**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАНИ**

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ**
**«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

**Навчально-науковий інститут комп'ютерних наук та інформаційних технологій**

**ЗАТВЕРДЖУЮ**
**Проректор**
**_____Руслан МИГУЩЕНКО**
**«__25__» ____05_____2025 р.**

**ПРОГРАМА**

для проведення вступних випробувань за фахом
при зарахуванні на навчання за освітньо-кваліфікаційним рівнем «магістр»
за конкурсною пропозицією:

**Кібербезпека**

Директор інституту
_____ Михайло ГОДЛЕВСЬКИЙ

Харків 2025

**ЗМІСТ**

**Кібербезпека**

## АНОТАЦІЯ

Програма фахового випробування розроблена для абітурієнтів, які вступають на навчання за освітньо-кваліфікаційним рівнем магістр за спеціальністю F5 “Кібербезпека та захист інформації”.

Завдання фахового випробування складено з метою виявлення знань, вмінь, компетентностей, якими володіє бакалавр за галуззю знань F “Інформаційні технології”, спеціальність F5 “Кібербезпека та захист інформації” (табл. 1).

Таблиця 1

Основні компетентності, якими повинен володіти бакалавр за галуззю знань F “Інформаційні технології”, спеціальність F5 “Кібербезпека та захист інформації”

| | |
|---|---|
| **Інтегральна компетентність** | |
| **ІК** | Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов. |
| **Загальні компетентності** | |
| **КЗ** | Здатність застосовувати знання у практичних ситуаціях |
| | Знання та розуміння предметної області та розуміння професії. |
| | Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. |
| | Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. |
| | Вміння виявляти, ставити та вирішувати проблеми. |
| | Здатність до пошуку, оброблення та аналізу інформації. |
| | Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. |
| | Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. |
| **Фахові компетентності** | |
| **КФ** | Здатність застосовувати законодавчу та нормативно- правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. |
| | Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. |
| | Здатність до використання програмних та програмно- апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. |
| | Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. |
| | Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. |
| | Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження. |
| | Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) |
| | Здатність здійснювати процедури управління інцидентами, проводити розслідування, |

| | |
|---|---|
| | надавати їм оцінку. |
| | Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. |
| | Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. |
| | Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. |
| | Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки. |

## ЗМІСТ ПРОГРАМИ

## ПЕРЕЛІК ПИТАНЬ ВСТУПНОГО ВИПРОБУВАННЯ

Тема 1. **Базові поняття криптології**.

Основні поняття криптографії.

Задачі криптографічного захисту інформації в інформаційних та телекомунікаційних системах.

Визначення та загальна математична модель симетричної криптосистеми.

Основні класи симетричних криптосистем (транзитивні, регулярні та мінімальні криптосистеми).

Визначення та математичні моделі шифрів простої заміни та перестановки.

Методика дешифрування простої заміни та перестановки.

Визначення та математичні модель табличного шифру гамування.

Шифри Цезаря, Віжінера, Вернама.

Розв'язання задач зашифрування та розшифрування повідомлень з використанням табличних шифрів гамування.

Тема 2. **Теоретичні основи побудови та аналізу симетричних криптосистем.**

Ймовірнісна модель шифру. Теоретична стійкість криптографічних систем, критерії теоретичної стійкості симетричних криптосистем. Обчислювальна стійкість криптосистем. Показники та критерії обчислювальної стійкості.

Основні класи симетричних криптосистем. Математична модель та принципи побудови потокових шифрів. Принципи побудови та критерії стійкості шифрів гамування.

Основні типи сучасних генераторів псевдовипадкових послідовностей (ПВП). Алгебраїчні та структурні властивості псевдовипадкових послідовностей (поняття періоду та еквівалентної лінійної складності ПВП). Статистичні властивості ПВП.

Основні властивості лінійних регістрів зсуву. Розв'язання задач визначення функції зворотного зв'язку та початкового заповнення лінійного регістру зсуву. Моделювання лінійних регістрів зсуву з використанням ПЕОМ. Моделювання нелінійних вузлів ускладнення з використанням ПЕОМ.

