

Затверджую



Голова Приймальної комісії
Ректор

підпис

Анатолій МЕЛЬНИЧЕНКО

28.03.2025 р.

дата

ПРОГРАМА

додакового вступного випробування

для вступу на освітньо-наукову програму підготовки доктора філософії «Кібербезпека»

за спеціальністю F5 Кібербезпека та захист інформації

Програму ухвалено:

Науково-методичною комісією за спеціальністю

F5 Кібербезпека та захист інформації

Протокол № 2 від 12 березня 2025 р.

Голова НМК

Дмитро ЛАНДЕ

ВСТУП

Програма визначає форму організації, зміст та особливості проведення додаткового вступного випробування на освітньо-наукову програму підготовки докторів філософії «Кібербезпека» за спеціальністю F5 Кібербезпека та захист інформації для вступників, які вступають для здобуття ступеня доктора філософії з іншої галузі знань (спеціальності), ніж та, яка зазначена в їхньому дипломі, на підставі якого здійснюється вступ.

Метою програми є перевірка набуття вступником компетентностей та результатів навчання, необхідних для опанування освітньо-наукової програми підготовки докторів філософії «Кібербезпека» за спеціальністю F5 Кібербезпека та захист інформації.

1. ОСНОВНИЙ ВИКЛАД

1.1. Перелік розділів та тем, які виносяться на додаткове вступне випробування

1. Нормативно-правові та організаційні засади кібербезпеки

- 1.1. **Нормативно-правове забезпечення** в сфері інформаційної і кібернетичної безпеки. Визначення, зміст та співвідношення понять «кібернетична безпека», «інформаційна безпека», «безпека інформації».
- 1.2. **Основи державної політики** України в сфері технічного захисту інформації. Захист інформації в інформаційно-телекомунікаційних системах.
- 1.3. **Організаційне забезпечення захисту інформації.** Склад і структура, основні завдання служби безпеки організації. Адміністративно-організаційні аспекти забезпечення режиму.
- 1.4. **Інформаційні аспекти безпеки підприємницької діяльності.** Інформаційна безпека в системі безпеки підприємницької діяльності. Комерційна таємниця. Адміністративно-організаційні аспекти забезпечення режиму комерційної таємниці на підприємстві.
- 1.5. **Класифікація інформації** за режимом доступу та правовим режимом. Інформація з обмеженим доступом. Державна таємниця. Система захисту державних секретів в Україні.
- 1.6. **Загрози.** Визначення поняття «кібернетична загроза». Основні види кіберзагроз.
- 1.7. **Ризики.** Фактори та умови виникнення ризиків. Зміст та сутність оцінювання ризиків. Концепції та моделі ризику.
- 1.8. **Цінність інформації.** Методики визначення цінності інформації. Рекомендації міжнародних стандартів щодо визначення цінності інформаційних ресурсів.

2. Системи та технології кібербезпеки

- 2.1. **Класичні схеми шифрування.** Моноалфавітні підстановки. Методи криптоаналізу. Поліалфавітні підстановки. Шифр Віженера та його криптоаналіз. Інші шифри підстановки. Шифри перестановки: загальне визначення, шифри обходу, табличні перестановки, маршрути Гамільтона, ґрати Кардано, магічні квадрати, інші шифри перестановки. Комбіновані шифри.
- 2.2. **Основи стеганографії.** Предмет, термінологія, області застосування. Основні поняття та методи стеганографії. Математичні моделі стегосистем. Огляд стего-алгоритмів. Атаки на стегосистеми та протидії їм. Приклади стеганографічних систем.
- 2.3. **Цифровий підпис.** Задачі цифрового підпису. Загальна концепція та схема цифрового підпису з геш-функцією в асиметричній криптографії. Цифровий підпис у схемі RSA з використанням геш-функцій, цифрові підписи Ель-Гамала, Рабіна. Сліпий підпис. Атаки на цифровий підпис.
- 2.4. **Криптографічні протоколи.** Протоколи розподілу секретів, доведення без розголошення, схеми пред'явлення випадкових бітів, протоколи електронної готівки. Імовірнісне шифрування.
- 2.5. **Безпека операційних систем.** Модель загроз для операційної системи, функціональні послуги безпеки і механізми, спрямовані на захист від кожної з загроз.
- 2.6. **Шкідливе програмне забезпечення** – класифікація, механізми функціонування, особливості застосування, заходи і технології протидії.
- 2.7. **Загрози безпеці інформації у комп'ютерних мережах.** Віддалені атаки (класифікація, приклади).
- 2.8. **Безпека веб-застосунків.** Атаки на сервери і клієнтів, заходи протидії.
- 2.9. **Архітектура безпеки взаємодії відкритих систем.** Стандарти, сервіси, механізми.
- 2.10. **Віртуальні приватні мережі.** Сервіси, технології, протоколи.

