним системам.

Кібертероризм та сучасні загрози в цій сфері.

Загальний огляд проблем комп’ютерної злочинності. Класифікація комп’ютерних злочинів.

Інформаційна війна та інформаційний вплив

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.

Інформаційні війни у сучасному соціально-політичному контексті. Інформаційні операції та технології їхнього здійснення. Захист інформаційного простору держави, суспільства та особистості від негативних впливів.

Інформаційна протидія. Роль геополітичного стратегічного аналізу. Основні принципи, завдання, цілі та методи стратегічного прогнозування.

Інформаційно-психологічний вплив. Його цілі та завдання. Особливості формування і функціонування суспільної думки.

Глобальні мережі: феномен Інтернет. Особливості інформаційно-психологічного впливу через Інтернет. Інтернет та сучасна політика.

Можливості і проблеми законодавчого регулювання Інтернет.

Принципи соціального інжинірингу.

Стандарти захисту інформації

Проблеми створення стандартів захисту інформації (ЗІ).

Критерії та класи захищеності засобів обчислювальної техніки та автоматизованих інформаційних систем. Стандарти щодо оцінки захищеності систем.

Міжнародні критерії безпеки комп'ютерних систем.

Захист інформації у комп'ютерних системах

Основні принципи та стратегії ЗІ у комп’ютерних системах.

Методи та види несанкціонованого доступу (НСД). Моделі загроз і порушника. Основні причини порушень безпеки.

Принципи побудови систем захисту інформації. Розмежування доступу користувачів до інформації. Методи ідентифікації та автентифікації (ІА) (парольні схеми ІА, біометричні системи ІА тощо).

Криптографічні засоби захисту інформації. Огляд і класифікація методів шифрування інформації.

Комплексний і фрагментарний підходи до забезпечення інформаційної безпеки. Зовнішня і внутрішня безпека.

Захист програм і даних від «вірусів», «хробаків» і «логічних бомб». Загальні моделі систем і процесів захисту інформації. Антивірусні програми (огляд).

Технології забезпечення безпеки мережевої інфраструктури

Забезпечення безпеки на відповідних рівнях моделі OSI: фізичному, канальному, мережному, транспортному, сеансовому. Сучасні системи виявлення вторгнень. Політики виявлення вторгнень. Засоби аналізу безпеки програмного забезпечення. Списки управління доступом (ACL). Передача потоку даних. Багатоадресна розсилка. Технології побудови віртуальних локальних мереж (VLAN).

Засоби забезпечення інформаційної безпеки та їх проектування

Принципи побудови технічних систем. Методологія побудови захищених інформаційних систем (ІС). Поняття архітектури систем. Особливості архітектури систем забезпечення інформаційної безпеки держави.

Особливості використовування засобів забезпечення інформаційної безпеки під час захисту інфраструктур.

Параметри функціонування ІС. Поняття критичних параметрів.

Особливості створення систем забезпечення інформаційної безпеки в державній сфері. Захист інформації державного призначення.

Основні засоби забезпечення інформаційної безпеки держави та принципи їх створення.

Методи шифрування як засіб забезпечення інформаційної безпеки.

Роль та функції держави в забезпеченні інформаційної безпеки країни.

Організаційно-технічні заходи щодо забезпечення захисту інформації. Організація і підрозділи служби безпеки (режиму, охорони, протипожежна, детективна, інформаційно-аналітична тощо).

Особливості захисту інформації в ПЕОМ і мережах. Особливості ЗІ у розподілених базах даних і телекомунікаціях. Проблема безпеки при підключенні автоматизованого робочого місця

5. Список рекомендованої літератури

1. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.: НАУ, 2013. – 432 с.

2. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці. – К.: ДУТ, 2015. – 345 с.

3. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. – К.: ТОВ «СІК ГРУП Україна», 2015. – 449 с.

4. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.