Принципи побудови та класифікація сучасних блокових шифрів. Огляд методів криптографічного аналізу та обґрунтування стійкості блокових шифрів. Схема алгоритму шифрування та математична модель блокового шифру ДСТУ ГОСТ-28147:2009. Режими використання алгоритму шифрування даних ДСТУ ГОСТ-28147:2009.

Rijndael: принципи побудови, математична модель та схема алгоритму шифрування. Криптографічні властивості блокового шифру Rijndael.

Принципи побудови, функціонування та криптоаналізу блокових шифрів DES, IDEA. Основні режими роботи сучасних блокових шифрів.

Тема 3. **Теоретичні основи побудови та аналізу асиметричних криптосистем.**

Загальні принципи побудови та використання асиметричних криптографічних систем. Основні класи задач, що вирішуються з використанням асиметричних криптографічних систем.

Задачі факторизації цілих чисел та дискретного логарифмування. Поняття про складність сучасних алгоритмів факторизації та дискретного логарифмування. Огляд сучасних методів обгрунтування обчислюваної стійкості асиметричних криптосистем.

Система відкритого шифрування RSA. Схема цифрового підпису RSA. Розв'язання задач зашифрування, розшифрування та цифрового підпису повідомлень з використанням криптосистеми RSA.

Алгоритми відкритого шифрування та розшифрування інформації в криптосистемі Ель-Гамаля. Розв'язання задач зашифрування та розшифрування повідомлень з використанням криптосистеми Ель-Гамаля. Алгоритми формування та перевірки підпису в схемі цифрового підпису Ель-Гамаля. Розв'язання задач формування та перевірки підпису з використанням схеми Ель-Гамаля.

Протокол Діффі – Геллмана. Розв'язання задачі узгодження ключу за протоколом Діффі – Геллмана.

Криптографічні протоколи STS та MTI. Розв'язання задач узгодження ключів за протоколами STS та MTI.

Тема 4. **Протоколи автентифікації. Цифрові підписи. Комплексні системи захисту даних.**

Принципи захисту інформації на мережевому рівні. Протоколи захисту та цілісності *IPSec*, *SSL*, *TLS*, їх сутність.

Класифікація механізмів автентифікації. *MDC*-коди, основні алгоритми. *MAC*-коди, основні способи формування. Класифікація стандартів електронних цифрових підписів. Основні стандарти цифрового підпису.

Основні функції систем захисту *PGP* і *CS MIME*. Принципи сумісності на рівні електронної пошти. Принципи побудови захищеної електронної пошті.

Тема 5. **Основи криптоаналізу**

Формальне математичне визначення криптосистеми.

Критерії та показники ефективності.

Класифікація криптоаналітичних атак.

Принципи лінійного та диференціального криптоаналізу.

Тема 6. **Основи цифрової стеганографії**

Основні принципи приховування повідомлення на основі методів стеганографії.

Класифікація и принципи приховування алгоритмів цифровій стеганографії.

Тема 7. **Основи технології відкритих ключів (PKI).**

Основні компоненти та сервіси інфраструктури відкритих ключів.

Архітектура та топологія PKI.

Сертифікати відкритих ключів X.509.

Тема 8. **Захист програмного забезпеченні в Інтернет-технологіях**

Основні принципи захисту інформації під час підключення до мережі Інтернет.

Використання паролів і механізмів контролю.

Тема 9. **Захист персональних даних**

Основні принципи захисту персональних даних на основі програмного коду.

Моделі захисту персональних даних.

## РЕКОМЕНДОВАНА ЛІТЕРАТУРА


1. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”
2. Закон України “Про захист персональних даних”
3. СТРАТЕГІЯ національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015)
4. Закон України “Про національну безпеку
5. Стратегія кібербезпеки України” (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016)
6. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229;
7. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення;
8. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;
9. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.
10. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп’ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації у комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ, К: 1999. – 34с.
11. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
12. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу.
13. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
14. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
15. НД ТЗІ 1.6-005-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці
16. Р.В. Грищук, та Ю. Г. Даник. Основи кібернетичної безпеки: Монографія /; за заг. ред. Ю. Г. Данника. Житомир: ЖНАЕУ, 2016.
17. О. Г. Корченко, О. Є. Архипов, та Ю. О. Дрейс, “Оцінювання шкоди національній безпеці України у разі витоку державної таємниці”, монографія, К: наук.-вид.центр НА СБУ України, 2014.
18. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. [Електронний ресурс] / [КорченкоО.Г., Гнатюк С.О., КазмірчукС.В. та ін.]. –К.: Центр навч.-наук. та наук.-пр. видань НАСБ України, 2014. – 190 с
19. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук’яненко В.В. ТПК «Орхідея», 2019. – 408 с. : іл.
20. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
21. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Os- tapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
22. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.

23. Євсеєв С.П., Остапов С.Е., Король О.Г. Кібербезпека: сучасні технології захисту: навч. посіб. для студ. вищ. навч. закл. Львів : “Новий Світ- 2000”, 2019. – 678 с.

24. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. — Львів : Видавництво Львівської політехніки, 2019. — 580 с. — ISBN 978-966-941-339-0.

25. Євсеєв С.П., Ткачов А.М., Алексієв В.О., Рябуха Ю.М. КІБЕРБЕЗПЕКА: WEB-технології . Навчально-довідковий посібник / С.П. Євсеєв, А.М. Ткачов, В.О. Алексієв, Ю.М. Рябуха – Харків : ХНЕУ ім. С. Кузнеця, – Львів: Видавництво «Новий Світ –2000», 2021. – 390 с.

26. Євсєев С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. “Новий Світ-2000”, 2023. – 657 с.

27. Kali Linux Web Penetration Testing Cookbook, Second Edition (Packt Publishing) URL: https://www.packtpub.com/product/kali-linux-web-penetration-testing-cookbook-second-edition/9781788991513.

28. Зразок звіту з тестування на проникнення URL: https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf.

29. Зразок технічного звіту з проникнення URL: https://tbgsecurity.

30. OWASP Top 10: issues in the 10 most critical security risk categories in your web applications URL: https://www.sonarqube.org/features/security/owasp/?gads_campaign=Europe-1-Generic&gads_ad_group=OWASP&
gads_keyword=owasp%20top%2010&gclid=CjwKCAiAsNKQBhAPEiwAB-I5zQywzTKai6fcrilMphlAn21CRehrI0q9DEjUZNpHUoDt5V_bVpLm4RoClIkQAvD_BwE

31. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування: Монографія. Харків. Видавництво “Форт”. 2012. 870 с.

## КРИТЕРІЇ ОЦІНЮВАННЯ ВСТУПНОГО ВИПРОБУВАННЯ, СТРУКТУРА ОЦІНКИ, І ПОРЯДОК ОЦІНЮВАННЯ ПІДГОТОВЛЕННОСТІ ВСТУПНИКІВ

Кожен білет складається з двох завдань, їх бездоганне виконання оцінюється 100 балами (максимальна оцінка) за шкалою НТУ «ХПІ».

Перше завдання є діагностичним і являє собою тест, що містить 5 питань. Тестові питання вимагають від абітурієнта знання основ з безпеки інформації в межах тем Програми. Перше завдання оцінюється від 0 до 40 балів. За кожну правильну відповідь питання абітурієнт отримує 2 бали.

Друге завдання – задача на формування відповідного механізму безпеки (конфіденційність, цифровий підпис, автентифікація) за допомогою несиметричної криптосистеми RSA. Передбачається використовувати наступні критерії для виставлення оцінок:

**Завдання 1.**

**Теоретичні питання** у кількості 5 питань з основних положень дисципліни. Перше питання оцінюється в 2 бали. Питання з 2-4 оцінюються по 2 бали за кожну правильну відповідь (сумарно 17 відповідей), яка необхідна для відповіді на питання, питання 5 оцінюється у 4 балів.

**Завдання 2.**

**Оцінка 60 балів.** Практичне завдання виконано бездоганно з повним обґрунтуванням кожного етапу виконання завдання, зроблені повні висновки та узагальнення. Приведений протокол обміну відповідає вимогам відповідного стандарту, приведені алгоритми шифрування/розшифрування з повними поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), визначені достоїнства і недоліки обґрунтовані, проведений порівняльний аналіз обґрунтований. Наведені механізми та послуги в яких використовуються відповідні протоколи (схеми шифрування).

**Оцінка 50 балів.** Практичне завдання виконано повністю з обґрунтуванням кожного етапу виконання завдання. Приведений протокол обміну відповідає вимогам відповідного стандарту, приведена структурна схема протоколу з повними поясненнями процедур шифрування/розшифрування, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), визначені основні достоїнства і недоліки обґрунтовані, в цілому проведений порівняльний аналіз обґрунтований.

**Оцінка 40 балів.** Практичне завдання виконано повністю. Приведений протокол обміну відповідає вимогам відповідного стандарту, приведені основні процедури шифрування/розшифрування з поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), але не в повному обсязі визначені основні достоїнства і недоліки, в цілому проведений порівняльний аналіз обґрунтований.

**Оцінка 30 балів.** Практичне завдання виконано повністю. Приведений протокол обміну відповідає вимогам відповідного стандарту, приведені основні процедури шифрування/розшифрування з поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), але не в повному обсязі визначені достоїнства і недоліки, проведений порівняльний аналіз не обґрунтований.

**Оцінка 20 балів.** Практичне завдання виконано повністю. Приведений протокол обміну відповідає вимогам відповідного стандарту, приведені основні процедури шифрування/розшифрування з поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), але не в повному обсязі визначені достоїнства і недоліки, не проведений порівняльний аналіз.

**Оцінка 15 балів.** Практичне завдання виконано неповністю. Приведений протокол обміну відповідає вимогам відповідного стандарту, приведені алгоритми шифрування/розшифрування, але сформована криптограма або повідомлення не відповідають алгоритму шифрування або розшифрування, не визначені основні достоїнства і недоліки, не проведений порівняльний аналіз.

**Оцінка 10 балів.** Практичне завдання виконано неповністю. Приведений протокол обміну в цілому відповідає вимогам відповідного стандарту, приведені алгоритми шифрування/розшифрування, але сформована криптограма і повідомлення не відповідають

алгоритму шифрування/розшифрування, не визначені основні достоїнства і недоліки, не проведений порівняльний аналіз.

**Оцінка 5 балів.** Практичне завдання не виконано. Приведений протокол обміну не відповідає вимогам відповідного стандарту, не приведені алгоритми шифрування/розшифрування, сформована криптограма і повідомлення не відповідають алгоритму шифрування/розшифрування, пояснень процедур не має, не визначені достоїнства і недоліки, не проведений порівняльний аналіз.

**Оцінка 0 балів.** Практичне завдання не виконано. Протокол обміну не приведений, не приведені алгоритми шифрування/розшифрування, сформована криптограма і повідомлення не відповідають алгоритму шифрування/розшифрування, не визначені достоїнства і недоліки, не проведений порівняльний аналіз.

Підсумкова оцінка за екзамен з кібербезпеки є сумою оцінок (балів), отриманих за кожне завдання.

Обмеження в часі на реалізацію завдань – 1 година 45 хвилин.

При оцінюванні знань за основу слід брати повноту і правильність виконання завдань. Загальна оцінка визначається як середня виважена з оцінок відповідей на усі запитання.

| Рейтингова оцінка, бали | Оцінка ECTS та її визначення | Національна оцінка | Критерії оцінювання | |
|---|---|---|---|---|
| | | | позитивні | негативні |
| 90-100 | A | Відмінно | – **глибоке знання** навчального матеріалу, що міститься в **літературних джерелах;**<br>– **вміння аналізувати** явища, які вивчаються, в їхньому взаємозв'язку і розвитку;<br>– **вміння** проводити **теоретичні розрахунки**;<br>– **відповіді** на запитання **чіткі, лаконічні, логічно-послідовні;**<br>– **вміння розв'язувати складні практичні задачі** | відповіді на запитання можуть містити **незначні неточності** |
| 82-89 | B | Добре | – **глибокий рівень знань** в обсязі **обов'язкового матеріалу**;<br>– вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**;<br>– вміння розв'язувати **складні практичні задачі** | відповіді на запитання містять **певні неточності** |
| 75-81 | C | Добре | – **міцні знання** матеріалу, що вивчається, та його **практичного застосування;**<br>– вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**;<br>– вміння розв'язувати **практичні задачі** | – невміння використовувати теоретичні знання для розв'язування **складних практичних задач** |

| Рейтингова оцінка, бали | Оцінка ECTS та її визначення | Національна оцінка | Критерії оцінювання | |
|---|---|---|---|---|
| | | | позитивні | негативні |
| 64-74 | D | Задовільно | – знання **основних фундаментальних положень** матеріалу, що вивчається, та їх **практичного застосування**;<br>– вміння розв'язувати прості **практичні задачі** | – невміння давати **аргументовані відповіді** на запитання;<br>– невміння **аналізувати** викладений матеріал і **виконувати розрахунки;**<br>– невміння розв'язувати **складні практичні задачі** |
| 60-63 | E | Задовільно | – знання **основних фундаментальних положень** матеріалу,<br>– вміння розв'язувати найпростіші **практичні задачі** | – незнання **окремих (непринципових) питань** з матеріалу;<br>– невміння **послідовно і аргументовано** висловлювати думку;<br>– невміння застосовувати теоретичні положення при розв'язанні **практичних задач** |
| 35-59 | FX | Незадовільно | – | – незнання **основних фундаментальних положень** навчального матеріалу;<br>– **істотні помилки** у відповідях на запитання;<br>– невміння розв'язувати **прості практичні задачі** |
| 1-34 (на комісії) | F | Незадовільно | – | – повна **відсутність знань** значної частини навчального матеріалу;<br>– **істотні помилки** у відповідях на запитання;<br>– незнання основних фундаментальних положень;<br>– невміння орієнтуватися під час розв'язання **простих практичних задач** |

*Переведення позитивної оцінки фахового вступного випробування для вступу на навчання для здобуття ступеня бакалавра на основі молодшого спеціаліста та магістра в шкалу 100-200, згідно Додатку 3 Правил прийому до НТУ «ХПІ» в 2025 році.*

**ТАБЛИЦЯ**
**ПЕРЕВЕДЕННЯ ПОЗИТИВНОЇ ОЦІНКИ ВИПРОБУВАННЯ ЗАМІСТЬ ЄВІ, ЄФВВ ТА ФАХОВОГО ІСПИТУ ДЛЯ ВСТУПУ НА НАВЧАННЯ ДЛЯ ЗДОБУТТЯ СТУПЕНЯ МАГІСТРА В ШКАЛУ 100–200**

| **Шкала оцінювання 60-100 (фахового вступного випробування)** | **Переведення в шкалу 100–200** |
|---|---|
| 60 | 100 |
| 61 | 103 |
| 62 | 105 |
| 63 | 108 |
| 64 | 110 |
| 65 | 113 |
| 66 | 115 |
| 67 | 118 |
| 68 | 120 |
| 69 | 123 |
| 70 | 125 |
| 71 | 128 |
| 72 | 130 |
| 73 | 133 |
| 74 | 135 |
| 75 | 138 |
| 76 | 140 |
| 77 | 143 |
| 78 | 145 |
| 79 | 148 |
| 80 | 150 |
| 81 | 153 |
| 82 | 155 |
| 83 | 158 |
| 84 | 160 |
| 85 | 163 |
| 86 | 165 |
| 87 | 168 |
| 88 | 170 |
| 89 | 173 |
| 90 | 175 |
| 91 | 178 |

| **Шкала оцінювання 60-100 (фахового вступного випробування)** | **Переведения в шкалу 100-200** |
|---|---|
| 92 | 180 |
| 93 | 183 |
| 94 | 185 |
| 95 | 188 |
| 96 | 190 |
| 97 | 193 |
| 98 | 195 |
| 99 | 198 |
| 100 | 200 |

Схвалено на засіданні вченої ради інституту ННІ комп'ютерних наук та інформаційних технологій.

Протокол № 4 від « 25 » травня 2025 р.

Голова вченої ради інституту _____ Михайло ГОДЛЕВСЬКИЙ

Голова фахової атестаційної комісії _____ Станіслав МІЛЕВСЬКИЙ