**«Ақпараттық қауіпсіздік негіздері» пәні бойынша**

**магистратураға түсуге арналған кешенді тестілеудің**

**ТЕСТ СПЕЦИФИКАЦИЯСЫ**

(2024 жылдан бастап қолданысқа енгізіледі)

**1. Құрастырудың мақсаты:** Қазақстан Республикасының жоғары оқудан кейінгі білім беру бағдарламаларын іске асыратын ұйымдарда оқуды жалғастыру мүмкіндігін анықтау.

**2. Міндеттері:** Үміткерлердің білім деңгейін білім беру бағдарламаларының келесі топтары бойынша анықтау:

**M195 - Криптология**

шифр Білім беру бағдарламалары тобының атауы

**3. Тесттің мазмұны:**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Тақырып мазмұны** | **Қиындық деңгейі** | **Тапсырмалар саны** |
| 1 | Криптография | А | 4 |
| 2 | Идентификация, Аутентификация, Авторизация | В | 2 |
| 3 | Желінің қауіпсіздігі | С | 5 |
| 4 | Зиянды бағдарлама | А/C | 2/1 |
| 5 | Ақпараттық қауіпсіздік технологиялары | В | 3 |
| 6 | Зиянкестердің түрлері | В | 3 |
| **Бір тестілік тапсырма саны** | | **20** | |

**4. Тапсырмалардың мазмұнын сипаттау:**

Бұл пәнде киберқауіпсіздік концепциясы, киберқауіпсіздікке төнетін қауіптер; ақпараттық қауіпсіздік технологияларының негіздері; ақпараттық қауіпсіздік инциденттеріне жауап қайтару және оларды өңдеу.

Ақпараттық қауіпсіздік негіздері пәні оқытады:

1. Киберқауіпсіздік ұғымы,

2. Зиянды бағдарламалардың түрлері

3. Киберқауіпсіздікке төнетін қауіптер;

4. Ақпараттық қауіпсіздік технологиялары

5. Симметриялық және асимметриялық шифрлау,

6. Хэш функциясы, HMAC,

7. Желілік қауіпсіздік инфрақұрылымы

8. Желілік қауіпсіздік мониторингі

9. Желіні қорғау

10. Ақпараттық қауіпсіздік инциденттеріне әрекет ету және өңдеу.

**5. Тапсырманы орындаудың орташа уақыты:**

Бір тапсырманың ұзақтығы - 2,5 минут.

Жалпы тестілеу уақыты - 50 минут.

**6. Тесттің бір нұсқасындағы тапсырмалар саны:**

Тесттің бір нұсқасында - 20 тапсырма.

Тест тапсырмаларын қиындық деңгейіне қарай бөлу:

- оңай (А) - 6 тапсырма (30%);

- орташа (В) - 8 тапсырма (40%);

- қиын (С) - 6 тапсырма (30%).

**7. Тапсырма формасы:**

Тест тапсырмалары жабық түрде, бір немесе бірнеше дұрыс жауапты таңдау арқылы ұсынылады.

**8. Тапсырманы бағалау:**

Үміткер ұсынылған нұсқалардың ішінен барлық дұрыс жауаптарды таңдап, толық жауап беруі керек. Барлық дұрыс жауаптардың таңдауы 2 (екі) баллмен бағаланады, бір қате үшін 1 (бір) балл, 2 (екі) немесе одан көп қате үшін 0 (нөл) балл алынады. Егер өтініш беруші қате жауап таңдаса немесе дұрыс жауапты таңдамаса, бұл қате ретінде қабылданады.

**9. Ұсынылатын әдебиеттер тізімі:**

1. Computer Security. Principles and Practice / William Stallings, Lawrie Brown.- Second edition.- USA: Pearson Education Inc., 2015.
2. Understanding Cryptography. Paar, C.- New York, 2010
3. Management of Information Security / M.E. Whitman, H.J. Mattord.- Fourth Edition.- USA: Cengage Learning, 2014
4. Applied cryptography: Protocols, Algorithms, and Source Code / Bruce Schneier.- United States of America: John Wiley & Sons, Inc, 1996
5. Securiti Enqineerinq  / R. Anderson.- Second edition.- Canada: Wiley, 2008.
6. Beautiful Security [Текст]: Leading Securuty Experts Explain How They Think / A. Oram, J. Viega.- USA, Sebastopol: O'Reilly, 2009.
7. Introduction to Hardware Security and Trust / M Tehranipoor; Editors: Wang Cliff.- USA: Springer, 2012.
8. Галицкий, А.В. Защита информации в сети - анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин. - М.: ДМК Пресс, 2016. - 615 c.
9. Емельянова, Н. З. Защита информации в персональном компьютере / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2015. - 368 c.
10. Степанов, Е.А. Информационная безопасность и защита информации. Учебное пособие / Е.А. Степанов, И.К. Корнеев. - М.: ИНФРА-М, 2014. - 304
11. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. - М.: "ДМК пресс. Электронные книги", 2014. - 592 c.
12. Алекс Вульф. Криптография. Основы практического шифрования и криптографии. 2023. ISBN 978-5-0060-1523-4. https://www.litres.ru/book/damir-sharifyanov/kriptografiya-osnovy-prakticheskogo-shifrovaniya-i-kript-69306412/chitat-onlayn/
13. Фрэнк Рубин: Криптография с секретным ключом. Издательство: ДМК-Пресс, 2022 г. ISBN: 978-5-97060-748-0. Страниц: 386
14. Воробьев С. П., Широбокова С. Н., Литвяк Р. К. Компьютерные сети и сетевая безопасность: учебное пособие. Издательство Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова. ISBN 978-5-9997-0805-2. 2022. 216 с.
15. Анализ вредоносных программ. Автор: Монаппа К. А Год: 2019. eBook. Страниц: 452. https://pyatilistnik.org/malware-analysis/