МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний аерокосмічний університет
«Харківський авіаційний інститут»

ЗАТВЕРДЖУЮ

Голова приймальної комісії
Національного аерокосмічного університету
«Харківський авіаційний інститут»
_____ Олексій ЛИТВИНОВ
«___» _____ 2026 р.

ПРОГРАМА ВСТУПНОГО ВИПРОБУВАННЯ

для здобуття освітнього ступеня магістра
за освітньо-професійною програмою
зі спеціальності

F5 «Кібербезпека та захист інформації»
(код та найменування)

(освітня програма «Безпека інформаційних і комунікаційних систем»)
(найменування)

у 2026 році

Харків
2026

ВСТУП

Вступне випробування для здобуття освітнього ступеня магістра за освітньо-професійною програмою зі спеціальності F5 «Кібербезпека та захист інформації»
(код та найменування)
(освітня програма «Безпека інформаційних і комунікаційних систем»)
(найменування)
відбувається відповідно до «Правил прийому на навчання до Національного аерокосмічного університету «Харківський авіаційний інститут» в 2026 році» у формі індивідуального письмового фахового іспиту, який приймає фахова екзаменаційна комісія з певної спеціальності (освітньої програми), склад якої затверджується наказом ректора Університету.

Порядок оцінювання

До фахового іспиту входять питання за темами:
- Управління інформаційною безпекою;
- Комплексні системи захисту інформації;
- Комп'ютерні мережі;
- Захист інформації в інформаційно-комунікаційних системах.

Перелік питань за темами наведений у програмі.

Критерії оцінювання знань

1. Результат фахового іспиту визначається за шкалою від 100 до 200 балів.

Фаховий іспит проводиться у формі тестів, що складаються з 20 завдань з переліку питань, що входять до програми фахового іспиту. Серед запропонованих відповідей у тестовому завданні слід обрати одну правильну. Правильна відповідь на тестове завдання оцінюється у 6 балів, неправильна – у 0 балів.

3. Результат фахового іспиту розраховується за формулою:

$80+ k_1 + k_2 +\ldots + k_n$, де k_i – кількість балів за правильну відповідь на завдання і, де і змінюється від 1 до n, n – кількість завдань.

4. Якщо вступник отримав менше ніж 100 балів, то вважається що він не склав іспит і до участі в конкурсі не допускається.

1 Питання за темою «Управління інформаційною безпекою»

(найменування)

1. Основні етапи розробки системи управління інформаційною безпекою.
2. Елементи структури ISMS.
3. Методики оцінки ризику.
4. Способи знищення інформації.
5. Рівні організаційної роботи в сфері інформаційної безпеки.
6. Програмні алгоритми знищення даних.
7. Менеджмент в сфері інформаційної безпеки.
8. Основні етапи моделі Шухарта-Демінга.
9. Політика інформаційної безпеки (SecurityPolicy).
10. Підсумковий коефеціент в групі користувачів.
11. Проміжна ймовірність реалізації загрози.
12. Розрахунок ризиків по ресурсам.
13. Система управління інформаційною безпекою (Information Security Management System або ISMS).
14. Формула Андерсона.
15. Основні політики в сфері управління інформаційною безпекою.
16. Основні стандарти в області інформаційної безпеки.
17. Управління інформаційною безпекою (Information Security Management або ISM).
18. Затвердження Security Policy.
19. Заходи з забезпечення інформаційної безпеки.
20. Метрики для процесу управління інформаційною безпекою.

Література

1. Гребенніков В.В. Управління інформаційною безпекою (Менеджмент інформаційної безпеки). – Ужгород: Ужгородський національний університет, 2012. – 221 с.

2. Basta A. Linux Operations and Administration. Cengage Learning, 2012. – 496 p.

3. Аудит та управління інцидентами інформаційної безпеки : навчальний посібник / [Корченко О.Г., Гнатюк С.О., Казмірчук С.В., Панченко В.М., Мельник С.В.] – Київ, 2014. – 189 с.

4. Управління інформаційною безпекою : Конспект лекцій / [Носок С. О, Фаль О. М, Ткач В.М.] – Київ, 2021. – 258 с.

2 Питання за темою «Комплексні системи захисту інформації»

(найменування)

1. Активна компонента (суб'єкт), що виконує контроль операцій суб'єктів над об'єктами в захищеній КС.
2. Головна мета створення системи захисту інформації.

3. Вимірювання напруги побічних електромагнітних випромінювань і наведень.
4. Інструментальні методи технічного контролю.
5. Необхідні компоненти для створення КСЗІ.
6. Замкнута КС по породженню суб'єктів.
7. Монітор безпеки об'єктів.
8. Джерело для суб'єкта.
9. Об'єкт в момент часу асоційований з суб'єктом.
10. Об'єкти тотожні в момент часу.
11. Пожежний сповіщувач.
12. Пожежний оповіщувач.
13. Потоком інформації між об'єктами.
14. Суб'єкти КСЗІ.
15. Групи сповіщувачів.
16. Призначення СКУД.
17. Призначення СКУД електронної прохідної.
18. Призначення СТС.
19. Основні вимоги при розробці СТС.
20. Призначення системи пожежної сигналізації.

Література

1. Singh A.K., Mohan A.(Eds.) Handbook of Multimedia Information Security: Techniques and Applications. Springer, 2019. – 808 p.
2. Bishop M. Computer Security. 2nd ed. – Addison-Wesley Professional, 2018. – 2065 p.
3. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2018. – 118 с.
4. Хорошко В. О. та ін Проектування комплексних систем захисту інформації - Л.: Львівська політехніка, 2020. – 320 с.
5. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: Навчальний посібник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я.Ю. Усов. – Ніжин, 2019. – 144 с.

3 Питання за темою «Комп'ютерні мережі»
(найменування)

1. Кадри «ARP-запит» і «ARP-відповідь».
2. Смуга пропускання і пропускна здатність.
3. Розбиття мережі класу С використовуючи технологію CIDR.
4. Рівні моделі OSI.
5. Логічні топології. Метод доступу «за опитуванням арбітра».
6. Логічні топології. Метод доступу CSMA / CD.
7. Фізична топологія технології Fast Ethernet.

8. Комутатори (switch) для передачі кадрів даних.
9. Смуга пропускання кабелю «вита пара» категорії 4.
10. Логічна топологія «Зірка».
11. Рівні моделі OSI.
12. Вікно передачі протоколу TCP.
13. Пакети «DNS-запит» і «DNS-відповідь».
14. Повторна передача в протоколі TCP. Відправлений пакет.
15. Повторна передача в протоколі TCP. Вікно передачі.
16. Протокол RIP.
17. Протокол UDP.
18. Сеансовий рівень моделі OSI.
19. Спектр.
20. Фізична топологія «Шина».

Література

1. Марченко, О. І. Структури даних та алгоритми. Підручник у 2-х частинах. Частина 1 [Електронний ресурс] : підручник для здобувачів ступеня бакалавра за спеціальністю «Комп'ютерна інженерія» / О. І. Марченко, О. О. Марченко ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 9,88 Мбайт). – Київ : Просвіта, 2024. – 268 с.

2. Andrew S. Tanenbaum, David J. Wetherall. Computer Networks (5th Edition). Prentice Hall, 2010. – 960 p.

3. Pant M., Kumar T., Basterrech S., Banerjee C. (Eds.) Computational Network Application Tools for Performance Management. Springer, 2020. – 269 p.

4. Vij E.V. Computer Networks. New Delhi: University Science Press, 2018. – 363 p.

4 Питання за темою «Захист інформації в інформаційно-комунікаційних системах»

(найменування)

1. Алгоритм шифрування RSA.
2. Алгоритм шифрування.
3. Обмін конфіденційними повідомленнями за допомогою симетричної криптосистеми.
4. Комбінована криптосистема.
5. Алгоритм цифрового підпису DSA.
6. Забезпечення практичної неможливості підбору пароля зловмисником.
7. Цифровий підпис повідомлення.
8. Розшифрування повідомлення за допомогою асиметричного криптоалгоритма.
9. Формування коду автентифікації повідомлення.
10. Довжина ключа (в бітах) та кількість раундів криптоалгоритма DES.

11. Довжина ключа (в бітах) та кількість раундів криптоалгоритма ГОСТ 21847-89.

12. Протокол відкритого ключового обміну Діффі-Хеллмана.

13. Шифруюча послідовность, яка генерується синхронним потоковим криптоалгоритмом.

14. Методи криптографії.

15. Основна частина цифрового сертифіката.

16. Протокол Фейге-Фіата-Шаміра.

17. Стійкість криптографічних хеш-функцій до криптоаналізу на основі парадокса дня народження.

18. Схема шифрування Віженера.

19. Умовии створення абсолютно-стійкої криптосистеми.

20. Криптоперетворення на і-тому раунді криптоалгоритма, що реалізований за схемою Фейстеля.

Література

1. Остапов С.Е. Євсеєв С.П., Король О.Г. Технології захисту інформації. Навч. посібник. – Харків: Вид. ХНЕУ, 2013. – 476 с.

2. Bruce Schneier. Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley, 2015. – 784 p.

3. Технології захисту інформації. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсеєв С. П., Король О. Г., Остапов С. Е., Коц Г. П. – Х.: ХНЕУ ім. С.Кузнеця, 2016. – 1013 Мб.

4. Захист інформації в автоматизованих системах управління: навч. посіб. /Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с.

5. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ2000», 2020 . – 678 с.

Гарант освітньої програми «Безпека інформаційних і комунікаційних систем»

_____ Дмитро УЗУН
(підпис) (ініціали та прізвище)

Програму розглянуто й узгоджено на випусковій кафедрі кібербезпеки та інтелектуальних інформаційних технологій.

Протокол № 7 від « 16 » лютого 2026 р.

Завідувач кафедри 503 _____ Вячеслав ХАРЧЕНКО
(підпис) (ініціали та прізвище)

Програму вступного випробування для здобуття освітнього ступеня магістра за освітньо-професійною програмою зі спеціальності F5 «Кібербезпека та захист інформації» (освітня програма «Безпека інформаційних і комунікаційних систем») узгоджено галузевою науково-методичною комісією НМК 2 Національного аерокосмічного університету «Харківський авіаційний інститут».

Протокол № 8 від «13» 03 2026 р.

Голова НМК 2
к.т.н., доцент Дмитро КРИЦЬКИЙ