**ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ**
**ПРИЙМАЛЬНА КОМІСІЯ**

ЗАТВЕРДЖЕНО
Голова приймальної комісії
_____ Анатолій МАЗАРАКІ
«27» березня 2025 р.

# ПРОГРАМА

## фахового іспиту замість ЄФВВ для вступу на навчання для здобуття освітнього ступеня магістра на основі НРК6 та НРК7

| | |
|---|---|
| **галузь знань** | **F «Інформаційні технології»** |
| **спеціальність** | **F5 «Кібербезпека та захист інформації»** |
| **факультет** | **Інформаційних технологій** |
| **освітня програма** | **«Кібербезпека та захист інформації»** |

**Київ 2025**

## ВСТУП

Програма фахового іспиту для здобуття освітнього ступеня «магістр» за галуззю знань F «Інформаційні технології» спеціальністю F5 «Кібербезпека та захист інформації» підготовлена на основі освітньо-професійної програми, яка забезпечує комплексний підхід до оцінки рівня теоретичної та практичної підготовки вступників до професійної діяльності.

Мета фахового іспиту – визначити обсяг та рівень теоретичних знань, практичних навичок та вмінь з профілюючих дисциплін у галузі інформаційних технологій, які пов’язані з усіма аспектами захисту інформації в системах і мережах, методами забезпечення кібербезпеки та криптографічними методами захисту інформації.

Фаховий іспит проводиться у вигляді тестування.

Програма містить такі розділи:

1. Соціотехнічна кібербезпека.
2. Архітектура комп’ютера.
3. Безпека операційних систем.
4. Організація комп’ютерних мереж.
5. Безпека баз даних.
6. Безпека інформаційних систем та мереж.
7. Криптографічні методи захисту інформації.

## ЗМІСТ ПРОГРАМИ ФАХОВОГО ІСПИТУ

### Розділ 1. СОЦІОТЕХНІЧНА КІБЕРБЕЗПЕКА

Поняття інформаційна безпека, кібербезпека, кіберпростір, кібероборотьба, кібертероризм, кібервійна, кіберзброя. Основні поняття кіберзахисту. Основи кібервпливу. Зміст, класифікація та ознаки кіберзагроз.

Модель кібербезпеки та тріада КЦД. Куб кібербезпеки. Принципи конфіденційності, цілісності, доступності. Захист конфіденційності даних. Керування доступом. Закони та відповідальність. Перевірка цілісності. Забезпечення доступності. Домени кібербезпеки.

Комп'ютерні атаки та технології їхнього виявлення. Сутність, класифікація та етапи реалізації атак. Загальні поняття про комп’ютерні віруси, історія їх виникнення та розвитку. Загальні принципи функціонування комп’ютерних вірусів, їх розмноження. Класифікація комп’ютерних вірусів і принципи її побудови. Алгоритми роботи вірусів. Основні типи шкідливого програмного забезпечення, шляхи розповсюдження та симптоми зараження ними.

Методи та засоби протидії соціотехнічним атакам. Канали несанкціонованого доступу до інформації. Методи і засоби соціального інжинірингу.

Криптографія, основні типи шифрів. Симетричні та асиметричні методи шифрування. Криптографічні протоколи та їх класифікація. Ідентифікація, аутентифікація та авторизація.

Комп'ютерна і цифрова стеганографія, цифрові водяні позначки. Модель комп'ютерної стеганографічної системи. Атаки на стеганосистеми.

Основні методи забезпечення кібербезпеки. Технології реагування на інциденти. Системи виявлення вторгнень. Системи запобігання вторгненням. Протоколи WEP, WPA/WPA2. Безпечний віддалений доступ. Захист мережних пристроїв.

## Розділ 2. АРХІТЕКТУРА КОМП'ЮТЕРА

Поняття архітектури ПК. Історія розвитку комп'ютерів та їх основні етапи. Архітектура фон Неймана. Основні компоненти комп'ютера та їх ролі у функціонуванні системи. Основні показники та характеристики комп'ютерів. Принципи побудови та функціонування комп'ютерів. Види комп'ютерів та їх властивості.

Представлення даних у комп'ютері. Типи, форми та формати подання інформації у ПК. Логічні операції, логічні операції з двійковими числами. Логічні елементи. Елементи пам'яті, тригери, регістри. Лічильники. Оперативна пам'ять.

Класифікація материнських плат. Функції материнської плати в комп'ютері. Компоненти з яких складається материнська плата та їх роль. Типи роз'ємів на материнській платі і як вони використовуються. Особливості роботи материнської плати з оперативною та постійною пам'яттю. Фактори які впливають на продуктивність материнської плати та способи покращення її роботи. Чипсети. Північний та південний міст. Програмні засоби тестування чипсет.

