«ЗАТВЕРДЖУЮ»
Ректор Національного університету
«Одеська юридична академія»
_____ Олег ТОДОЩАК
протокол засідання Приймальної комісії
№ 3 від «28» березня 2025 р.

ПРОГРАМА

фахового іспиту

зі спеціальності F5 «Кібербезпека та захист інформації»

Одеса – 2025

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Фаховий іспит з «Кібербезпеки» – форма вступного випробування, яка передбачає очне або дистанційне оцінювання підготовленості (оцінювання знань, умінь та навичок) вступників для здобуття ступеня вищої освіти за спеціальністю F5 «Кібербезпека». За результатами фахового іспиту виставляється оцінка за шкалою 100-200 балів або ухвалюється рішення про негативну оцінку вступника («незадовільно»).

Фахове вступне випробування з «Кібербезпеки» проводиться у формі тестування.

Допуск вступників до фахового іспиту здійснюється за умови наявності документа, який засвідчує особу (зокрема з використанням Дії). У разі неможливості ідентифікації вступника фаховий іспит проводитись не може.

Фаховий іспит проводиться згідно з графіком, складеним приймальною комісією.

Під час фахового іспиту не дозволяється порушувати тишу, спілкуватися з іншими вступниками, користуватися електронними, друкованими, рукописними інформаційними джерелами.

Вступники, які не з'явилися фаховий іспит без поважних причин у визначений час, до участі у подальших випробуваннях та в конкурсі не допускаються. У разі виникнення обставин, що можуть становити загрозу для життя та здоров'я вступників співбесіда може бути припинена. За наявності поважних причин, підтверджених документально, вступники можуть бути допущені до пропущеного фахового іспиту з дозволу відповідального секретаря приймальної комісії в межах встановлених термінів та графіку вступних випробувань.

Перескладання фахового іспиту не дозволяється.

Середовищем для проведення фахового іспиту в дистанційному форматі (за рішенням закладу освіти; для осіб, які зареєстровані та перебувають на тимчасово окупованій території – за зверненням вступника) є сервіс Zoom. Приймальною

комісією надається Веб-посилання для доступу, інформація про час та вимоги проведення співбесіди в дистанційному форматі.

Вступники мають самостійно заздалегідь забезпечити технічну можливість приєднатися до фахового іспиту, виконати ряд вимог, які дадуть можливість ідентифікувати його та дотримання ним доброчесності:

- в приміщенні під час проходження фахового іспиту крім вступника не повинно бути інших осіб;
- перед початком фахового іспиту вступник через вебкамеру демонструє приміщення членам комісії та ідентифікує себе на підставі документа (одного з документів), що посвідчує особу.
- забороняється користуватись електронними приладами, підручниками. Весь час вступник повинен дивитися в напрямку відеокамери. Напрямок камери повинен бути налаштований таким чином, щоб було видно також робоче місце вступника. Мікрофон вступника також має бути постійно ввімкнений.

Вступники, які не можуть забезпечити виконання вимог до умов проведення фахового іспиту в дистанційному форматі, не допускаються до його проходження.

Вимоги до знань та умінь

Під час вступного випробування вступник повинен виявити знання:

- моделей та політик безпеки на основі використання сучасних принципів, способів та методів теорії захищених систем;
- клієнтських та серверних операційних систем з метою забезпечення цілісності, доступності та конфіденційності інформації та протидії несанкціонованому доступу;
- засобів та технологій криптографічного захисту інформації;
- програмного забезпечення інформаційних систем і мереж та їх компонентів для забезпечення їх належного функціонування;
- систем організації служби інформаційної безпеки в закладах різної інфраструктури та систем управління доступом до роботи з інформаційними системами;

- засобів та технологій захисту інформаційних систем і мереж на організаційно-адміністративному рівні;
- інформаційних систем різного призначення, засобів протоколювання, моніторингу та діагностики роботи складових систем і мереж;
- засоби і технології інженерно-технічного захисту інформаційних систем і інформації.

В цілому, ті, хто вступають повинні продемонструвати не лише знання базових теоретичних та методологічних основ кібербезпеки.

