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

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

ПРОГРАМА
ДОДАТКОВОГО 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

Програма додаткового вступного випробування до аспірантури зі спеціальності F5 Кібербезпека та захист інформації відображає такі розділи теоретичних та практичних основ у сфері кібербезпеки:

— основи кібербезпеки;

— комп'ютерні системи та мережі;

— операційні системи та технології їх захисту.

1. ПЕРЕЛІК ПИТАНЬ ДЛЯ ПІДГОТОВКИ ДО ДОДАТКОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

1.1. ОСНОВИ КІБЕРБЕЗПЕКИ

1. Дайте визначення поняттю та категорії теорії національної безпеки.
2. Дайте визначення факторам забезпечення національної безпеки в основних сферах.
3. Дайте визначення системи забезпечення національної безпеки. Назвіть функції системи забезпечення національної безпеки.
4. Охарактеризуйте основні види національної безпеки України
5. Загрози інформаційній безпеці. визначте дестабілізуючі фактори інформаційної безпеки
6. Чому полягають основні принципи забезпечення інформаційної безпеки.
7. Дайте визначення поняттям інформаційна війна, тероризм, злочинність.
8. Вкажіть відмінності інформаційної зброї воєнного та невоєнного застосування.
9. Вкажіть основні організаційні напрями протидії загрозам у сфері інформаційної безпеки.
10. Основні напрями забезпечення безпеки інформації держави.
11. У чому полягає правовий статус та який порядок використання кваліфікованого-електронного підпису ?
12. Який порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації?
13. Охарактеризуйте основи регулювання правових відносин щодо захисту інформації в автоматизованих системах.
14. Проведіть класифікацію класів та підкласів автоматизованих систем.
15. Що таке функціональний профіль захищеності? Наведіть приклад.

1.2. КОМП'ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖІ

1. Назвіть основні властивості та технології локальних і глобальних мереж.
2. Опишіть структуру стандартів IEEE 802.x

3. Опишіть технологію Frame Relay.
4. Опишіть принципи роботи маршрутизатора.
5. Назвіть основні види фізичного та логічного кодування.
6. Опишіть принципи роботи комутаторів.
7. Назвіть основні характеристики технології FDDI.
8. Опишіть особливості адресація за протоколами IPv4 та IPv6.
9. Назвіть основні характеристики технології локальних мереж Token Ring.
10. Назвіть основні характеристики Ethernet та Fast Ethernet.
11. Опишіть лінії зв'язку та типи кабелю в комп'ютерній мережі.
12. Назвіть основні характеристики Gigabit Ethernet.
13. Опишіть функції та параметри мережних адаптерів.
14. Дайте визначення статичної маршрутизації. Наведіть приклад налаштування.
15. Дайте визначення динамічної маршрутизації. Наведіть приклад налаштування.

1.3. ОПЕРАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ ЇХ ЗАХИСТУ

1. Моделі безпеки операційних систем: порівняння моделей Белла-Лападули, Брюера-Неша та Кларка-Вілсона.
2. Архітектура безпеки ядра операційних систем: принципи роботи механізмів контролю доступу.
3. Механізми аутентифікації в операційних системах: паролі, біометрія, токени, багатофакторна аутентифікація.
4. Механізми авторизації та управління доступом в ОС: порівняння моделей ACL (Access Control List) та RBAC (Role-Based Access Control).
5. Принципи захисту пам'яті в операційних системах: ASLR, DEP, контроль стеку.
6. Механізми контролю та моніторингу активності користувачів в ОС: системні журнали (log files), засоби аудиту.
7. Управління правами та політиками безпеки в ОС Windows та Linux: аналіз та налаштування Group Policy, SELinux, AppArmor.
8. Захист файлової системи: методи шифрування (BitLocker, LUKS), журнальні та криптографічні файлові системи.
9. Шкідливе програмне забезпечення в ОС: механізми поширення, виявлення та протидії вірусам, руткітам та експлойтам.

10. Захист мережевих з'єднань в ОС: налаштування брандмауерів (Windows Firewall, iptables), VPN, IPSec.

11. Безпека віртуалізації та контейнеризації: ризики та механізми захисту (Hyper-V, VMware, Docker, LXC).

12. Програмні вразливості ОС: буферний переповнення (Buffer Overflow), ін'єкції коду, атаки на привілеї.

13. Механізми оновлення та патч-менеджменту: автоматичне оновлення ОС, управління вразливостями (WSUS, unattended-upgrades).

14. Методи форензічного аналізу операційних систем: виявлення та аналіз слідів злому, відновлення даних після атак.

15. Захист вбудованих систем та IoT-пристроїв: особливості безпеки операційних систем реального часу (RTOS) та IoT-середовищ.

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. СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. 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.

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

3. 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.

4. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. Вступ до кібербезпеки:навч. посіб. – Кропивницький: ЦНТУ, 2022. – 967 с.

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

6. 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.

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

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

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

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

11. 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