Структура та функції центрального процесора. Архітектура процесора та його основні компоненти. Поняття розрядності процесора. Принцип роботи кеш-пам'яті. Особливості взаємодії процесора з іншими компонентами комп'ютера.

Структура і принцип роботи жорстких дисків. Технології виготовлення і характеристики жорстких дисків. Форм-фактори жорстких дисків і їх використання в різних пристроях. Файлові системи, які використовуються на жорстких дисках. Сучасні тенденції в розвитку жорстких дисків.

Послідовні та паралельні порти введення/виведення. Типи портів. Інтерфейси шин. Протоколів передачі даних через порти та шини. Види кабелів та конекторів, що використовуються для підключення до портів та шин. Робота контролерів портів та шин. Сумісності портів та шин між різними пристроями. Інтерфейси бездротового підключення периферійних пристроїв.

Комп'ютерний блок живлення. Системна шина (FSB). Шина даних.

Типи оперативної пам'яті. Характеристики оперативної пам'яті та її продуктивність. Процеси які відбуваються під час зчитування та запису даних в оперативну пам'ять. Фактори які впливають на швидкість роботи оперативної пам'яті. Способи та програмні засоби тестування оперативної пам'яті.

Історія розвитку операційної системи MS DOS і її архітектура. Основні концепції та інтерфейс MS DOS. Системні вимоги до MS DOS. Основні проблеми безпеки та захисту інформації в операційній системі MS DOS. Порівняння MS DOS з іншими операційними системами, такими як Windows та Linux.

BIOS і які функції він виконує в комп'ютері. Основні компоненти BIOS. Налаштування BIOS. Різновиди BIOS. Спеціальні утиліти для роботи з BIOS. Забезпечити безпеку при роботі з BIOS.

Компоненти з яких складається відеосистема комп'ютера. Різновиди відео карт. Вплив відеокарти на продуктивність комп'ютера. Основні характеристики та параметри відеокарт. Робота відеокарта та її функції. Інтерфейси для підключення відеокарт до комп'ютера. Робота монітора для відображення графічної інформації. Основні характеристики моніторів і як вони впливають на якість відображення зображення.

Програма самотестування комп’ютерів POST. Усунення помилок та обслуговування комп’ютерів. Методика обслуговування комп’ютерів та її особливості.

## Розділ 3. БЕЗПЕКА ОПЕРАЦІЙНИХ СИСТЕМ

Поняття операційної системи, її призначення та функції. Історія розвитку операційних систем. Класифікація сучасних операційних систем. Функціональні компоненти операційних систем.

Поняття архітектури операційних систем. Взаємодія операційної системи з апаратним забезпеченням. Взаємодія операційної системи з програмним забезпеченням. Підходи до реалізації архітектури операційних систем. Архітектура системи UNIX. Архітектура системи Linux. Архітектура системи Windows.

Базові поняття процесів і потоків. Багатопотоковість та її реалізація. Стани процесів і потоків. Опис процесів і потоків. Загальні принципи планування. Види планування. Стратегії планування. Витісняюча та невитісняюча багатозадачність. Алгоритми планування. Реалізація планування в Linux. Реалізація планування у Windows.

Основні принципи взаємодії потоків. Взаємодія потоків у Linux. Взаємодія потоків у Windows.

Основи технології віртуальної пам’яті. Сегментація пам’яті. Сторінкова організація пам’яті. Сторінково-сегментна організація пам’яті. Реалізація керування основною пам’яттю у Linux. Реалізація керування основною пам’яттю у Windows.

Динамічна ділянка пам’яті процесу. Особливості розробки розподілювачів пам’яті. Послідовний пошук підходящого блоку. Ізольовані списки вільних блоків. Системи двійників. Підрахунок посилань і збирання сміття. Реалізація динамічного керування пам’яттю в Linux. Реалізація динамічного керування пам'яттю в Windows.

Поняття файлу і файлової системи. Організація інформації у файловій системі. Зв’язки. Атрибути файлів. Операції над файлами і каталогами. Налагодження взаємодії між процесами на основі інтерфейсу файлової системи.

Базові відомості про дискові пристрої. Розміщення інформації у файлових системах. Продуктивність файлових систем. Надійність файлових систем.

Файлові системи ext2fs і ext3fs. Файлові системи лінії FAT. Файлова система NTFS. Особливості кешування у Windows. Системний реєстр Windows.

Вертикальна декомпозиція архітектури ОС Windows. Компоненти комплексу засобів захисту (КЗЗ) Windows. Взаємодія компонентів й бази даних (БД) системи безпеки. Основні принципи реалізації системи розмежування доступу. Суб'єкти доступу Windows. Стандартні суб'єкти доступу. Стандартні типи об'єктів доступу Windows. Методи доступу. Специфічні методи доступу для деяких об'єктів. Спеціальні привілеї. Права доступу. Об'єкти із стандартним та нестандартним захистом. Посилання процесу на об'єкт по існуючому визначнику. Модель захисту Windows для Win32. Ідентифікатори захисту SID. Маркери. Ідентифікатори маркера. Дескриптори захисту. Списки керування доступом. Алгоритми з'ясування прав доступу. Позначення в описі алгоритмів. Алгоритм з'ясування максимальних прав доступу. Архітектура підсистеми автентифікації Windows. Послідовність входу користувача в систему. Особливості підсистеми автентифікації Windows. Загальна оцінка системи Windows.

Модель безпеки системи UNIX. Підсистема ідентифікації та автентифікації (традиційна). Підсистема ідентифікації та автентифікації (сучасна). Налаштування PAM. Модулі PAM. Приклади модулів PAM. Підсистема розмежування доступу. Опис прав доступу до файлу. Списки керування доступом (Solaris, Linux). Суперкористувач в UNIX. Захист від використання вразливостей коду – ASLR. Основні недоліки традиційної моделі безпеки Linux і Unix.

## Розділ 4. ОРГАНІЗАЦІЯ КОМП'ЮТЕРНИХ МЕРЕЖ

Комп'ютерні мережі, їх класифікація та призначення. Концепції побудови комп'ютерних мереж: локальні та глобальні комп'ютерні мережі. Типи локальних комп'ютерних мереж: однорангові мережі та мережі побудовані на основі клієнт / сервер-технологіях. Особливості і доцільність використання.

Поняття та порівняння комутації пакетів та комутації каналів.

Базові топології комп'ютерних мереж. Еталонна мережна модель OSI як глобальний стандарт для визначення функціональних рівнів, необхідних для підтримки з'єднання між комп'ютерами. Поняття мережних стеків. Мережний рівень, його призначення. Поняття дейтаграми.

Рівень маршрутизації, його зв'язок з мережними протоколами, поняття протоколів з установленим з'єднанням та без встановленого з'єднання.

Архітектура Ethernet. Сучасні стандарти Ethernet: Fast Ethernet та Gigabit Ethernet. Архітектура Token Ring. Перспективи розвитку Token Ring. Технологія FDDI. Місце технології FDDI на сучасному ринку технологій комп'ютерних мереж. Технологія ATM. Перспективи впровадження технології ATM.

Апаратні засоби комп'ютерних мереж: призначення та їх класифікація. Типи апаратних засобів, критерії вибору, співвідношення між їх функціями та рівнями моделі OSI. Вплив топології на вибір апаратних засобів. Лінії зв'язку, їх типи та основні характеристики. Стандарти кабелів: кабелі на основі неекранованої звитої пари; кабелі на основі екранованої пари; волоконно-оптичні кабелі, одномодові та багатомодові.

Мережева операційна система – основа функціонування комп’ютерних мереж. Функціональна структура та стандартні служби мережевої операційної системи.

Технології мобільного доступу в Інтернеті. Базові технології мобільного зв’язку: першого покоління – GPRS, EGPRS; другого покоління – CDMA – 2000. Безпровідні комп’ютерні мережі.

## Розділ 5. БЕЗПЕКА БАЗ ДАНИХ

Реляційний підхід до організації баз даних / Міжтабличні зв'язки в реляційній базі даних: відношення «один-до-одного», «один-до-багатьох», «багато-до-багатьох».

Проблеми маніпулювання даними та обмеження цілісності даних. Поняття цілісності даних. Підтримка цілісності в реляційних базах даних. Засоби контролю цілісності інформації. Обмеження цілісності. Потенційні та зовнішні ключі. Нормалізація відношень. Нормальні форми.

Функціональна мова SQL. Категорії операторів SQL. Схеми даних. Технологія створення таблиць бази даних та ключових полів. Прості представлення мови SQL для вибірки даних. Багатотабличні запити відбору даних. Збережені процедури в системах управління базами даних.

Обробка транзакцій. Створення та управління транзакціями. Журнал транзакції. Логічна та фізична архітектура журналу транзакцій.

Створення резервних копій бази даних. Критерії вибору стратегій резервного копіювання. Типи резервних копій баз даних.

Відновлення системи баз даних. Методи автоматичного і ручного відновлення бази даних. Моделі відновлення баз даних. Точність відновлення або точка повернення. Швидкість відновлення або час відновлення. Відновлення бази даних до точки збою.

Забезпечення безпеки БД на основі концепції об'єктів, що захищаються. Дозволи на доступ до об'єктів. Засоби аутентифікації об'єктів баз даних. Режими аутентифікації.

Забезпечення доступності систем БД на основі ролей. Три рівні безпеки БД: рівень сервера, рівень бази даних, рівень схеми.

Верифікація баз даних і проведення аудиту бази даних. Організація аудиту подій в системах керування базами даних. Ведення журналу аудиту.

Моніторинг продуктивності сервера баз даних. Моніторинг активності користувачів на рівні СКБД.

Управління ключами безпеки. Шифрування даних.

## Розділ 6. БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Види можливих порушень в роботі інформаційної системи. Розголошування. Витік інформації. Несанкціонований доступ до системи або мережі. Загрози інформації. Основні поняття і класифікація загроз. Основні загрози доступності. Основні загрози цілісності. Основні загрози конфіденційності. Порушники інформаційної безпеки. Класифікація порушників. Методика вторгнення. Умови, що сприяють неправомірному

оволодінню інформацією. Канали витоку інформації та перехоплення даних. Модель безпеки: структура і компоненти. Засоби забезпечення безпеки інформаційних систем і мереж. Призначення і завдання у сфері забезпечення інформаційної безпеки на рівні держави. Міжнародні стандарти інформаційної безпеки. Державний стандарт України із захисту інформації.

Стандарти інформаційної безпеки. Критерії оцінювання захищеності інформаційної системи. «Критерії оцінки довірених комп'ютерних систем» («Помаранчева книга»). Міжнародний стандарт побудови ефективної системи безпеки ISO 17799. Аналіз засобів порушення інформаційної безпеки. Інженерно-технічний рівень інформаційної безпеки. Технічні засоби для несанкціонованого доступу до інформації. Засоби протидії несанкціонованому доступу до інформації. Канали витоку інформації. Захист інформації від витоку по технічним каналам. Апаратні засоби захисту. Програмні засоби захисту.

Основні терміни та поняття криптографії. Одноалфавітні системи шифрування Віженера, Плейфейра та інші. Багатоалфавітні системи шифрування: Бьюфорта, Віженера та інші Основні типи алгоритмів шифрування. Електронний цифровий підпис. Управління ключами та сертифікація ключів. Стеганографічні методи захисту інформації. Поняття і класифікація комп'ютерних вірусів. Коротка характеристика вірусів. Програмні закладки. Програми – шпигуни і логічні бомби. Антивірусні програми. Корпоративні антивіруси. Правила використання стороннього програмного забезпечення. Спам і засоби боротьби з ним. Фішинг.

Правила безпечної роботи в мережах. Захист на мережевому рівні. Системи виявлення вторгнення в безпроводові мережі.

## Розділ 7. КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

Базові поняття криптографії. Поняття та види шифрів: шифр простої заміни, шифри перестановки, шифр багатоалфавітної заміни. Роль криптографії у захисті даних. Поняття та види шифрів. Вимоги до шифрів – принцип Керкгоффса. Шифрувальні машини та підходи до їх аналізу. Ідеальний шифр і класи стійкості шифрів.

Основні види криптографічних методів. Реалізація криптографічних методів. Симетричні і асиметричні методи шифрування. Шифри на основі мережі Фейстеля. Мережа Фейстеля. Американський шифр DES. Шифри на основі SP-мережі.

Сучасні блокові шифри. Компоненти сучасного блокового шифру. Розгляд відомих блокових шифрів (ГОСТ 28147, DES, AES, ДСТУ 7624 і т.д.). Переваги недоліки. Складені шифри. Режими роботи блокових шифрів.

Криптографічне перетворення. Симетричні криптографічні перетворення. Методи генерації псевдовипадкових числових послідовностей. Модулярна арифметика. Створення комбінованих криптографічних засобів та нові підходи до побудови шифрів.

Криптосистема Ель-Гамаля. Шифрування та розшифрування в криптосистемі Ель-Гамаля. Коректність, ефективність та надійність криптосистем Рабіна та Ель-Гамаля. Криптосистема Діфі-Хелмана.

Шифрування та розшифрування в криптосистемі Діфі-Хелмана. Коректність, ефективність та надійність криптосистем Діфі-Хелмана.

Принципи еліптичної криптографії. Методи шифрування в еліптичній криптографії. Алгебраїчні операції в скінчених полях. Особливості програмної реалізації операції над точками еліптичної кривої.

Поняття криптографічних протоколів. Їх опис. Класифікація криптографічних протоколів. Властивості, що визначають безпеку криптографічних протоколів. Атаки на протоколи. Аналіз та моделювання криптографічних протоколів. Протоколи електронного цифрового підпису.

Принцип Керкгоффса. Стандарти генерації ключів. Накопичення, розподілення, оновлення, зберігання, резервування ключів. Генерація та модифікація ключа. Зберігання та розподіл ключів. Протоколи обміну ключами. Протоколів, що ґрунтуються на симетричних криптосистемах. Протоколи, що ґрунтуються на асиметричних криптосистемах.

Типи та класи порушників безпеки стеганографічних систем. Типи атак на стеганографічні системи. Атака з відомим контейнером. Атака з вибором контейнера. Атака з відомим повідомленням. Атака з вибором повідомлення. Атака, що направлена на руйнування повідомлення.

## СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

### *ОСНОВНИЙ*


1. С.Е. Остапов, С.П. Євсеєв, О.Г. Король «Проектування систем захисту інформації в економіці, Підготовка до ЄДКІ, Навчальний посібник, «Новий Світ-2000» Львів 2023, 678 с.
2. В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа “Інформаційна та Кібербезпека: соціотехнічний аспект”, Підручник, Видавництво "Магнолія 2006" Львів- 2024, 320 с.
3. Гулак Г.М., Жильцов О.Б., Киричок Р.В., Коршун Н.В., Складанний П.М., “ІНФОРМАЦІЙНА та КІБЕРНЕТИЧНА БЕЗПЕКА ПІДПРИЄМСТВА" Підручник, Видавець МарченкоТ.В. Львів – 2024, 370 с.
4. В.Л. Бурячок, С.В. Толюпа, В.В. Семко, П.М. Складанний, Л.В. Бурячок, Н.В. Лукова-Чуйко, “ІНФОРМАЦІЙНИЙ ТА КІБЕРПРОСТОРИ: проблеми безпеки, методи та засоби боротьби”, НАВЧАЛЬНИЙ ПОСІБНИК (Лабораторний практикум), Видавництво ПП "Магнолія 2006" Львів 2024, 176 с.
5. В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко, “ІНФОРМАЦІЙНИЙ ТА КІБЕРПРОСТОРИ: проблеми безпеки, методи та засоби боротьби”, Підручник, Видавництво ПП "Магнолія 2006" Львів 2024, 448 с


### *ДОДАТКОВИЙ*


6. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник, Комп’ютерні мережі. Книга 2 [навчальний посібник] – Львів, «Магнолія 2006», 2024. – 328 с

7. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – Львів: «Магнолія 2006», 2024. – 432 с.
8. Богуш В.М. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / В.М. Богуш, В.В. Богуш, В.Д. Бровко, В.П. Настрадін; під. ред. В. М. Богуша. — К.: Видавництво Ліра-К, 2020. — 554 с.
9. Основи кібербезпеки : навчально-практичний посібник / уклад. С. П. Євсеєв, О. В. Шматко, О. Б. Ахієзер, Т. В. Горбач ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий світ-2000», 2025. – 95 с
10. Гапак О. М., Балога С.І., «ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ», Підручник для студентів спеціальності 123 «комп'ютерна інженерія», Ужгород - 2021

### *ІНТЕРНЕТ-РЕСУРСИ*

11. Cisco-Україна. – URL: *https://www.cisco.com*
12. Networking Academy CISCO. – URL: *https://www.netacad.com/*
13. Державна служба спеціального зв'язку та захисту інформації України. – URL: *http://www.dsszzi.gov.ua/dsszzi/control/uk/index*
14. Захист інформації. – URL: *http://jrnl.nau.edu.ua/index.php/ZI*
15. Бізнес і безпека. – URL: *www.bsm.com.ua*

## КРИТЕРІЇ
## оцінювання фахового іспиту замість ЄФВВ для здобуття освітнього ступеня магістра на основі НРК6 та НРК7

### 1. Загальні положення

Мета фахового іспиту – оцінити відповідність знань, умінь та навичок згідно з вимогами програми фахового іспиту.

### 2. Структура екзаменаційного білета

Екзаменаційний білет фахового іспиту складається з 50-ти закритих тестових завдань.

### 3. Критерії оцінювання

- Рівень знань оцінюється за 200-баловою шкалою.
- Серед відповідей на тестове завдання слід обрати одну правильну.
- Правильна відповідь на тестове завдання оцінюється у 4 бали, а неправильна – у 0 балів.
- Особи, які отримали менше ніж 100 балів, до наступних випробувань не допускаються та участі у конкурсі не беруть.