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»
_____ Олексій ЛИТВИНОВ
«28» 05 2024 р.

ПРОГРАМА ВСТУПНОГО ВИПРОБУВАННЯ

для здобуття освітнього ступеня доктора філософії
за освітньо-науковою програмою
зі спеціальності

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

(освітньо-наукова програма «Кібербезпека та захист інформації»)
(найменування)

у 2024 році

Харків
2024

ВСТУП

Вступне випробування для здобуття освітнього ступеня доктора філософії за освітньо-науковою програмою зі спеціальності 125 «Кібербезпека та захист інформації»
(код та найменування)
(освітньо-наукова програма «Кібербезпека та захист інформації»)
(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:

- Загрози кібербезпеці.
- Криптографія.
- Комплексна система захисту від кіберзагроз.
- Технології адміністрування та експлуатації систем кіберзахисту.
- Управління кібербезпекою.

Перелік питань за темами наведений у програмі.

Критерії оцінювання знань

1. Результат фахового іспиту визначається за шкалою від 100 до 200 балів.
2. Фаховий іспит проводиться у формі екзамену. Екзаменаційний білет складається з трьох питань, що входять до програми фахового іспиту.
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 Загрози кібербезпеці

(найменування)

1. Типи атак на інформаційні ресурси.
2. Типи атак на інформаційні системи.
3. Атаки доступу.
4. Атаки модифікації.
5. Комбіновані атаки.
6. Переповнення буферу.
7. DoS-атака.
8. SQL-ін'єкція.
9. Шкідливе програмне забезпечення.
10. Типи вірусів.
11. Механізми зараження.
12. Пошук вірусів.
13. Системи антивірусного захисту.
14. Антивірусне програмне забезпечення.
15. Трояни.
16. Комп'ютерні «черв'яки».
17. Сканери атак.
18. Евристичні аналізатори.
19. Аналіз коду підозрілих об'єктів.
20. Поведінковий аналіз.

Література

1. Когут Ю. І. Кібербезпека та ризики цифрової трансформації компаній. – Київ: SIDCON, 2021. – 372 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. Проєктування комплексних систем захисту інформації : підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. – 320 с.

2 Питання за темою Криптографія

(найменування)

1. Криптосистеми: базові поняття, призначення, класифікація.
2. Криптопротоколи: базові поняття, призначення, класифікація.
3. Симетричні криптоалгоритми.
4. Асиметричні криптоалгоритми.
5. Цифровий підпис.
6. Автентифікація користувачів.
7. Механізми розподілу ключів.
8. Методи аналізу криптосистем.

9. Методи побудови криптосистем.
10. Основні стандарти щодо реалізації криптосистем.

Література

1. Технології захисту інформації [Електронний ресурс]: підручник / Ю. А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с. URL: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf.
2. Криптографія від історії до сучасних стандартів: навч.посібник / Г. Л. Козіна. – Запоріжжя : НУ «Запорізька політехніка», 2020. – 192 с.
3. William Stallings. Cryptography and Network Security Principles and Practice, 7th Edition. Pearson, 2017. – 767 p.
4. Lorne Lantz, Daniel Cawrey. Mastering Blockchain : Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications. O'Reilly Media, Inc, USA, 2020. – 272 p.

3 Питання за темою Комплексна система захисту від кіберзагроз
(найменування)

1. Нормативно-правова база.
2. Програмні засоби захисту.
3. Технічні засоби захисту.
4. Механізми захисту мереж.
5. Аналіз трафіку.
6. Безпека в безпровідних мережах.
7. Безпека в операційних системах.
8. Функціональна безпека і кібербезпека.
9. Стандарти функціональної безпеки.
10. Методи оцінювання та забезпечення функціональної безпеки.

Література

1. Stallings William. Operating Systems: Internals and Design Principles. Pearson, 2017. – 704 p.
2. Krogh Einar. An Introduction to Windows Operating System. Bookboon, 2nd edition, 2017. – 137 p.
3. Лісовська Ю. П. Кібербезпека: ризики та заходи: навч. посібник. – К.: Видавничий дім «Кондор», 2019. – 272 с.
4. Гребенюк А. М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с.
5. Проєктування комплексних систем захисту інформації : підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. – 320 с.

4 Питання за темою Технології адміністрування та експлуатації систем кіберзахисту

(найменування)

1. Основи технології адміністрування та експлуатації систем кіберзахисту (СКЗ).
2. Адміністрування процесу проектування СКЗ.
3. Адміністрування процесу вводу в експлуатацію СКЗ.
4. Технічна експлуатація та обслуговування СКЗ.
5. Надійність СКЗ.

Література

1. Управління інформаційною безпекою. Конспект лекцій [Електронний ресурс] : навчальний посібник. – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с. URI: https://ela.kpi.ua/handle/123456789/43377
2. Проєктування комплексних систем захисту інформації : підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. – 320 с.
3. Bishop M. Computer Security. 2nd ed. – Addison-Wesley Professional, 2018. – 2065 p.
4. Гребенюк А. М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с.

5 Питання за темою Управління кібербезпекою

(найменування)

1. Система моніторингу.
2. Система аналізу уразливостей.
3. Система виявлення вторгнень.
4. Управління комплексними системами захисту.
5. Стандартизація у галузі моніторингу кіберсистем. Аналіз і управління ризиками.

Література

1. Проєктування комплексних систем захисту інформації : підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. – 320 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. Лісовська Ю. П. Кібербезпека: ризики та заходи: навч. посібник. – К.: Видавничий дім «Кондор», 2019. – 272 с.

Гарант освітньо-наукової програми «Кібербезпека та захист інформації»

_____ Володимир ПЄВНЄВ
(підпис) (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 _____ Вячеслав ХАРЧЕНКО
(підпис) (ініціали та прізвище)

ПОГОДЖЕНО

Проректор з наукової роботи університету Володимир ПАВЛІКОВ

Завідувач відділу аспірантури і докторантури Володимир СЕЛЕВКО