ТЕМАТИЧНИЙ ВИКЛАД ЗМІСТУ

Перелік питань

для підготовки до фахового іспиту зі спеціальності F5 «Кібербезпека»

1. У чому полягає проблема «кібербезпеки»?
2. Дайте визначення «кібербезпеки».
3. Перерахуйте компоненти кібербезпеки і їх визначення.
4. Яким чином взаємопов'язані між собою складові кібербезпеки? Наведіть власні приклади.
5. Перерахуйте рівні формування режиму кібербезпеки.
6. Перерахуйте основні документи по «кібербезпеки».
7. Які види вимог включає стандарт ISO / IEC 15408?
8. Дайте характеристику складових «кібербезпеки» стосовно до обчислювальних мереж.
9. Перерахуйте основні механізми безпеки.
10. Що розуміється під адмініструванням коштів безпеки?
11. Класи захищеності міжмережевих екранів.
12. Зміст адміністративного рівня забезпечення «кібербезпеки».
13. Дайте визначення політики безпеки.
14. Які характерні риси комп'ютерних вірусів?
15. Дайте визначення програмного вірусу.

16. Який вид вірусів найбільш розповсюджуваний в розподілених обчислювальних мережах? Чому?

17. Перерахуйте класифікаційні ознаки комп'ютерних вірусів.

18. У чому особливості резидентних вірусів?

19. Перерахуйте деструктивні можливості комп'ютерних вірусів.

20. Поясніть самошифрування і поліморфічность як властивості комп'ютерних вірусів.

21. Перерахуйте види «вірусоподібних» програм.

22. Поясніть механізм функціонування «троянської програми» (логічної бомби).

23. Поясніть поняття «сканування на льоту» і «сканування за запитом».

24. Перерахуйте види антивірусних програм.

25. uхарактеризуйте антивірусні сканери.

26. У чому особливості евристичних сканерів?

27. Які фактори визначають якість антивірусної програми?

28. Перерахуйте найбільш поширені шляхи зараження комп'ютерів вірусами.

29. Перерахуйте основні правила захисту від комп'ютерних вірусів, одержуваних з обчислювальних мереж.

30. Характерні риси макровірусу.

31. Як перевірити систему на наявність макровірусу?

32. Чи є наявність прихованих аркушів в Excel ознакою зараження макровірусів?

33. У чому полягають особливості забезпечення «кібербезпеки» комп'ютерних мереж?

34. Дайте визначення поняття «віддалена загроза».

35. У чому полягає специфіка методів і засобів захисту комп'ютерних мереж?

36. Поясніть поняття «глобальна мережева атака», наведіть приклади.

37. Які протоколи утворюють модель TCP / IP?

38. Який протокол забезпечує перетворення логічних мережевих адрес в апаратні?

39. Проведіть порівняльну характеристику моделей передачі даних TCP / IP і OSI / ISO.

40. На якому рівні моделі OSI / ISO реалізується сервіс безпеки «неспростовності» (згідно «Загальним критеріям»)?

41. Для чого призначений DNS-сервер?

42. Перерахуйте класи віддалених загроз.

43. Як класифікуються віддалені загрози «за характером впливу»?

44. Охарактеризуйте віддалені загрози «по ланцюгу впливу».

45. Чи може пасивна загроза привести до порушення цілісності інформації?

46. Дайте визначення типової віддаленої атаки.

47. Що є метою зловмисників при «аналізі мережевого трафіку»?

48. Назвіть причини успіху віддаленої атаки «помилковий об'єкт».

49. Що таке "сірі" IP-адреси і чим вони відрізняються від "білих"?

50. Назвіть основні рівні моделі OSI.

51. Що розуміється під ідентифікацією й аутентифікації користувача?

52. Перерахуйте можливі ідентифікатори при реалізації механізмів ідентифікації і аутентифікації.

53. Що таке «електронний ключ»?

54. Який з видів аутентифікації (стійка аутентифікація або постійна аутентифікація) більш надійний?

55. Що входить до складу криптосистеми?

56. Як реалізуються симетричний і асиметричний методи шифрування?

57. Що таке електронний цифровий підпис?

58. Перерахуйте методи розмежування доступу.

59. На чому заснований механізм реєстрації?

60. Які події, пов'язані з безпекою, підлягають реєстрації?

61. Чим відрізняються механізми реєстрації та аудиту?

62. Які етапи передбачають механізми реєстрації та аудиту?

63. У чому полягає принцип міжмережевого екранування?

64. Принцип функціонування міжмережевих екранів з фільтрацією пакетів.

65. Які сервіси безпеки включає технологія віртуальних приватних мереж?

66. Чому при використанні технології VPN IP-адреси внутрішньої мережі недоступні зовнішньої мережі?

67. Чим визначається політика безпеки віртуальної приватної мережі?

68. Опишіть структуру мережі Фейстеля

69. У чому полягає роль замін і перестановок в шифрі DES?

70. Назвіть слабкі сторони режиму шифрування ECB, як вони виправлені в режимі CBC?

71. Опишіть операцію розшифрування в режимі CFB.