3. Математичні методи кібербезпеки

- 3.1. **Джерела загроз як основний чинник невизначеності.** Стохастична та лінгвістична невизначеність.
- 3.2. **Аналіз структури складних систем безпеки: Q-аналіз.** Симплекційний комплекс як модель системи складної структури. Алгоритми Q-аналізу: побудова структурного дерева та локальних карт, розрахунок ексцентриситетів.

- 3.3. **Ухвалення рішень в умовах ризику.** Дерево рішень. Основні елементи дерева рішень, алгоритм згортання дерева. Профіль ризику.
- 3.4. **Оцінка пріоритетів системою забезпечення безпеки.** Формування ієрархії задачі. Заповнення елементів матриці порівнянь. Оцінка значень змінних стану окремих сценаріїв.
- 3.5. **Стратегічне планування системою забезпечення кібербезпеки: SWOT - аналіз.** Правила здійснення SWOT - аналізу. Системна аналітика і SWOT – аналіз.
- 3.6. **Сучасні наукові концепції безпечного розвитку особи, суспільства та держави в кіберпросторі.** Концепція "суспільства ризику". Концепція "прийнятнього ризику". Концепція "стратегічних ризиків".
- 3.7. **Марківський випадковий процес з дискретним часом як модель зміни стану захищеності складних систем.** Кількісна оцінка стану захищеності складних систем за допомогою однорідного марківського ланцюга.
- 3.8. **Марківський випадковий процес з дискретним часом як модель зміни стану захищеності складних систем.** Кількісна оцінка стану захищеності складних систем за допомогою неоднорідного марківського ланцюга.
- 3.9. **Марківський випадковий процес з неперервним часом як модель зміни стану захищеності складних систем.** Кількісна оцінка стану захищеності складних систем за допомогою однорідного марківського процесу з неперервним часом.
- 3.10. **Марківський випадковий процес з неперервним часом як модель зміни стану захищеності складних систем.** Правила побудови диференціальних рівнянь Колмогорова для оцінки стану захищеності складних систем, що описуються марківськими процесами з неперервним часом.

4. Системи технічного захисту інформації

- 4.1. **Варіанти утворення небезпечних сигналів.**
- 4.2. **Поняття перетворювача фізичних величин.** Фізична природа первинних перетворювачів.
- 4.3. **Небезпечні сигнали.** Об'єкти захисту інформації. Розгляд системи ТЗПІ при організації захисту інформації.
- 4.4. **Акустoeлектричні перетворювання та перетворювачі.** Метод ВЧ наві'язування, як спосіб інформаційної атаки.
- 4.5. **Технічні заходи, спрямовані на захист інформації.** Перелік та опис.

- 4.6. **Основні канали витоку інформації на ОІД.** Організаційні заходи та технічні засоби протидії витоку мовної інформації з виділених приміщень.
- 4.7. **Методи та засоби активного захисту інформації,** поширюваної акустичними (мовними) каналами витоку в приміщеннях та каналах зв'язку.
- 4.8. **Межі ослаблення електромагнітних хвиль** для різних типів електромагнітних екранів. Конструкції екранів.
- 4.9. **Типи екранів.** Вимоги до безпомилкового монтажу електростатичного та електромагнітного екранів.
- 4.10. **Пошук закладних пристроїв.** Детектування диктофонів, котрі працюють в режимі запису. Нелінійна локація. Принцип роботи нелінійних локаторів.

