МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

ЗАТВЕРДЖЕНО:
в.о. президента ДУ КАІ
_____Ксенія СЕМЕНОВА
«11» 04 2025 року

ПРОГРАМА
ВСТУПНОГО ВИПРОБУВАННЯ ДО АСПІРАНТУРИ

зі спеціальності F5 Кібербезпека та захист інформації

на здобуття ступеня доктора філософії

третього (освітньо-наукового) рівня вищої освіти

Галузь знань F Інформаційні технології

Освітньо-наукова програма «Кібербезпека»

Київ – 2025

ВСТУП

Програма фахового вступного випробування до аспірантури за галуззю знань F «Інформаційні технології» за спеціальністю F5 «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 рівня знань за напрямами професійної діяльності. Вступник повинен продемонструвати фундаментальні, професійно-орієнтовні знання та уміння, здатність вирішувати типові професійні завдання, передбачені програмою вступу, 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 F «Інформаційні технології» за спеціальністю F5 «Кібербезпека та захист інформації».

1. ПЕРЕЛІК ПИТАНЬ ДЛЯ ПІДГОТОВКИ ДО ВСТУПНОГО ВИПРОБУВАННЯ

1.1. ПРИКЛАДНА КРИПТОЛОГІЯ

1. Охарактеризуйте та проведіть класифікацію шифрів однозначної заміни. Наведіть приклад шифрування методом Цезаря.
2. Охарактеризуйте та проведіть класифікацію поліграмних шифрів. Наведіть приклад шифру Playfair.
3. Охарактеризуйте та проведіть класифікацію поліалфавітних шифрів. Наведіть приклад шифрування методом Віженера.
4. Охарактеризуйте шифр гамування. Наведіть приклад.
5. Проведіть загальну класифікацію шифрів. Назвіть умови стійкості шифрів.
6. Проведіть порівняльний аналіз властивостей випадкових та псевдовипадкових послідовностей в криптосистемах.
7. Проведіть класифікацію криптографічно стійких генераторів псевдовипадкових чисел.
8. Охарактеризуйте алгоритм Блюм-Блюма-Шуба (BBS). Наведіть приклад
9. Охарактеризуйте лінійний конгруентний метод генерування псевдовипадкових чисел. Наведіть приклад.

10. Опишіть особливості застосування MDC та MAC кодів.
11. Охарактеризуйте алгоритм гешування SHA-1.
12. Охарактеризуйте режими роботи та типи реалізації алгоритмів блочного симетричного шифрування.
13. Охарактеризуйте стандарт шифрування DES.
14. Охарактеризуйте стандарт шифрування AES.
15. Охарактеризуйте стандарт шифрування ДСТУ 28147:2009.
16. Охарактеризуйте стандарт шифрування ДСТУ Калина.
17. Охарактеризуйте потоковий алгоритм шифрування RC4.
18. Проведіть аналіз асиметричних криптографічних перетворень. Модель асиметричної криптосистеми.
19. Охарактеризуйте алгоритм RSA. Наведіть приклад.
20. Охарактеризуйте алгоритм Ель-Гамаля. Наведіть приклад.
21. Охарактеризуйте алгоритм Шаміра. Наведіть приклад.
22. Охарактеризуйте алгоритм Рабіна. Наведіть приклад.
23. Охарактеризуйте процедуру шифрування та дешифрування з використанням еліптичних кривих. Наведіть приклад.
24. Поясність основні напрями використання криптографічних систем, які засновані на базі еліптичних кривих.
25. Охарактеризуйте принципи формування та класифікацію електронного підпису. Наведіть приклади.
26. Охарактеризуйте принципи формування та верифікації електронно підпису з використанням алгоритму DSA. Наведіть приклад.
27. Охарактеризуйте принципи формування та верифікації електронно підпису з використанням алгоритму ECDSA. Наведіть приклад.
28. Охарактеризуйте функції і проведіть класифікацію систем управління криптографічними ключами. Наведіть приклад реалізації схеми Діффі-Хеллмана.
29. Охарактеризуйте принципи автентифікації на основі шифрування з відкритим ключем. Наведіть приклад схеми Клауса Шнорра.
30. Охарактеризуйте особливості реалізації комбінованої криптографічної системи. Наведіть приклад.

1.2. БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

1. Охарактеризуйте комп'ютерні віруси та антивіруси. Охарактеризуйте SpyWare, AdWare та інше шкідливе програне забезпечення.
2. Опишіть засоби виявлення шкідливого програного забезпечення.