72. У чому полягають завдання факторизації і визначення квадратичного вирахування? Розмістіть ці проблеми в порядке збільшення складності.

73. Опишіть алгоритм асиметричного шифрування RSA.

74. Коректно чи наступне висловлювання: «Злом алгоритму шифрування RSA еквівалентний розкладанню на множники модуля шифрування».

75. Порівняйте алгоритми RSA і Ель-Гамаля з точки зору можливості використання для постановки і верифікації ЕЦП.

76. Як з використанням електронного цифрового підпису вирішується завдання аутентифікації?

77. Чим хеш-функції відрізняються від блокових шифрів?

78. Опишіть алгоритм цифрового підпису DSA і поясніть, як в ньому забезпечується стійкість.

79. Що собою являє проблема розподілу ключів?

80. Які дії виконує центр сертифікації ключів?

81. Чому в сертифікат ключа включають термін його дії?

82. Перший етап злому: пасивний і активний збір інформації

83.Другий етап злому: сканування системи

84.Третій етап злому: отримання доступу

85.Четвертий етап злому: закріплення в системі

86.П'ятий етап злому: приховування слідів перебування

87.Короткий огляд вразливостей Wi-Fi

88.Бездротові мережі - загрози для WEP

89.Бездротові мережі - загрози для WPA

90.Бездротові мережі - загрози для Bluetooth

91.Атаки на веб-додатки:-файли

92.Атаки на веб-додатки: Міжсайтовий скриптинг (XSS)

93.Атаки на веб-додатки: Включення локальних або віддалених файлів

94.Атаки на веб-додатки: SQL-ін'єкції

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна література

1. Jason Andress. Foundations of Information Security: A Straightforward Introduction. No Starch Press, 1 edition, 2019.
2. Michael Collins. Network Security Through Data Analysis: From Data to Action. O'Reilly Media, 2 edition, 2017.
3. Gary McGraw. Software Security: Building Security In. Addison-Wesley Professional, 2006.
4. Grossman J. et al. XSS attacks: cross site scripting exploits and defense. – Syngress, 2007.
5. Stuttard D., Pinto M. The web application hacker's handbook: Finding and exploiting security flaws. – John Wiley & Sons, 2011.
6. Stallings W. et al. Computer security: principles and practice. – Upper Saddle River, NJ, USA : Pearson Education, 2012. – C. 978-0.
7. Cross M. Developer's guide to web application security. – Elsevier, 2011.
8. Wu H., Zhao L. Web Security: A WhiteHat Perspective. – CRC Press, 2015.
9. Rao U. H., Nayak U. The InfoSec handbook: An introduction to information security. – Apress, 2014.
10. Sullivan B., Liu V. Web application security, a beginner's guide. – McGraw-Hill Education Group, 2011.
11. Harper A. et al. Gray hat hacking the ethical hackers handbook. – McGraw-Hill Osborne Media, 2011.
12. Goodrich M. T., Tamassia R. Introduction to computer security. – Pearson, 2011.
13. Shema M. Hacking web apps: detecting and preventing web application security problems. – Newnes, 2012.
14. Shostack A. Threat modeling: Designing for security. – John Wiley & Sons, 2014.
15. Snyder, Chris, Thomas Myer, and Michael Southwell. Pro PHP security: from application security principles to the implementation of XSS defenses. Apress, 2011.
16. Weiss A. The Dark Side of Our Digital World: And What You Can Do about It. – Rowman & Littlefield Publishers, 2020.
17. Pauli J. The basics of web hacking: tools and techniques to attack the web. – Elsevier, 2013.
18. Scambray J., McClure S., Kurtz G. Hacking exposed. – McGraw-Hill Professional, 2000.
19. Chauhan S., Panda N. K. Hacking web intelligence: open source intelligence and web reconnaissance concepts and techniques. – Syngress, 2015.
20. Najera-Gutierrez G., Ansari J. A. Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux. – Packt Publishing Ltd, 2018.
21. Oriyano S. P. Hacker techniques, tools, and incident handling. – Jones & Bartlett Publishers, 2013.

22. ISO/IEC 14443-1. Identification Cards – Contactless integrated circuit(s) cards Proximity Cards Part 1: Physical characteristics International Standard. – 15.04.2000.
23. ISO/IEC 14443-2. Identification Cards – Contactless integrated circuit(s) cards Proximity Cards Part 2: Radio frequency power and signal interface International Standard. – 01.07.2001.