1.2. Порядок проведення додаткового вступного випробування

Завдання додаткового вступного випробування складається з двох теоретичних питань. До екзаменаційного білету включаються відповідно: 1 питання з першого розділу, та 1 питання з другого, третього або четвертого розділів.

Додаткове вступне випробування зі спеціальності проводиться у формі усного екзамену. Тривалість підготовки вступника до відповіді – 60 хвилин. Після закінчення етапу підготовки до відповіді, проводиться заслуховування вступника та оцінювання всіма членами комісії. Члени предметної комісії приймають спільне рішення щодо виставлення оцінки на відповідь до кожного з питань екзаменаційного білету. Ці оцінки виставляються на аркуші з відповідями студента.

Підведення підсумку додаткового вступного випробування здійснюється шляхом занесення балів в екзаменаційну відомість. Ознайомлення вступника з результатами додаткового вступного випробування проводиться згідно з правилами прийому до університету.

1.3. Допоміжні матеріали для складання

Під час складання додаткового вступного випробування заборонено використання допоміжної літератури та інших допоміжних матеріалів та засобів.

1.4. Рейтингова система оцінювання (РСО)

Під час складання додаткового вступного випробування вступники виконують письмову контрольну роботу. Кожний екзаменаційний білет містить два теоретичні питання. Обидва завдання рівнозначні.

В залежності від повноти і правильності відповіді на питання вступник отримує:

46...50	балів за	91...100 %	правильної відповіді
41...45	балів за	81...90 %	правильної відповіді
36...40	балів за	71...80 %	правильної відповіді
31...35	балів за	61...70 %	правильної відповіді
26...30	балів за	51...60 %	правильної відповіді
21...25	балів за	41...50 %	правильної відповіді
16...20	балів за	31...40 %	правильної відповіді
11...15	балів за	21...30 %	правильної відповіді
6...10	балів за	11...20 %	правильної відповіді
1...5	балів за	5...10 %	правильної відповіді
0	балів за	0...5 %	правильної відповіді

Правильною відповіддю в даному контексті вважається повне і адекватне висвітлення питання згідно з програмою.

У відповідях на теоретичні завданнях екзаменаційного білета оцінюють:

- повноту розкриття питання;
- уміння чітко формулювати визначення понять/термінів та пояснювати їх;
- здатність аргументувати відповідь;
- аналітичні міркування, порівняння, формулювання висновків;
- акуратність оформлення письмової роботи.

Загальна оцінка за вступне випробування обчислюється як арифметична сума балів за дві відповіді на запитання екзаменаційного білету. Таким чином, згідно з рейтинговою системою оцінювання, за результатами вступного випробування вступник може набрати від 0 до 100 балів.

Вступники, результати додаткового вступного випробування яких за шкалою РСО складають від 60 до 100 балів, отримують оцінку "зараховано" і допускаються до складання вступного іспиту зі спеціальності.

Вступники, результати додаткового вступного випробування яких за шкалою РСО складають від 0 до 59 балів, отримують оцінку "не зараховано" і не допускаються до участі в наступних вступних випробуваннях і в конкурсному відборі.

1.5. Приклад типового завдання іспиту зі спеціальності

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»**

Освітній ступінь	доктор філософії
Спеціальність	F5 Кібербезпека та захист інформації
Освітня програма	Кібербезпека та захист інформації
Іспит	Додаткове вступне випробування

ЕКЗАМЕНАЦІЙНИЙ БІЛЕТ № 88

1. Визначення поняття «кібернетична загроза». Основні види кіберзагроз.
2. Задачі цифрового підпису. Загальна концепція та схема цифрового підпису з геш-функцією в асиметричній криптографії.

Затверджено на засіданні НМКУ
протокол № ____ від ____ березня 2025 р.

Гарант освітньої програми

Дмитро ЛАНДЕ

2. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

1. Особи, які без поважних причин не з'явилися на вступні випробування у визначений розкладом час, особи, знання яких було оцінено балами нижче встановленого рівня, до участі в наступних вступних іспитах і в конкурсному відборі не допускаються.
2. Перескладання вступних випробувань не допускається.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

Література до 1-го розділу

1. Богуш В.М. Інформаційна безпека від А до Я / Богуш В.М., Кудін А.М. - К.: МОУ, 1999. - 456 с.
2. Грайворонський М.В. Безпека інформаційно-комунікаційних систем: підручник для ВНЗ / Грайворонський М.В., Новіков О.М. – К.:Видавнича група BVH, 2009.– 608 с.
3. Закон України «Про інформацію», 1999 р.

4. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
5. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
6. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
7. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
8. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах

Література до 2-го розділу

9. Грайворонський М.В. Безпека інформаційно-комунікаційних систем: підручник для ВНЗ / Грайворонський М.В., Новіков О.М. – К.: Видавнича група ВНУ, 2009. – 608 с.
10. Антонюк А.О. Основи захисту інформації в автоматизованих системах: Навч. посіб. – К.: Видавничий дім «КМ Академія», 2003. – 243 с.
11. Математичні методи захисту інформації. Курс лекцій. Ч І. / Укладачі Завадська Л.О., Савчук М.М. – К.: НТУУ «КПІ», 2008. – 128 с.
12. Вербіцький О.В. Вступ до криптології. – Львів: Науково-технічна література, 1998. – 248с.
13. Шеховцов В. А. Операційні системи – К.: Видавнича група ВНУ, 2005. – 576 с.
14. Буров Є.В. Комп'ютерні мережі. / 2-е вид., оновл. і доп. – Львів: Бак, 2003.
15. Пасічник В.В. Організація баз даних та знань: підручник для ВНЗ / В.В. Пасічник, В.А. Резніченко. – К.: Видавнича група ВНУ, 2006. – 384с.
16. Антонюк А.О. Основи захисту інформації в автоматизованих системах: Навч. посіб. – К.: Видавничий дім «КМ Академія», 2003. – 243 с.
17. Menezes A. Handbook of Applied Cryptography / Menezes A., P. van Oorschot, S.Vanstone. – CRC Press, 1997. – 780 p.
18. Архипов О.Є. Захист інформації в телекомунікаційних мережах та системах зв'язку: навч.-метод. посібник / Архипов О.Є., Луценко В.М, Худяков В.О. - К.: ІВЦ "Видавництво "Політехніка", 2003. - 40 с.
19. Вінницький І.П. Термінальне устаткування та передавання інформації в телекомунікаційних системах / В.П.Вінницький, В.Г.Поліщук. – К.: ІВЦ "Видавництво «Політехніка»", 2004. – 436 с.
20. Khan S.A., Kumar R., Khan R.A. Software Security: Concepts & Practices. 2023 – 330 с.
21. Sirapat Boonkrong, Nakhon Ratchasima. Authentication and Access Control. Practical Cryptography Methods and Tools – 242 с.
22. Threat Modeling A Practical Guide for Development Teams. Yvonne Wilson, Abhishek Hingnikar. Solving Identity Management in Modern Applications. –398 с.

23. Andrew Hoffman. Web Application Security Exploitation and Countermeasures for Modern Web Applications – 330 с.
24. Організація комп'ютерних мереж [Електронний ресурс]: підручник: для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки»/ КПП ім. Ігоря Сікорського; Ю.А.Тарнавський, І.М.Кузьменко. – Електронні текстові дані (1 файл:45,7Мбайт). – Київ : КПП ім. Ігоря Сікорського, 2018. – 259с.
25. Tanenbaum, Andrew S., Computer networks / Andrew S. Tanenbaum, David J. Wetherall. — 5th ed. — Pearson Education, Inc., 2011. — 816 p. — ISBN-13: 978-0-13-212695-3
26. Kurose, James F., Computer Networking: A Top-Down Approach / James F. Kurose, Keith W. Ross. — 7th ed. — Pearson Education, Inc., 2017. — 864 p. — ISBN-13: 978-0-13-359414-0
27. Windows Internals, Seventh Edition, Part 1: System architecture, processes, threads, memory management, and more by Pavel Yosifovich, Alex Ionescu, Mark E. Russinovich, and David A. Solomon. - Microsoft Press, 2017. - ISBN: 978-0-7356-8418-8
28. Windows Internals, Seventh Edition, Part 2 by Andrea Allievi, Alex Ionescu, Mark E. Russinovich, and David A. Solomon. - Microsoft Press, 2021. - ISBN: 978-0-13-546240-9

Література до 3-го розділу

29. Качинський А.Б. Безпека складних систем: математичне моделювання небезпечних процесів і системний аналіз її забезпечення – К.: «Азимут-Україна», 2016. 498 с.
30. Архипов О. Є. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації / О. Е. Архипов, А. В. Скиба // Захист інформації. – 2012. – Т. 15. – № 4. – С. 366– 375.
31. Полуциганова В.І., Смирнов С.А. Методологія побудови основних метрик Q-аналізу та їх застосування // Системний аналіз та інформаційні технології, 2019, №3, с. 76-88.
32. Зайченко Ю.П. Теорія прийняття рішень: підручник .- НТУУ «КПІ», -2014. -412 с.
33. Томашевський В.М. Моделювання систем. -К.: Видавнича група ВНУ. -2005. - 352 с.
34. Волошин О.Ф., Мащенко С.О. Моделі та методи прийняття рішень. -Київ.; Університет. -2010. -336 с.

Література до 4-го розділу

35. Архипов О.Є. Захист інформації в телекомунікаційних мережах та системах зв'язку: навч.-метод. посібник / Архипов О.Є., Луценко В.М, Худяков В.О. - К.: ІВЦ "Видавництво "Політехніка", 2003. - 40 с.

36. Вінницький І.П. Термінальне устаткування та передавання інформації в телекомунікаційних системах / В.П.Вінницький, В.Г.Поліщук. – К.: ІВЦ “Видавництво «Політехніка»”, 2004. – 436 с.
37. Методи та засоби технічного захисту інформації. Опорний конспект лекцій [Електронний ресурс]: навч. посіб. для здобувачів ступеня бакалавра за освітньою програмою «Системи технічного захисту інформації» спеціальності 125 «Кібербезпека»/ КПІ ім. Ігоря Сікорського/ уклад.: В. М. Луценко, Д. О. Прогонов. – Київ: КПІ ім. Ігоря Сікорського, 2021. – 306 с. URI (Уніфікований ідентифікатор ресурсу): <https://ela.kpi.ua/handle/123456789/42397>.
38. Спеціальна техніка: підручник/ [Керницький І. С., Щур Б. В., Хараберюш І. Ф. та ін.]; за ред. професора І. С. Керницького. – Львів: Львівський державний університет внутрішніх справ, 2010. – 356 с.
39. Кобець М. В., Ланевський Е. В., Хахановський В. Г., Яковенко О. В. Засоби і системи зв'язку ОВС: Навчальний посібник. – К.: НАВСУ, 2004. – 83 с.
40. Зубок М. І. Охорона та охоронна діяльність: навчально-методичний посібник. – Київ, 2006. – 246 с.
41. Методичні рекомендації для проведення практичних занять та самостійної підготовки студентів з дисципліни «Технічні засоби охоронного призначення»/ Укладач: Ю. М. Крамаренко. – Запоріжжя: ЗНТУ, 2015. – 22 с.

РОЗРОБНИКИ ПРОГРАМИ:

д.т.н., зав. каф. ІБ, НН ФТІ



Дмитро ЛАНДЕ

к.т.н., проф. каф. ІБ, НН ФТІ



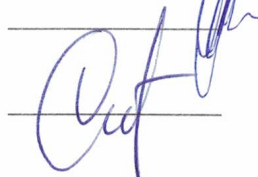
Євгеній МАЧУСЬКИЙ

к.т.н., зав. каф. ММЗІ, НН ФТІ



Сергій ЯКОВЛЕВ

к.ф.-м.н., доц. каф. ІБ, НН ФТІ



Сергій СМІРНОВ