3. Розкрийте поняття «ідентифікація» та «автентифікація». Опишіть типи автентифікації. Охарактеризуйте методи та системи автентифікації. Наведіть класифікацію систем ідентифікації та автентифікації.

4. Охарактеризуйте технології біометричної ідентифікації. Наведіть їх класифікацію.

5. Охарактеризуйте PE-файли та їх структура. Опишіть механізми модифікації PE-файлів. Опишіть аналіз структури та вмісту PE-файлів, який доцільний для вирішення задач кібербезпеки.

6. Опишіть захист операційної системи WINDOWS.

7. Охарактеризуйте засоби адміністрування операційної системи WINDOWS.

8. Опишіть парольний захист операційної системи WINDOWS. Порівняйте організацію парольного захисту для різних версій операційної системи WINDOWS.

9. Опишіть механізми забезпечення безпеки даних в комп'ютерних мережах.

10. Охарактеризуйте вразливості веб-серверів.

11. Охарактеризуйте види кібератак та способи запобігання їм. Опишіть DOS та DDOS-атаки. Опишіть механізми виявлення DOS та DDOS-атак та захисту від них.

12. Охарактеризуйте системи SIEM, принцип роботи, функції. Наведіть класифікацію рішень SIEM, приклади. Охарактеризуйте системи SOAR, принцип роботи, функції, приклади.

13. Охарактеризуйте системи виявлення та запобігання вторгнень.

14. Охарактеризуйте DLP-системи, їх призначення, принцип дії, технології, приклади.

15. Розкрийте основні поняття захисту інформації і інформаційної безпеки.

16. Охарактеризуйте підходи до забезпечення безпеки інформаційних систем. Опишіть аналіз загроз інформаційної безпеки.

17. Опишіть механізми забезпечення безпеки та архітектуру підсистеми захисту операційних систем.

18. Розкрийте основні поняття політики безпеки. Охарактеризуйте структуру політики безпеки організації.

19. Розкрийте поняття шкідливого програмного забезпечення: механізми поширення, виявлення та протидії вірусам, руткітам та експлойтам.

20. Опишіть технології аналізу захищеності і виявлення атак.

21. Охарактеризуйте технології автентифікації.

22. Опишіть застосування систем виявлення вторгнень до корпоративних мереж.

23. Охарактеризуйте особливості функціонування міжмережевих екранів на різних рівнях моделі OSI.

24. Опишіть інфраструктуру захисту на прикладному рівні.

25. Опишіть концепцію побудови віртуальних захищених мереж VPN. Назвіть переваги застосування технологій VPN.

26. Опишіть протоколи формування захищених каналів на канальному рівні.

27. Опишіть протоколи формування захищених каналів на сеансовому рівні.

28. Охарактеризуйте захист на мережному рівні — протокол IPSec.

29. Опишіть методи управління засобами мережевої безпеки.

30. Опишіть організацію захищеного віддаленого доступу.

1.3. НОРМАТИВНО ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1. Проведіть класифікацію інформації за правовим режимом доступу. Визначте перелік інформації, що мають обмежений доступ.

2. Визначте цілі та напрями державної політики в науковій і науково-технічній діяльності.

3. Основні заходи щодо розвитку національної складової глобальної інформаційної мережі.

4. Охарактеризуйте правові основи розвитку та діяльності галузі інформатизації та науково-технічної діяльності Україні.

5. У чому полягає охорона таємниці інформації, що передається засобами зв'язку?

6. Розкрийте поняття національної системи конфіденційного зв'язку та її складових.

7. Наведіть основні види загрози інформації в інфотелекомунікаційних системах.

8. Розкрийте питання КСЗІ в телекомунікаційних системах, а також висвітліть порядок розроблення та впровадження КСЗІ

9. Які організаційні та правові засади технічного захисту інформації в Україні?

10. У чому полягає правовий статус та який порядок використання електронно-цифрового підпису?

11. Який порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації?

12. Назвіть суб'єкти відносин, пов'язаних з обробленням інформації в автоматизованих системах.

13. Охарактеризуйте основи регулювання правових відносин щодо захисту інформації в автоматизованих системах.

14. Проведіть класифікацію класів та підкласів автоматизованих систем.

15. Вкажіть особливості захисту інтересів держави в інформаційній сфері

16. Наведіть суб'єкти та об'єкти захисту інформаційних ресурсів

17. Який контроль за функціонуванням системи технічного захисту інформації

18. Вкажіть основні положення концепції інформаційної безпеки

19. Наведіть принципи формування і проведення державної політики у сфері ТЗІ.