Список додаткової літератури

1. James Forshaw. Attacking Network Protocols: A Hacker's Guide to Capture, Analysis, and Exploitation. No Starch Press, 1 edition, 2018. Al Sweigart. Cracking Codes with Python: An Introduction to Building and Breaking Ciphers. No Starch Press, 2018.
2. Jean-Philippe Aumasson. Serious Cryptography: A Practical Introduction to Modern Encryption. No Starch Press, 2018.
3. Anthony DeBarros. Practical SQL: A Beginner's Guide to Storytelling with Data. No Starch Press, 2018.
4. Joshua Saxe. MALWARE DATA SCIENCE Attack Detection and Attribution. No Starch Press, 2018.
5. OccupyTheWeb. Linux Basics for Hackers: Getting Started with Networking, Scripting, and Security in Kali. No Starch Press, paperback edition, 2018.
6. Dennis Andriesse. Practical Binary Analysis. Build Your Own Linux Tools for Binary Instrumentation, Analysis, and Disassembly. No Starch Press, 2018.
7. Alana Maurushat. Ethical Hacking. Law, Technology And Media. University Of Ottawa Press, 2019.
8. Jim Kou. Hacking: The Practical Guide to Become a Hacker | Field Manual for Ethical Hacker | Including Ethical Hacking with Kali Linux. Independently published, 2019.
9. Stephan Goericke. The Future Of Software Quality Assurance. Springer, 2020.
10. Eben Hewitt. Semantic Software Design: A New Theory and Practical Guide for Modern Architects. O'Reilly Media, Inc., 2020.
11. Dimitre Dimitrov. Software Project Estimation: Intelligent Forecasting, Project Control, And Client Relationship Management. Apress, 2020.
12. Hyrum Wright Titus Winters, Tom Manshreck. Software Engineering at Google: Lessons Learned from Programming Over Time. O'Reilly Media, original retail edition, 2020.
13. Julia H. Allen, Sean J. Barnum, Robert J. Ellison, Gary McGraw, and Nancy R. Mead. Software Security Engineering. Addison-Wesley Professional, 1 edition, 2008.
14. Bruce Schneier, Tadayoshi Kohno, Niels Ferguson, and Tadayoshi Kohno. Cryptography Engineering: Design Principles and Practical Applications. John Wiley & Sons, Inc, 2012.
15. Peter van der Linden. Expert C Programming, Deep C Secrets. Prentice Hall, 1994.
16. Michal Zalewski. The tangled Web: a guide to securing modern Web applications. No Starch Press, 2012.

17. Jonathan E. Steinhart. The Secret Life of Programs. No Starch. No Starch Press, 2019.
18. Josh Lospinoso. C++ Crash Course: A Fast-Paced Introduction. No Starch Press, 2019.
19. Sergey Bratus Alex Matrosov, Eugene Rodionov. Rootkits And Bootkits: Reversing Modern Malware And Next Generation Threats. No Starch Press, 2019.

Інформаційні ресурси

1. OWASP Top Ten Web Application Security Risks | OWASP [Електронний ресурс]. – Режим доступу : https://owasp.org/www-project-top-ten/ (дата звернення: 2022-08-31). – Назва з екрана.
2. Security in Django | Django documentation | Django [Електронний ресурс]. – Режим доступу : https://docs.djangoproject.com/en/3.1/topics/security/ (дата звернення: 2022-08-31). – Назва з екрана.
3. Web Security [Електронний ресурс]. – Режим доступу : https://infosec.mozilla.org/guidelines/web_security.html (дата звернення: 2022-08-31). – Назва з екрана.
4. OWASP Automated Threats to Web Applications [Електронний ресурс]. – Режим доступу : https://owasp.org/www-project-automated-threats-to-web-applications/ (дата звернення: 2022-08-31). – Назва з екрана.
5. Table of Contents | OWASP [Електронний ресурс]. – Режим доступу : https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/ (дата звернення: 2022-08-31). – Назва з екрана.
6. Middleware | Django documentation | Django [Електронний ресурс]. – Режим доступу : https://docs.djangoproject.com/en/3.1/ref/middleware/ (дата звернення: 2022-08-31). – Назва з екрана.
7. C3: Secure Database Access | OWASP [Електронний ресурс]. – Режим доступу : https://owasp.org/www-project-proactive-controls/v3/en/c3-secure-database (дата звернення: 2022-08-31). – Назва з екрана.
8. OWASP Application Security Verification Standard [Електронний ресурс]. – Режим доступу : https://owasp.org/www-project-application-security-verification-standard/ (дата звернення: 2022-08-31). – Назва з екрана.
9. WSTG - Latest | OWASP [Електронний ресурс]. – Режим доступу : https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05-Testing_for_SQL_Injection (дата звернення: 2022-08-31). – Назва з екрана.
10. https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/12-Testing_for_Command_Injection
11. Injection Prevention - OWASP Cheat Sheet Series [Електронний ресурс]. – Режим доступу : https://cheatsheetseries.owasp.org/cheatsheets/Injection_Prevention_Cheat_Sheet.html (дата звернення: 2022-08-31). – Назва з екрана.

12. SQL Injection Prevention - OWASP Cheat Sheet Series [Електронний ресурс]. – Режим доступу : https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html (дата звернення: 2022-08-31). – Назва з екрана.
13. Injection Prevention in Java - OWASP Cheat Sheet Series [Електронний ресурс]. – Режим доступу : https://cheatsheetseries.owasp.org/cheatsheets/Injection_Prevention_in_Java_Cheat_Sheet.html (дата звернення: 2022-08-31). – Назва з екрана.
14. https://cheatsheetseries.owasp.org/cheatsheets/Query_Parameterization_Cheat_Sheet.html
15. Query Parameterization - OWASP Cheat Sheet Series [Електронний ресурс]. – Режим доступу : https://cheatsheetseries.owasp.org/cheatsheets/Query_Parameterization_Cheat_Sheet.html (дата звернення: 2022-08-31). – Назва з екрана.
16. Flask-Security — Flask-Security 3.0.0 documentation [Електронний ресурс]. – Режим доступу : https://pythonhosted.org/Flask-Security/ (дата звернення: 2022-08-31). – Назва з екрана.
17. How to Secure your Flask Application [Електронний ресурс]. – Режим доступу : https://damyanon.net/post/flask-series-security/ (дата звернення: 2022-08-31). – Назва з екрана.
18. Welcome to Flask-Security — Flask-Security 3.4.4 documentation [Електронний ресурс]. – Режим доступу : https://flask-security-too.readthedocs.io/en/stable/ (дата звернення: 2022-08-31). – Назва з екрана.
19. Running Your Flask Application Over HTTPS - miguelgrinberg.com [Електронний ресурс]. – Режим доступу : https://blog.miguelgrinberg.com/post/running-your-flask-application-over-https (дата звернення: 2022-08-31). – Назва з екрана.
20. How to build a web application using Flask and deploy it to the cloud [Електронний ресурс]. – Режим доступу : https://www.freecodecamp.org/news/how-to-build-a-web-application-using-flask-and-deploy-it-to-the-cloud-3551c985e492/ (дата звернення: 2022-08-31). – Назва з екрана.
21. SSL - Python Wiki [Електронний ресурс]. – Режим доступу : https://wiki.python.org/moin/SSL (дата звернення: 2022-08-31). – Назва з екрана.
22. Strong, Simple, and Precise security for Flask APIs (using jwt) [Електронний ресурс]. – Режим доступу : https://github.com/dusktreader/flask-praetorian (дата звернення: 2022-08-31). – Назва з екрана.
23. MB blog: XSS in Google Colaboratory + CSP bypass [Електронний ресурс]. – Режим доступу : https://blog.bentkowski.info/2018/06/xss-in-google-colaboratory-csp-bypass.html (дата звернення: 2022-08-31). – Назва з екрана.
24. MB blog: Another XSS in Google Colaboratory [Електронний ресурс]. – Режим доступу : https://blog.bentkowski.info/2018/09/another-xss-in-google-colaboratory.html (дата звернення: 2022-08-31). – Назва з екрана.
25. SSRF bible. Cheatsheet - Google Документи [Електронний ресурс]. – Режим доступу :

https://docs.google.com/document/d/1v1TkWZtrhzRLy0bYXBcdLUedXGb9njTNIJXa3u9akHM/edit (дата звернення: 2022-08-31). – Назва з екрана.
26. How to Hunt Bugs in SAML; a Methodology - Part I [Електронний ресурс]. – Режим доступу : https://epi052.gitlab.io/notes-to-self/blog/2019-03-07-how-to-test-saml-a-methodology/ (дата звернення: 2022-08-31). – Назва з екрана.
27. How to Hunt Bugs in SAML; a Methodology - Part II [Електронний ресурс]. – Режим доступу : https://epi052.gitlab.io/notes-to-self/blog/2019-03-13-how-to-test-saml-a-methodology-part-two/ (дата звернення: 2022-08-31). – Назва з екрана.
28. How to Hunt Bugs in SAML; a Methodology - Part III [Електронний ресурс]. – Режим доступу : https://epi052.gitlab.io/notes-to-self/blog/2019-03-16-how-to-test-saml-a-methodology-part-three/ (дата звернення: 2022-08-31). – Назва з екрана.
29. Excess XSS: A comprehensive tutorial on cross-site scripting [Електронний ресурс]. – Режим доступу : https://excess-xss.com/ (дата звернення: 2022-08-31). – Назва з екрана.
30. What Do WebLogic, WebSphere, JBoss, Jenkins, OpenNMS, and Your Application Have in Common? This Vulnerability. [Електронний ресурс]. – Режим доступу : https://foxglovesecurity.com/2015/11/06/what-do-weblogic-websphere-jboss-jenkins-opennms-and-your-application-have-in-common-this-vulnerability/ (дата звернення: 2022-08-31). – Назва з екрана.
31. GitHub's CSP journey - The GitHub Blog [Електронний ресурс]. – Режим доступу : https://github.blog/2016-04-12-githubs-csp-journey/ (дата звернення: 2022-08-31). – Назва з екрана.
32. GitHub's post-CSP journey - The GitHub Blog [Електронний ресурс]. – Режим доступу : https://github.blog/2017-01-19-githubs-post-csp-journey/ (дата звернення: 2022-08-31). – Назва з екрана.
33. GitHub - cure53/H5SC: HTML5 Security Cheatsheet - A collection of HTML5 related XSS attack vectors [Електронний ресурс]. – Режим доступу : https://github.com/cure53/H5SC (дата звернення: 2022-08-31). – Назва з екрана.
34. GitHub - dxa4481/cssInjection: Stealing CSRF tokens with CSS injection (without iFrames) [Електронний ресурс]. – Режим доступу : https://github.com/dxa4481/cssInjection (дата звернення: 2022-08-31). – Назва з екрана.
35. GitHub - LucaBongiorni/XSS.png: A XSS mind map ;) [Електронний ресурс]. – Режим доступу : https://github.com/LucaBongiorni/XSS.png (дата звернення: 2022-08-31). – Назва з екрана.
36. GitHub - payloadbox/sql-injection-payload-list: SQL Injection Payload List [Електронний ресурс]. – Режим доступу : https://github.com/payloadbox/sql-injection-payload-list (дата звернення: 2022-08-31). – Назва з екрана.
37. GitHub - payloadbox/xss-payload-list: Cross Site Scripting (XSS) Vulnerability Payload List [Електронний ресурс]. – Режим доступу : https://github.com/payloadbox/xss-payload-list (дата звернення: 2022-08-31). – Назва з екрана.

38. GitHub - qazbnm456/awesome-web-security: A curated list of Web Security materials and resources. [Електронний ресурс]. – Режим доступу : https://github.com/qazbnm456/awesome-web-security#xss---cross-site-scripting (дата звернення: 2022-08-31). – Назва з екрана.
39. GitHub - s0md3v/AwesomeXSS: Awesome XSS stuff [Електронний ресурс]. – Режим доступу : https://github.com/s0md3v/AwesomeXSS (дата звернення: 2022-08-31). – Назва з екрана.
40. PayloadsAllTheThings/CSRF Injection at master · swisskyrepo/ PayloadsAllTheThings · GitHub [Електронний ресурс]. – Режим доступу : https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/CSRF%20Injection (дата звернення: 2022-08-31). – Назва з екрана.
41. PayloadsAllTheThings/SAML Injection at master · swisskyrepo/ PayloadsAllTheThings · GitHub [Електронний ресурс]. – Режим доступу : https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/SAML%20Injection (дата звернення: 2022-08-31). – Назва з екрана.
42. PayloadsAllTheThings/Server Side Request Forgery at master · swisskyrepo/ PayloadsAllTheThings · GitHub [Електронний ресурс]. – Режим доступу : https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Server%20Side%20Request%20Forgery (дата звернення: 2022-08-31). – Назва з екрана.
43. PayloadsAllTheThings/SQL Injection at master · swisskyrepo/PayloadsAllTheThings · GitHub [Електронний ресурс]. – Режим доступу : https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/SQL%20Injection (дата звернення: 2022-08-31). – Назва з екрана.
44. PayloadsAllTheThings/Web Cache Deception at master · swisskyrepo/ PayloadsAllTheThings · GitHub [Електронний ресурс]. – Режим доступу : https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Web%20Cache%20Deception (дата звернення: 2022-08-31). – Назва з екрана.
45. PayloadsAllTheThings/XSS Injection at master · swisskyrepo/PayloadsAllTheThings · GitHub [Електронний ресурс]. – Режим доступу : https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XSS%20Injection (дата звернення: 2022-08-31). – Назва з екрана.
46. Any protection against dynamic module import? · Issue #243 · w3c/webappsec-csp · GitHub [Електронний ресурс]. – Режим доступу : https://github.com/w3c/webappsec-csp/issues/243 (дата звернення: 2022-08-31). – Назва з екрана.
47. HackerOne [Електронний ресурс]. – Режим доступу : https://hackerone.com/reports/293689 (дата звернення: 2022-08-31). – Назва з екрана.
48. Stored XSS on Facebook | OpnSec [Електронний ресурс]. – Режим доступу : https://opnsec.com/2018/03/stored-xss-on-facebook/ (дата звернення: 2022-08-31). – Назва з екрана.
49. Evading CSP with DOM-based dangling markup | PortSwigger Research [Електронний ресурс]. – Режим доступу :

https://portswigger.net/research/evading-csp-with-dom-based-dangling-markup (дата звернення: 2022-08-31). – Назва з екрана.
50. Practical Web Cache Poisoning | PortSwigger Research [Електронний ресурс]. – Режим доступу : https://portswigger.net/research/practical-web-cache-poisoning (дата звернення: 2022-08-31). – Назва з екрана.
51. XSS without parentheses and semi-colons | PortSwigger Research [Електронний ресурс]. – Режим доступу : https://portswigger.net/research/xss-without-parentheses-and-semi-colons (дата звернення: 2022-08-31). – Назва з екрана.
52. NetSPI SQL Injection Wiki [Електронний ресурс]. – Режим доступу : https://sqlwiki.netspi.com/ (дата звернення: 2022-08-31). – Назва з екрана.
53. StamOne_ [Електронний ресурс]. – Режим доступу : http://stamone-bug-bounty.blogspot.com/2017/10/dom-xss-auth14.html (дата звернення: 2022-08-31). – Назва з екрана.
54. $20000 Facebook DOM XSS : Vinoth Kumar [Електронний ресурс]. – Режим доступу : https://vinothkumar.me/20000-facebook-dom-xss/ (дата звернення: 2022-08-31). – Назва з екрана.
55. SSL & TLS HTTPS Testing [Definitive Guide] - Aptive [Електронний ресурс]. – Режим доступу : https://www.aptive.co.uk/blog/tls-ssl-security-testing/ (дата звернення: 2022-08-31). – Назва з екрана.
56. The most complete guide to finding anyone's email [Електронний ресурс]. – Режим доступу : https://www.blurbiz.io/blog/the-most-complete-guide-to-finding-anyones-email (дата звернення: 2022-08-31). – Назва з екрана.
57. Introduction to XSS [Електронний ресурс]. – Режим доступу : https://www.google.com/intl/sw/about/appsecurity/learning/xss/ (дата звернення: 2022-08-31). – Назва з екрана.
58. What is Clickjacking | Attack Example | X-Frame-Options Pros & Cons | Imperva [Електронний ресурс]. – Режим доступу : https://www.imperva.com/learn/application-security/clickjacking/ (дата звернення: 2022-08-31). – Назва з екрана.
59. SQL Injection Cheat Sheet | Netsparker [Електронний ресурс]. – Режим доступу : https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/ (дата звернення: 2022-08-31). – Назва з екрана.
60. Why CSP Should be carefully crafted: Twitter XSS & CSP Bypass - Paulos Yibelo - Blog [Електронний ресурс]. – Режим доступу : https://www.paulosyibelo.com/2017/05/twitter-xss-csp-bypass.html (дата звернення: 2022-08-31). – Назва з екрана.
61. THE BIG BAD WOLF - XSS AND MAINTAINING ACCESS - Paulos Yibelo - Blog [Електронний ресурс]. – Режим доступу : https://www.paulosyibelo.com/2018/06/the-big-bad-wolf-xss-and-maintaining.html (дата звернення: 2022-08-31). – Назва з екрана.
62. OSINT x UCCU Workshop on Open Source Intelligence [Електронний ресурс]. – Режим доступу : https://www.slideshare.net/miaoski/osint-x-uccu-workshop-on-open-source-intelligence (дата звернення: 2022-08-31). – Назва з екрана.
63. Red Team Tales 0x01: From MSSQL to RCE - Tarlogic Security - Cyber Security and Ethical hacking [Електронний ресурс]. – Режим доступу :

