Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут комп'ютерних наук та штучного інтелекту

«ЗАТВЕРДЖУЮ»
Заступник голови Приймальної комісії, проректор з науково-педагогічної роботи Харківського національного університету імені В.Н. Каразіна
Олександр ГОЛОВКО
березня 2025 р.

**ПРОГРАМА ФАХОВОГО ІСПТУ**
**(письмово) зі спеціальності F5 «Кібербезпека та захист інформації»**
**освітня програма «Кібербезпека та захист інформації» для здобуття ступеня магістра на основі НРК6 та НРК7.**

Харків 2025

## І. Перелік питань за темами

### *Тема №1. Теорія чисел*

1. Прості числа і "основна" теорема арифметики. Канонічне подання раціональних чисел. Решето Ератосфена для пошуку простих чисел. Взаємно прості числа. Теорема Чезаро.
2. Ланцюгові дроби. Розкладання чисел в ланцюгові дроби. Скінченні та нескінченні ланцюгові дроби та їх зв'язок із раціональними та ірраціональними числами.
3. Обчислення придатних дробів. Застосування алгоритму Евкліда для обчислення придатних дробів. Властивості придатних дробів. Основні рекурентні співвідношення.
4. Формули Біне. Послідовності чисел Фібоначчі та чисел Люка, їх властивості та зв'язок із придатними дробами. Щільність послідовностей чисел та пар чисел.
5. Визначення і прості властивості порівнянь. Кільце лишків. Повна та приведена система вирахувань. Визначення та основні властивості.
6. Теорема Ейлера і теорема Ферма. Порівняння першого ступеня, визначення та основні властивості. Вирішення порівняння із застосуванням функції Ейлера.
7. Китайська теорема про лишки. Вирішення системи порівнянь. Схема розподілу секрету із застосуванням китайської теореми про лишки.
8. Алгоритм обміну ключами Діффі-Хеллмана. Алгоритм шифрування з відкритими ключами RSA. Алгоритм електронного підпису RSA.

### *Тема №2. Теорія груп, полів, кілець*

1. Дайте визначення та наведіть основні властивості групи. Поясніть на прикладі властивість комутативності групи. Дайте визначення підгрупи, наведіть приклади.
2. Дайте визначення та наведіть основні властивості векторного простору над кінцевим полем. Що таке базис векторного простору та його розмірність?
3. Дайте визначення та наведіть основні властивості кільця. Поясніть на прикладі властивість комутативності кільця.
4. Дайте визначення та наведіть основні властивості поля. Що таке поле Галуа? Наведіть приклади. Дайте визначення таких понять як підполе та розширення поля.
5. Дайте визначення незвідного полінома. Що таке приведений поліном?
6. Дайте визначення порядку точки еліптичної кривої. За якими формулами обчислюються операції подвоєння та додавання точок еліптичної кривої у простому полі характеристики $p>3$?
7. Дайте визначення та наведіть основні властивості примітивних елементів кінцевого поля. Що таке примітивний поліном?

### *Тема №3. Прикладна криптологія*

1. У чому сутність основних положень щодо управління ключами? Стани ключа та переходи між станами. Захист ключів криптографічними, фізичними та організаційними засобами.

2. Визначення, властивості та застосування ВП та ПВП. У чому сутність методик тестування ВП та ПВП з використанням FIPS 140-1 та NIST STS?

3. Які основні задачі криптоаналізу відносно симетричних криптосистем та при яких вхідних даних вони можуть вирішуватись?

4. В чому сутність та відмінності ЕП з додатком та відновленням повідомлення? Які основні вимоги висуваються до ЕП з додатком та з відновленням повідомлення?

5. Основні підходи до побудування БСШ. У чому сутність підходу до побудування БСШ на основі SPN структур та які БСШ побудовані на основі SPN структур і їх властивості?

6. У чому сутність вимог коректності та повноти криптографічного протоколу? У чому сутність та які можливості криптографічного протоколу з нульовим розголошенням?

7. Які основні задачі криптоаналізу відносно асиметричних криптосистем та при яких вхідних даних вони можуть вирішуватись? Модель криптоаналітика та його практичні та потенційні можливості.

8. Дайте характеристику та обґрунтуйте вимоги до загальних параметрів та ключової пари для криптоперетворення в групі точок еліптичної кривої.

9. Умови та приклади реалізації криптосистем з безумовним рівнем стійкості. Особливості реалізації обчислювальної та ймовірної стійкості криптоперетворень.

10. Класифікація та сутність криптографічних перетворень і їх застосування для надання послуг безпеки інформації.

***Тема №4. Системи технічного захисту інформації***

1. Технічні канали витоку інформації.
2. Структура і класифікація радіоканалів витоку інформації.
3. Електричні і візуально-оптичні канали витоку інформації. Заходи технічного захисту.
4. Класифікація матеріально-речових каналів витоку інформації. Джерела та носії інформації.

***Тема №5. Захист інформації в інформаційних і комунікаційних системах***

1. Проаналізуйте і надайте характеристику забезпечення безпеки засобами СУБД.
2. Проаналізуйте і надайте характеристику засобам та методам захисту, які використовуються в СУБД Microsoft Access.
3. Проаналізуйте і надайте характеристику основних методів і засобів захисту від шкідливого програмного забезпечення.
4. Проаналізуйте і надайте пояснення, що таке комп'ютерне піратство? Надайте характеристику основних способів боротьби з комп'ютерним піратством.
5. Назвіть, охарактеризуйте та порівняйте основні захисні механізми універсальних і захищених операційних систем (наприклад, MS Windows і Linux).

6. Чи достатніми є три базові права доступу до файлів для реалізації в ОС Linux необхідної політики безпеки? Які права по відношенню до файлів і каталогів необхідно мати для копіювання файлу?

7. Які ви знаєте заходи по організації захищених мереж з використанням технології VPN? Охарактеризуйте можливі для використання при цьому безпечні протоколи.

8. Сутність захисту локальних мереж за допомогою міжмережевих екранів. Міжмережева політика, типова архітектура та компоненти при реалізації екранування мереж.

9. Які ви знаєте типові уразливості інформаційно-телекомунікаційних систем та методи підвищення їх захищеності? Наведіть приклади криптографічних методів і засобів їх реалізації.

***Тема №6. Комплексні системи захисту інформації***

1. Правові основи створення КСЗІ. Визначення КСЗІ. У яких випадках створюються КСЗІ? Склад КСЗІ та характеристика складових.

2. Етапи створення КСЗІ. Сутність етапів.

3. Обстеження інформаційно-телекомунікаційної системи. Середовища функціонування інформаційно-телекомунікаційної системи (складові середовища).

4. У яких випадках розроблюється технічне завдання (ТЗ) на створення КСЗІ. Що є вихідними даними для створення ТЗ на КСЗІ. Функціональний профіль захищеності (ФПЗ) інформації. Визначення ФПЗ. Семантика профілю.

5. Політика безпеки інформації (ПБІ). Чим визначається зміст ПБІ? Склад документу «Політика безпеки інформації».

6. Надати визначення наступним термінам: виток інформації, порушення цілісності інформації в системі, блокування та знищення інформації в системі, технічний захист інформації, криптографічний захист інформації, комплексна система захисту інформації.

7. Призначення та основні завдання Держспецз'вязку щодо захисту інформації.

***Тема №7. Компоненти складних комп'ютерних мереж***

1. Модель взаємодії відкритих систем.

2. Основні принципи багатоканального зв'язку. Часове, частотне і кодове розділення сигналів абонентів.

3. Системи передачі даних плезіохронної і синхронної цифрової ієрархії.

4. Системи мобільного зв'язку: стандарти AMPS, GSM, CDMA.

5. Мережі мобільного зв'язку третього покоління (3G).

6. Транкінгові системи. Протокол TETRA.

***Тема №8. Стеганографія***

1. Дайте визначення низькорівневих властивостей зорової системи людини та приклади їхнього використання в стеганографії. Які методи приховування даних у просторовій області нерухомих зображень Ви знаєте? Дайте визначення пропускної здатності каналів передачі прихованих повідомлень (стеганографічних каналів).

2. Дайте визначення складних дискретних сигналів. Наведіть правило формування складних сигналів Уолша-Адамара. Які відомі Вам методи стеганографічного приховування застосовують ці сигнали?

3. Наведіть структурну схему та математичну модель стеганографічної системи. Поясніть функціонування стеганографічної системи за її структурною схемою, дайте визначення та поясніть функціональне призначення структурних елементів стеганосистеми.

4. Поясність сутність методу фазового кодування при стеганографічному перетворенні із аудіоконтейнерами. Поясність сутність семантичних методів лінгвістичної стеганографії.