20. Назвіть загальні положення щодо розвитку інформатизації та науково-технічної діяльності в Україні.

21. Вкажіть порядок проведення робіт із сертифікації засобів ТЗІ

22. Вкажіть правові основи розвитку та діяльності галузі інформатизації та науково-технічної діяльності Україні.

23. Проведіть класифікацію інформації за правовим режимом доступу.

24. Визначте перелік інформації, що має обмежений доступ.

25. Розкрийте питання програми інформатизації України.

26. Які організаційні та правові засади технічного захисту інформації в Україні?

27. Як проводиться державна експертиза у сфері технічного захисту інформації?

28. Яка концепція технічного захисту інформації в Україні?

29. Яка основна мета і завдання сертифікації засобів забезпечення ТЗІ загального призначення?

30. Охарактеризуйте основні напрями забезпечення інформації безпеки.

Програму розробили:

Завідувач кафедри кібербезпеки, к.т.н., доц. Анна ІЛЬЄНКО

Заступник декана з наукової роботи
факультету комп'ютерних наук та технологій,
к.т.н., ст. дослідник Тетяна ОХРІМЕНКО

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	70
Виконання завдання №2	70
Виконання завдання №3	60
Усього	200

Значення рейтингових оцінок за виконання завдань вступного іспиту та їх критерії

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

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

1. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч.посібник / Г. Л. Козіна. – Запоріжжя : НУ «Запорізька політехніка», 2020. – 192 с.

2. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. – 120 с.

3. Anubhab Baksi. Classical and Physical Security of Symmetric Key Cryptographic Algorithms (Computer Architecture and Design Methodologies). Springer. 2022 . – 300 p.

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. Безпека інформації : конспект лекцій / укладач О. С. Кушнерьов. – Суми: Сумський державний університет, 2021. – 99 с.

6. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А.,Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах : навч. посіб. —Кропивницький: Видавець Лисенко В. Ф., 2020. — 295 с.

7. Богуш В.М., Богуш В.В. Основи кіберпростору, кібербезпеки та кіберзахисту : навч. посіб. Київ : Ліра-К, 2020. 552 с.

8. Лаптєв О.А. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності: навчальний посібник / О.А. Лаптєв, В.А. Савченко, Г.В. Шуклін. – К.: ДУТ, 2020.

9. Dr.Sonali Ridhorkar. Elliptic Curve Cryptography: Implementation Issues: Key Establishment Protocol. LAP LAMBERT Academic Publishing. 2021. – 152 p.

10. Aiden A. Bruen, Mario A. Forcinito, James M. McQuillan Cryptography, Information Theory, and Error-Correction. Wiley. 2021. – 688 p.

11. Duncan Buell. Fundamentals of Cryptography: Introducing Mathematical and Algorithmic Foundations. Springer. 2021. – 296 p.

12. Lisa Bock. Modern Cryptography for Cybersecurity Professionals. Packt Publishing. 2021. – 286 p.

13. О. Г. Додонов, Д. В. Ланде, В. Г. Путятін. Інформаційні потоки в глобальних комп'ютерних мережах. — К.: Наук, думка, 2009. – 295 с

14. Тимошенко А.О. Методи аналізу та проектування систем захисту інформації:курс лекцій.-.:Політехніка, 2007. – 174 с.

15. Остапов С. Е. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці : Видавничий дім "РОДОВІД", 2014. – 428 с.

16. Даник Ю. Г. Основи кібернетичної безпеки: монографія / Ю. Г. Даник, Р. В. Грищук; за заг. ред. проф. Ю. Г. Даника. – Житомир: ЖНАЕУ, 2016. – 636с.

17. Brooks C. J., Grow, C., Craig, P., & Short, D. Cybersecurity essentials. John Wiley & Sons, 2018. 767 p.

(Ф 03.02 - 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки

(Ф 03.02 -02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

№ п/п	Прізвище ім'я по-батькові	Підпис ознайомленої особи	Дата ознайомлення	Примітки

(Ф 03.02 -03)

АРКУШ ОБЛІКУ ЗМІН

№ зміни	№ листа (сторінки)				Підпис особи, яка внесла зміну	Дата внесення зміни	Дата введення зміни
	зміненого	заміненого	нового	анульованого			

(Ф 03.02 -04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЙ

№ пор.	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності