МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

магістр

Факультет:
автоматизації і інформаційних технологій

«Затверджую»
Голова приймальної комісії
Ректор
Олексій ДНІПРОВ

П Р О Г Р А М А
вступних фахових випробувань
до вступу на навчання для здобуття
ступеня магістра зі спеціальності
F5. « КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ»
за освітньо-професійною програмою
«БЕЗПЕКА ІНФОРМАЦІЙНИХ І КОМУНІКАЦІЙНИХ СИСТЕМ»
галузі знань «Інформаційні технології»

Затверджено на засіданні
приймальної комісії, протокол
№ 2 від « 24 » березня 2025 р.

КИЇВ – 2025

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Вступні випробування проводяться фаховою атестаційною комісією для осіб, які закінчили ЗВО та отримали диплом за освітнім ступенем «бакалавр» (освітньо-кваліфікаційним ступенем «спеціаліст», «магістр») і вступають на спеціальність F5. «Кібербезпека» відповідно правилам прийому до КНУБА на 2025 р. Бажаючі навчатися для отримання рівня ступеня магістра складають контрольні заходи у формі тестування з фахових дисциплін «Захист даних в інформаційних системах» і «Організація баз даних та знань».

Складати фаховий іспит замість єдиного фахового вступного випробування (ЄФВВ) можуть тільки вступники, які користуються спеціальними умовами вступу на навчання та мають на це право відповідно до розділу 8 Правил прийому до КНУБА у 2025 році.

Другий (магістерський) освітній рівень є освітньо-професійним і обов'язковим для продовження навчання за однією зі спеціальностей в аспірантурі.

Студенти спеціальності F5. «Кібербезпека» одержують теоретичні знання що необхідні для забезпечення профілю фахівця: технологічне і організаційне забезпечення захисту інформації в комп'ютеризованих технічних системах та охоронна діяльність, що здійснюється за допомогою комп'ютеризованих захисних пристроїв.

Об'єктами професійної діяльності випускників спеціальності є технології та інструментальні засоби забезпечення безпеки ресурсів інформаційних і комунікаційних систем.

Магістр зі спеціальності F5. «Кібербезпека» можуть обіймати посади в службах інформаційної та кібернетичної безпеки державних та недержавних установ та підприємств; обслуговування систем інформаційної безпеки та кіберзахисту; інформаційних технологій та інформаційних послуг; науково-дослідних та освітніх закладах.

Після закінчення навчання випускники отримують диплом та освітню кваліфікацію – магістр із організації інформаційної безпеки.

2. ЗМІСТ ПРОГРАМИ ВСТУПНОГО ВИПРОБУВАННЯ

2.1. Дисципліна «Захист даних в інформаційних системах».

2.1.1 Комп'ютерні мережі

2.1.1.1 Налаштування мережевої операційної системи.

2.1.1.2 Поняття мережевих протоколів та комунікацій.

2.1.1.3 Еталонна модель OSI.

2.1.1.4 Мережевий доступ.

2.1.1.5 Ethernet.

2.1.1.6 Сеансовий доступ.

2.1.1.7 IP-адресація.

2.1.1.8 Розділення IP-мережі на під мережі.

2.1.1.9 Транспортний рівень.

2.1.1.10 Рівень застосунків.

2.1.2 Технологія захисту даних

2.1.2.1 Основні види і джерела атак на інформацію.

2.1.2.2 Сучасна ситуація в області інформаційної безпеки.

2.1.2.3 Категорії інформаційної безпеки.

2.1.2.4 Абстрактні моделі захисту інформації.

2.1.2.5 Найбільш поширені методи «злому».

2.1.2.6 Симетричні криптоалгоритми та криптосистеми.

2.1.2.7 Потокові шифри, скремблери.

2.1.2.8 Блокові шифри.

2.1.2.9 Мережа Фейштеля.

2.1.2.10 Алгоритми створення ланцюжків.

2.1.2.11 Загальні принципи архівації. Класифікація методів.

2.1.2.12 Хешування паролів.

2.1.2.13 Транспортне кодування.

2.1.2.14 Асиметричні криптоалгоритми та криптосистеми.

2.1.2.15 Алгоритм RSA.

2.1.2.16 Технології цифрових підписів.

2.1.3 Захист даних в інформаційних системах.

2.1.3.1 Метод цифрових підписів.

2.1.3.2 DLP системи.

2.1.3.3 Класифікація зловмисних кодів.

2.1.3.4 Комп’ютерні віруси та антивіруси.

2.1.3.5 Причини створення зловмисного коду та узагальнений портрет його автора.

2.1.3.6 Засоби розповсюдження зловмисного коду та методи протидії.

2.1.3.7 Соціальна інженерія та методи протидії.

2.1.3.8 Конфіденційні та відкриті данні.

2.1.3.9 Основні принципи керування доступом.

2.1.3.10 Властивості інформації та захищених АС.

2.1.3.11 Об`єкт інформаційної діяльності

2.1.4 Проектування захищених інформаційних систем.

2.1.4.1 Поняття, мета, особливі властивості та задачі системного аналізу при розробці інформаційних систем.

2.1.4.2 Задачі системного аналізу при забезпеченні захисту інформації в інформаційних системах і технологіях.

2.1.4.3 Комплексна система захисту даних як складна система.

2.1.4.4 Склад та структура системи. Статичні та динамічні моделі структури систем.

2.1.4.5 Інформаційна система. Класифікація інформаційних систем.

2.1.4.6 Оцінка рівня захищеності інформації з застосуванням методів експертного оцінювання.

2.1.4.7 Особливості колективного експертного оцінювання

2.1.4.8 Метод морфологічного аналізу при формуванні проектних рішень комплексних систем захисту даних.

2.1.4.9 Порівняльна оцінка рівня захищеності інформацій в інформаційних системах на основі МАІ.

2.1.4.10 Оцінка та вибір альтернативних варіантів побудови системи захисту даних та окремих її складових на основі метода МАІ.

2.1.4.11 Стадії та етапи життєвого циклу (ЖЦ) Інформаційних систем.

2.1.4.12 Стадії та етапи ЖЦ систем захисту інформації.

2.1.4.13 Аналіз та формування вимог до системи. Концепція та технічне завдання на розробку системи.

2.1.4.14 Етапи логічного та технічного проектування ІС. Технічний проект системи.

2.1.4.15 Задачі прийняття рішень в інформаційних системах проектування, управління та захисту даних.

2.1.4.16 Прийняття рішень в умовах невизначеності. Критерії прийняття рішень.

2.1.4.17 Розв'язання конфліктних ситуацій прийняття рішень на основі теорії ігор.

ЛІТЕРАТУРА ДЛЯ ПІДГОТОВКИ

1. Тарнавський Ю. А. Технології захисту інформації: підручник / Ю.А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.

2. Інформаційна безпека: навч. посіб. / С. В. Кавун, В. В. Носов, О. В. Манжай. Харків: Вид. ХНЕУ, 2008. – 352 с.

3. Остапов С.Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х.: ХНЕУ, 2013. – 476 с.

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

5. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 510 с.

6. Полторак В.П. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах. – Київ: КПІ ім. Ігоря Сікорського, 2020. – 78 с.

7. Інформаційна безпека держави: підручник / [О.О.Бакалинський, В.М.Петрик, М.М.Присяжнюк, Д.С.Мельник, О.О.Климчук, В.В.Остроухов, Я.М.Жарков, О.А.Штоквиш, Л.Ф.Компанцева, В.І.Полевий, О.Д.Бойко] ; в 2 т. – Т. 1. / за заг. ред. В.М. Петрика. – К. : Вид-во ІСЗЗІ НТУУ «КПІ», 2016. – 264 с.

2.2. Дисципліна «Організація баз даних і знань».

2.2.1 Основні визначення та поняття бази даних і знань.

2.2.2 Поняття системи управління базою даних.

2.2.3 Основні поняття та визначення реляційної бази даних.

2.2.4 Поняття об'єктно-орієнтованої бази даних.

2.2.5 Представлення концептуальної моделі бази даних.

2.2.6 Функції виконання фактографічної інформаційної системи.

2.2.7 Моделі даних, що реалізує сучасні СУБД.

2.2.8 Поняття та визначення незалежність даних.

2.2.9 Вигляд представлення запиту в реляційному обчисленні зі змінними кортежами.

2.2.10 Проблеми, для вирішення яких необхідно виконувати нормалізацію бази даних.

2.2.11 Визначення і поняття першої нормальної форми.

2.2.12 Визначення і поняття другої нормальної форми.

2.2.13 Визначення і поняття третьої нормальної форми.

2.2.14 Визначення поняття “цілісність бази даних”.

2.2.15 Визначення поняття «відношення».

2.2.16 Визначення поняття «кортеж».

2.2.17 Визначення поняття “домен”.

2.2.18 Поняття «ключ» в реляційній базі даних.

2.2.19 Визначення поняття «зовнішній ключ».

2.2.20 Визначення поняття «реплікація».

2.2.21 Визначення поняття «тригер».

2.2.22 Визначення поняття “транзакція”.

2.2.23 Використання метадані в базах даних.

2.2.24 Особливості архітектури файл-сервер.

2.2.25 Реалізація, що дозволяє зробити індекси.

2.2.26 Дії, що передбаченні для забезпечення безпеки даних в базі даних.

2.2.27 Функції виконання представлення (view).

2.2.28 Архітектура програмно-технічних засобів розподілених СУБД.

2.2.29 Функції виконання сервер застосувань.

2.2.30 Використання технології, що передбачає реплікацію.

2.2.31 Використання технології, що передбачає фрагментацію.

2.2.32 Рівні ієрархії пристроїв пам’яті бази даних.

2.2.33 Використання кеш-пам’ять для потреб.

2.2.34 Визначення та поняття дамп бази даних.

2.2.35 Застосування memo-поле в базах даних.

2.2.36 Застосування B-дерева в базах даних.

2.2.37 Визначення “ADO”.

2.2.38 Визначення “OLE DB”.

2.2.39 Представлення інтерфейсу ISAPI/NSAPI.

2.2.40 Визначення “QBE”.

2.2.41 Визначення типу мов програмування, що відносяться до мови SQL.

2.2.42 Вигляд, що має правильний синтаксис для виключення пустих значень з таблиці.

2.2.43 Команди, які включають мову запитів до бази даних.

2.2.44 Команди, які включають мову маніпулювання з даними DML.

2.2.45 Команди, які на мові SQL застосовуються для визначення обмежень полів в базі даних.

2.2.46 Визначення “ACID”.

2.2.47 Визначення і поняття інкрементного поля.

2.2.48 Представлення програми – клієнт.

2.2.49 Правила перетворення ER-діаграм, які перетворюються в логічні моделі реляційної бази даних.

2.2.50 Правильність складання SQL-запитів до бази даних.

2.2.51 Правильність застосування команд SQL по створенню бази даних.

2.2.52 Правильність приведення логічної схеми бази даних до третьої нормальної форми.

2.2.53 Представлення “CORBA”.

2.2.54 Класична архітектура бази даних, яка включає запропоновану ANSI.

2.2.55 Основні поняття та визначення сховище даних.

2.2.56 Рівні ізоляції транзакцій і в чому їх особливості.

2.2.57 Головні властивості розподіленої бази даних.

2.2.58 Моделі або модель, яка підтримує об’єктно-реляційну базу даних.

2.2.59 Поняття хешування і для чого воно використовується.

2.2.60 Визначення репозиторій.

2.2.61 Функції, що виконують серіалізацію транзакцій.

2.2.62 Функції, що виконують файловий сервер.

2.2.63 Поняття, визначення “BLOB”.

2.2.64 Журнал реєстрації транзакцій, принцип використання.

ЛІТЕРАТУРА ДЛЯ ПІДГОТОВКИ

1. Тарасов О. В. Використання мови SQL для роботи з сучасними системами керування базами даних / О. В. Тарасов, В. В. Федько, М. Ю. Лосєв. – Х. : Вид. ХНЕУ, 2013. – 348 с.

2. Тарасов О. В. Проектування баз даних : навч. посіб. / О. В. Тарасов, В. В. Федько, М. Ю. Лосєв. – Х. : Вид. ХНЕУ, 2011. – 200 с.

3. Анісімов А.В., Кулябко П.П. Інформаційні системи та бази даних: Навчальний посібник для студентів факультету комп’ютерних наук та кібернетики. – Київ. – 2017. – 110 с.

4. Гайна Г.А. Основи проектування баз даних: Навчальний посібник / Г.А. Гайна. − К. : КНУБА, 2005. – 204 с.

5. Мулеса О.Ю. Інформаційні системи та реляційні бази даних. Навч.посібник. – Ужгород: ДВНЗ УжНУ, Електронне видання, 2018. – 118 с.

6. Ковальчук А.М. Принципи проектування баз даних: Навчальний посібник. / Ковальчук А.М., Левицький В.Г. та ін. – Ж.: ЖДТУ, 2009. – 123с.

7. Atkinson P., Vieira R. Beginning Microsoft SQL Server 2012 Programming. - Wiley, 2016, – 864с.

3. СТРУКТУРА ЕКЗАМЕНАЦІЙНОГО БІЛЕТА. КРИТЕРІЇ ОЦІНЮВАННЯ

Оцінювання знань вступників на вступному випробуванні здійснюється за шкалою від 60 до 100 балів по кожній із зазначених дисциплін. Вступне випробування включає тестові завдання з дисциплін, кожне з яких налічує 20 питань. Кожне питання має чотири відповіді позначені літерами (цифрами), одна з яких вірна. Вступник обирає правильну відповідь до тестового питання та позначає її відповідною літерою (цифрою) напроти номера питання у стовпчику «відповідь» бланка-відповіді. Якщо вступник вирішив виправити відповідь на питання, то має внести зміну літерою (цифрою) у стовпчик «виправлена відповідь». Прийнятим до оцінювання буде запис внесений у стовпчик «виправлена відповідь». Викреслювати відповіді (літери, цифри) не дозволяється. Кожна правильна відповідь на питання оцінюється в 1 (один) бал, неправильна відповідь – 0 (нуль) балів і за таблицею переведення визначається конкурсна оцінка з фахового випробування.

Якщо вступник не склав контрольний захід хоча б по одній з дисциплін, вважається що він не пройшов фахове випробування та втрачає право брати участь в конкурсі на навчання для отримання ступеня магістра.

Таблиця переведення результатів випробування (тестування) з фахової дисципліни із 20-ти бальної у 100-бальну шкалу оцінювання знань

Кількість вірних відповідей на запитання тестового завдання	Кількість балів за шкалою ECTS
0…5	**0 (незадовільно – контрольний захід нескладений)**
6	**60**
7	**61**
8	**63**
9	**65**

10	**68**
11	**71**
12	**74**
13	**77**
14	**80**
15	**83**
16	**86**
17	**89**
18	**92**
19	**96**
20	**100**

За результатами вступного випробовування визначається сумарна кількість балів з зазначених дисциплін, на підставі якої фахова атестаційна комісія вносить на розгляд приймальної комісії університету затвердження результатів фахового випробування.

Голова фахової атестаційної комісії  Олександр ТЕРЕНТЬЄВ