5. Які основні галузі використання стеганографічних систем Ви знаєте? Що таке «цифрові водяні знаки», де вони використовується і які головні відмінності від інших прикладів використання стегосистем?

***Тема №9. Управління інформаційною безпекою***

1. Системи управління інформаційною безпекою (СУІБ): визначення, основні підходи, нормативна база.

2. Комплексні системи захисту інформації (КСЗІ): визначення, основні підходи, нормативна база, мета та методи.

3. Етапи проведення державної експертизи КСЗІ та засобів захисту інформації. Призначення та сутність етапів. Зміст робіт, що виконуються на відповідних етапах.

4. Комплекс технічного захисту інформації (КТЗІ). Визначення, в яких випадках створюється. Етапи створення та їх характеристика.

5. Організаційно-правові заходи щодо охорони державної таємниці. Порядок надання допуску до державної таємниці. За яких умов організаціям надається дозвіл на провадження діяльності, пов'язаної з державною таємницею?

6. Класифікація інформації з обмеженим доступом. Особливості захисту інформації з обмеженим доступом.

7. Персональні дані (ПД). Що відноситься до персональних даних. Правові основи захисту ПД. Основні визначення: персональні дані; база персональних даних; обробка персональних даних; суб'єкти персональних даних.

8. Електронна ідентифікація та електронні довірчі послуги: основні визначення, поняття та призначення.

## *РЕКОМЕНДОВАНА ЛІТЕРАТУРА*

1. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Монографія. – Харків: Видавництво «Форт», 2012. – 878 с.

2. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Підручник. – Харків: ХНУРЕ, Форт, 2013. – 878 с.

3. Зеліско В. Р. Основи лінійної алгебри і аналітичної геометрії, навчальний посібник. Львів: ЛНУ імені Івана Франка, 2011.

4. Євсєєв 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.

5. Бондаренко М. Ф. Комп'ютерна дискретна математика:

підручник / М. Ф. Бондаренко, Н. В. Білоус, А. Г. Руткас. – Харків: Компанія СМІТ, 2004. – 477 с.

6. Кривий С. Л. Дискретна математика. Чернівці – Київ: Букрек, 2014.

7. М.Л. Жалдак, Н.М. Кузьміна, Г.О. Михалін. Теорія ймовірностей і математична статистика. Київ: НПУ імені М.П. Драгоманова, 2015.

8. Фельдман Л. П., Петренко А. І., Дмитрієва О. А. Чисельні методи в інформатиці. – К.: Видавнича група BHV, 2006.

9. Єсін В. І., Кузнецов О. О., Сорока Л. С. Безпека інформаційних систем і технологій. – Харків: ХНУ імені В. Н. Каразіна, 2013. – 632 с.

10. Домарєв Валерій Нормативно-правове забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури. [Електронний ресурс]. – Режим доступу: https://security.ukrnet.net/.

11. Горбенко Ю. І., Горбенко І. Д. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика. – Х.: Форт, 2010. – 593 с.

12. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Г.М. Гулак. – Київ: Видавництво НА СБ України, 2020. – 256 с.

13. Жилін А. В. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

14. Замула О. А. Нормативно-правове забезпечення інформаційної безпеки. Комплексні системи захисту інформації: навч. посібник. / О. А. Замула, Ю. І. Горбенко, О. І. Шумов. – Харків: ХНУРЕ, 2010. – 248 с.

15. Горбенко І. Д., Гріненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. Посібник. Ч. 1. Криптографічний захист інформації. – Харків: ХНУРЕ, 2004. – 368 с.

16. Закон України «Про електронну ідентифікацію та електронні довірчі послуги». [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

17. Горбенко Ю. І. Побудування та аналіз систем, протоколів та засобів криптографічного захисту інформації. Монографія. Частина 1. Методи побудування та аналізу, стандартизація та застосування криптографічних систем. Харків, 2016. – 959 с.

18. Кузнецов О. О, Потій О. В., Полуяненко М. О., Горбенко Ю. І. Потокові шифри. Монографія. – Харків: Форт, 2019. – 544 с.

19. NIST.IR 8413 Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. 2022. – 99 p. [Електронний ресурс]: https://doi.org/10.6028/NIST.IR.8413.

20. Bruce Schneier Applied Cryptography: Protocols, Algorithms and Source Code in C. – John Wiley & Sons, 2017. – 784 p.

21. William Stallings Cryptography and network security: principles and practice. 7-th edition. – Pearson, 2017. – 767 p.

22. Антіпов І. Є., Олейніков А. М., Ликов Ю. В., Кукуш В. Д., Милютченко І. О. Засоби та системи технічного захисту інформації. Навчальний посібник для студентів ЗВО // Харків: ФОП Панов А. М., 2019. – 216 с.

23. ДСТУ 3396.0-96 Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення.

24. ДСТУ 3396.1-96 Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

25. ДСТУ 3396.2-97 Державний стандарт України. Захист інформації. Технічний захист інформації. Терміни та визначення.

## ІІ. Критерії оцінювання знань

Білет складається з 4-ох питань теоретичного характеру. Максимальна кількість балів за письмову відповідь на кожне питання дорівнює 50 балів.

**Критерії підсумкової оцінки знань вступників (одне питання теоретичного характеру екзаменаційного білету)**

| Кількість балів | Критерії оцінки |
|---|---|
| 40-50 | Вступник має стійкі системні знання та продуктивно їх використовує, стійкі навички керування інформаційною системою в нестандартних ситуаціях; уміє вільно використовувати нові інформаційні технології для поповнення власних знань та розв'язування задач. |
| 30-39 | Вступник вільно володіє матеріалом, застосовує знання на практиці; вміє узагальнювати і систематизувати навчальну інформацію; самостійно виконує передбачені програмою навчальні завдання; самостійно знаходить і виправляє допущені помилки; може аргументовано обрати раціональний спосіб виконання навчального завдання. |
| 20-29 | Вступник має рівень знань вищий, ніж початковий; може з допомогою викладача відтворити значну частину навчального матеріалу з елементами логічних зв'язків; має стійкі навички виконання елементарних технологічних застосувань та їх опрацювання. |
| 10-19 | Вступник має фрагментарні знання при незначному загальному їх обсязі (менше половини навчального матеріалу) за відсутності сформованих умінь та навичок. |
| 0-9 | Робота виконана не в повному обсязі, не самостійно, допущені грубі помилки. |

**Загальні критерії оцінювання знань**

| Оцінка ECTS | Вимоги |
|---|---|
| 170–200 | Тверде засвоєння теоретичного матеріалу, глибокі та вичерпні знання змісту програмного матеріалу по суті питання, розуміння сутності та взаємозв'язку розглянутих процесів і явищ, тверде знання основних положень суміжних питань. Уміння самостійно використовувати математичний апарат для аналізу та вирішення практичних завдань, робити правильні висновки з отриманих результатів. |
| 140–169 | Тверді і досить повні знання теоретичного матеріалу по суті питання, правильне розуміння сутності та взаємозв'язку розглянутих процесів і явищ, розуміння основних положень суміжних питань. Уміння самостійно застосовувати математичний апарат для вирішення практичних завдань. |
| 100–139 | Тверде знання і розуміння теоретичного матеріалу по суті питання. Правильні і конкретні відповіді на поставлені питання за наявності окремих неточностей і несуттєвих помилок при висвітленні окремих положень. Уміння застосовувати теоретичні знання до вирішення основних практичних завдань при обмеженні математичного апарату. |
| 0–99 | Недостатнє розуміння суті розглянутих процесів і явищ, наявність грубих помилок у відповіді. Невміння застосовувати знання при вирішенні практичних завдань. |

Вступники, які набрали за шкалою 100-200 менше ніж 100 балів, отримують незадовільну оцінку та не допускаються до участі у конкурсному відборі

РОЗРОБНИКИ ПРОГРАМИ:
д.т.н., професор Горбенко Іван Дмитрович
д.т.н., професор Лисицька Ірина Вікторівна
д.т.н., професор Єсін Віталій Іванович
д.т.н., професор Олійников Роман Васильович
к.т.н., доцент Єсіна Марина Віталіївна

Голова фахової атестаційної комісії,

професор кафедри кібербезпеки інформаційних систем, мереж і технологій
д.т.н., професор — Ірина ЛИСИЦЬКА

Затверджено на засіданні Приймальної комісії Харківського національного університету імені В. Н. Каразіна, протокол №_2_від « 20 » березня 2025р.

Відповідальний секретар
Приймальної комісії — Ганна ЗУБЕНКО