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»
_____ М. В. Нечипорук
«__22__» _____ 2021 р.

ПРОГРАМА ВСТУПНОГО ВИПРОБУВАННЯ

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

125 «Кібербезпека»
(код та найменування)

(освітньо-наукова програма «Кібербезпека»)
(найменування)

у 2021 році

Харків
2021

ВСТУП

Вступне випробування для здобуття освітнього ступеня доктора філософії за освітньо-науковою програмою зі спеціальності 125 «Кібербезпека»
(код та найменування)
(освітньо-наукова програма «Кібербезпека»)
(найменування)
відбувається відповідно до «Правил прийому на навчання до Національного аерокосмічного університету імені М. Є. Жуковського «Харківський авіаційний інститут» в 2021 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. 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., Shenoi S. (Eds.) Security and Privacy Protection in Information Processing Systems. Springer, 2013. – 447 p.

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. Горбенко Ю. І., Горбенко І. Д. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика. Монографія. – Х.: Форт, 2010. – 608 с.

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

3. William Stallings. Cryptography and Network Security Principles and Practices, Fourth Edition. Prentice Hall, 2005. – 592 p.

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

5. Katz J., Lindell Y. Introduction to Modern Cryptography: Principles and Protocols. Chapman and Hall/CRC, 2007. – 552 p.

3 Питання за темою <u>Комплексна система захисту від кіберзагроз</u>
(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. Tanenbaum A. S., Bos H. Modern Operating Systems. Prentice Hall, 2014. – 1136 p.

3. Кобозева А. А., Мачалін І. О., Хорошко В. О. Аналіз захищеності інформаційних систем. Підручник. – К.: ДУІКТ, 2010. – 316 с.

4. Управління інформаційною безпекою. Підручник. / Л. Ф. Єжова, І. О. Мачалін, Я. В. Невойт, В. О. Хорошко. – Севастополь: СНУ, 2010.

5. Павлов І. М., Хорошко В. О. Проектування комплексних систем захисту інформації. – К.: ВІП, 2011. – 245 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. Остапов С. Е. Євсеєв С. П., Король О. Г. Технології захисту інформації. Навч. посібник. – Харків: Вид. ХНЕУ, 2013. – 476 с.
2. Гребенніков В. В. Комплексні системи захисту інформації: проектування, впровадження, супровід. – Ужгород: Ужгородський національний університет, 2013. – 161 с.
3. Гребенніков В. В. Управління інформаційною безпекою (Менеджмент інформаційної безпеки). – Ужгород: Ужгородський національний університет, 2012. – 221 с.
4. Павлов І. М., Хорошко В. О. Проектування комплексних систем захисту інформації. – К.: ВІП, 2011. – 245 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. 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.

Гарант освітньо-наукової програми «Кібербезпека»

_____ В. Я. Пєвнєв
(підпис) (ініціали та прізвище)

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

Протокол № 7 від « 21 » січня 2021 р.

Завідувач кафедри 503 _____ В. С. Харченко
(підпис) (ініціали та прізвище)

ПОГОДЖЕНО

Проректор з наукової роботи університету _____ В. В. Павліков

Завідувач відділу аспірантури і докторантури _____ В. Б. Селевко