5. Бурячок В.Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К., 2018. – 320 с

6. Buriachok V.L. Methods of information protection in telecommunication systems: [manual]. / V.L.Buriachok, Ie.V.Duravkin, N.V. Lukova-Chuyko, P.M.Skladanniy / – K.:KUBG, 2019. – 74 c.

7. Козачок В.А., Коршун Н.В., Мазур Н.П., Платоненко А.В., Складанний П.М. Прикладні аспекти аналізу та синтезу політик безпеки. Навчальний посібник для студентів галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека – Київ: Вид-во КУБГ. 2021. 160 с

8. Соколов, В. Ю. Безпека безпроводових і мобільних мереж: Навчальний посібник / В. Ю. Соколов, В. Л. Бурячок, М. М. Таджділні / ред. перекл. О. П. Райтер. — 2 вид., доп. — К. : КУБГ, 2019. — 130 с.

9. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. – К.: ДУТ, 2015. – 449 с.

10. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації: підручник. - В.: ВНТУ, 2011. - 198 с.

11. Ленков С.В. Методи та засоби захисту інформації / Ленков С.В., Перегудов Д.А., Хорошко В.О. - К.: Арій, 2008. Том 1 - 464 с., Том II – 344 с.

12. Пасічник В.В. , Виклюк Я.І., Камінський Р.М. Моделювання складних систем. - Львів: Новий світ-2000, 2021. - 404 с.

13. Горбань І.І. Теорія ймовірностей та математична статистика для наукових працівників та інженерів. - К.: НАН України, 2003. - 239 с.

14. Ржевський С.В., Александрова В.М. Дослідження операцій. - К.: Академвидав, 2006. - 558 с.

15. Зайченко Ю. П. Дослідження операцій: Навч. посібник для ВНЗ. - 7-е вид., перероб. и доп. - К.: Слово, 2006. - 688 с.

16. Ложковський А.Г. Теорія масового обслуговування в телекомунікаціях. - Одеса: ОНАЗ ім. О.С. Попова, 2010. – 112 с

17. Коваленко А. О. Політичний аналіз і прогнозування. - К.: Наук. світ, 2002. - 201 с.

18. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: Навч. посібник. - К.: Кондор, 2004. - 384 с.

19. Литвиненко О.В. Інформаційні впливи та операції. Теоретико-аналітичні нариси: Монографія. - К.: НІСД, 2003. - 240 с. - (Сер. "Національна безпека"; Вип. 6).

20. Бутко М.П. Системний підхід і моделювання в наукових дослідженнях. - К.: ЦУЛ, 2014. - 360 с.

21. Толюпа С.В. Захист об’єктів інформаційної діяльності /Толюпа С.В., Оксіюк О.Г., Бурячок В.Л., Вялкова В.І.// К.: ККБ та ЗІ ФІТ КНУ імені Тараса Шевченка, 2018. – 322 с.

22. НД ТЗІ 1.1-001-98. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу / ДСТСЗІ СБ України. - Введ. 1998.

23. НД ТЗІ 1.1-002-98. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу / ДСТСЗІ СБ України. - Введ. 1998.

24. НД ТЗІ 2.2-001-98. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу / ДСТСЗІ СБ України. - Введ. 1998.

25. НД ТЗІ 2.2-002-98. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу / ДСТСЗІ СБ України. - Введ. 1998.

26. Про державну таємницю: Закон України від 21.01.94 № 3855-XII [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12#Text

27. Про захист інформації в автоматизованих системах: Закон України від 05.07.94 № 80/94-ВР [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

28. Про інформацію: Закон України від 02.10.92 № 2657 - XII [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text

29. Про Концепцію Національної програми інформатизації: Закон України від 04.02.98 №75/98-ВР [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text

30. Про науково-технічну інформацію: Закон України від 25.06.93 № 3322 - XII [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/3322-12#Text

33. Про Національну програму інформатизації: Закон України від 04.02.98 № 74/98 - ВР [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text

34. Стратегія кібербезпеки України [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#top

35. Доктрина інформаційної безпеки України [Електронний ресурс]. - Режим доступу: https://www.president.gov.ua/documents/472017-21374