

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
Національний аерокосмічний університет ім. М. Є. Жуковського  
«Харківський авіаційний інститут»

**ЗАТВЕРДЖУЮ**

Голова приймальної комісії  
Національного аерокосмічного  
університету ім. М. Є. Жуковського  
«Харківський авіаційний інститут»

  
Олександр ЛИТВИНОВ  
2024 р.



**ПРОГРАМА  
ВСТУПНОГО ВИПРОБУВАННЯ**

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

**125 «Кібербезпека та захист інформації»**

(код та найменування)

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

**у 2024 році**

Харків  
2024

## ВСТУП

Вступне випробування для здобуття освітнього ступеня магістра за освітньо-професійною програмою зі спеціальності 125 «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 ім. М. Є. Жуковського «Харківський авіаційний інститут» в 2024 році» у формі індивідуального письмового фахового іспиту, який приймає фахова екзаменаційна комісія з певної спеціальності (освітньої програми), склад якої затверджується наказом ректора Університету.

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:

$80+k*n$ , де  $k$  – кількість балів за правильну відповідь на питання,  $n$  – кількість правильних відповідей.

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 (Security Policy).
10. Підсумковий коефіцієнт 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. Venkateswarlu N.B. (ed.) Introduction to Linux: Installation and Programming. BS Publications, 2008. – 607 p.
3. Adelstein Tom, Lubanovic Bill. Linux System Administration. O'Reilly Media, 2007. – 297 p.
4. Basta A. Linux Operations and Administration. Cengage Learning, 2012. – 496 p.
5. Campi N., Bauer K. Automating Linux and Unix System Administration. Apress, 2009. – 491 p.

## **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. Поток 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. Гребенніков В.В. Комплексні системи захисту інформації: проектування, впровадження, супровід. – Ужгород: Ужгородський національний університет, 2013. – 161 с.
2. Singh A.K., Mohan A.(Eds.) Handbook of Multimedia Information Security: Techniques and Applications. Springer, 2019. – 808 p.
3. Bishop M. Computer Security. 2nd ed. – Addison-Wesley Professional, 2018. – 2065 p.
4. Janczewski L.J., Wolfe H.B., Sheno S. (Eds.) Security and Privacy Protection in Information Processing Systems. Springer, 2013. – 447 p.

#### 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. Prasad K.V. Principles of Digital Communication Systems and Computer Networks. Charles River Media, 2003. – 815 p.
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.
5. Кулаков Ю.А. Луцький Г.М. Комп'ютерні мережі. Підручник за редакцією Ю.С. Ковтанюка – Київ.: Видавництво «Юніор», 2005. – 397с.

#### 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 послідовність, 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  $i$ -тому раунді криптоалгоритма, що реалізований за схемою Фейстеля.

### Література

1. Остапов С.Е. Євсєєв С.П., Король О.Г. Технології захисту інформації. Навч. посібник. – Харків: Вид. ХНЕУ, 2013. – 476 с.
2. William Stallings. Cryptography and Network Security Principles and Practices, Fourth Edition. Prentice Hall, 2005. – 592 p.
3. Bruce Schneier. Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley, 2015. – 784 p.
4. Katz J., Lindell Y. Introduction to Modern Cryptography: Principles and Protocols. Chapman and Hall/CRC, 2007. – 552 p.

Гарант освітньої програми «Безпека інформаційних і комунікаційних систем»



(підпис)

Дмитро УЗУН

(ініціали та прізвище)

Програму розглянуто й узгоджено на випусковій кафедрі комп'ютерних систем, мереж і кібербезпеки.

Протокол № 7 від «21» січня 2024 р.

Завідувач кафедри 503



(підпис)

Вячеслав ХАРЧЕНКО

(ініціали та прізвище)

Програму вступного випробування для здобуття освітнього ступеня магістра за освітньо-професійною програмою зі спеціальності 125 «Кібербезпека та захист інформації» (освітня програма «Безпека інформаційних і комунікаційних систем») узгоджено науково-методичною комісією Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» з галузей знань «Математика та статистика», «Інформаційні технології», «Автоматизація та приладобудування», «Хімічна та біоінженерія», «Електроніка та телекомунікації», «Природничі науки», «Архітектура та будівництво» (НМК 2).

Протокол № 8 від «22» 03 2024 р.

Голова НМК 2  
к.т.н., доцент



Дмитро КРИЦЬКИЙ