https://www.tarlogic.com/en/blog/red-team-tales-0x01/ (дата звернення: 2022-08-31). – Назва з екрана.
64. CWE - Common Weakness Enumeration [Електронний ресурс]. – Режим доступу : https://cwe.mitre.org/ (дата звернення: 2023-02-02). – Назва з екрана.
65. CVE [Електронний ресурс]. – Режим доступу : https://cve.mitre.org/ (дата звернення: 2023-02-02). – Назва з екрана.
66. MITRE ATT&CK® [Електронний ресурс]. – Режим доступу : https://attack.mitre.org/ (дата звернення: 2023-02-02). – Назва з екрана.
67. Matrix - Enterprise | MITRE ATT&CK® [Електронний ресурс]. – Режим доступу : https://attack.mitre.org/matrices/enterprise/ (дата звернення: 2023-02-02). – Назва з екрана.
68. What Is MITRE ATT&CK and How Is It Useful? | From Anomali [Електронний ресурс]. – Режим доступу : https://www.anomali.com/resources/what-mitre-attck-is-and-how-it-is-useful (дата звернення: 2023-02-02). – Назва з екрана.
69. Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards [Електронний ресурс]. – Режим доступу : https://www.pcisecuritystandards.org/document_library (дата звернення: 2023-02-02). – Назва з екрана.
70. https://www.iso.org/isoiec-27001-information-security.html
71. ISO - ISO/IEC 27001 — Information security management [Електронний ресурс]. – Режим доступу : https://www.iso.org/isoiec-27001-information-security.html (дата звернення: 2023-02-02). – Назва з екрана.
72. Schneier on Security [Електронний ресурс]. – Режим доступу : https://www.schneier.com/ (дата звернення: 2023-02-02). – Назва з екрана.
73. nmap [Електронний ресурс]. – Режим доступу : https://nmap.org/ (дата звернення: 2023-02-02). – Назва з екрана.
74. The GNU Netcat -- Official homepage [Електронний ресурс]. – Режим доступу : http://netcat.sourceforge.net/ (дата звернення: 2023-02-02). – Назва з екрана.
75. tcpdump [Електронний ресурс]. – Режим доступу : https://www.tcpdump.org (дата звернення: 2023-02-02). – Назва з екрана.
76. Logwatch SourceForge.net [Електронний ресурс]. – Режим доступу : https://sourceforge.net/projects/logwatch/ (дата звернення: 2023-02-02). – Назва з екрана.
77. BorgBackup – Deduplicating archiver with compression and authenticated encryption [Електронний ресурс]. – Режим доступу : https://www.borgbackup.org/ (дата звернення: 2023-02-02). – Назва з екрана.
78. Github.com / linux-audit [Електронний ресурс]. – Режим доступу : https://github.com/linux-audit (дата звернення: 2023-02-02). – Назва з екрана.
79. Lynis - Security auditing tool for Linux, macOS, and Unix-based systems - CISOfy [Електронний ресурс]. – Режим доступу : https://cisofy.com/lynis/ (дата звернення: 2023-02-02). – Назва з екрана.
80. systemd [Електронний ресурс]. – Режим доступу : https://systemd.io/ (дата звернення: 2023-02-02). – Назва з екрана.

81. systemd - Debian Wiki [Електронний ресурс]. – Режим доступу : https://wiki.debian.org/systemd (дата звернення: 2023-02-02). – Назва з екрана.
82. systemd/Journal - ArchWiki [Електронний ресурс]. – Режим доступу : https://wiki.archlinux.org/index.php/Systemd/Journal (дата звернення: 2023-02-02). – Назва з екрана.
83. SystemdForUpstartUsers - Ubuntu Wiki [Електронний ресурс]. – Режим доступу : https://wiki.ubuntu.com/SystemdForUpstartUsers (дата звернення: 2023-02-02). – Назва з екрана.
84. Clonezilla - About [Електронний ресурс]. – Режим доступу : https://clonezilla.org/ (дата звернення: 2023-02-02). – Назва з екрана.
85. Security - ArchWiki [Електронний ресурс]. – Режим доступу : https://wiki.archlinux.org/index.php/Security (дата звернення: 2023-02-02). – Назва з екрана.
86. Zimmerman C. The strategies of a world-class cybersecurity operations center [Електронний ресурс]. – Режим доступу : http://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf (дата звернення: 2023-02-02). – Назва з екрана.

КРИТЕРІЇ ОЦІНЮВАННЯ

Фаховий іспит складається з 25 тестових завдань закритого типу. Завдання має основу та чотири варіанти відповіді, з яких лише один правильний. Завдання вважається виконаним, якщо учасник/ця тестування вибрав/ла, позначив/ла відповідь, а також підтвердив/ла свій вибір.

Схема нарахування балів: 0 або 1 бал

1 бал, якщо вказано правильну відповідь;

0 балів, якщо вказано неправильну відповідь, вказано декілька відповідей або відповідь на завдання не надано.

Максимальна кількість балів за виконання тестових завдань – 25, мінімальна – 0.

Результат фахового іспиту переводиться в шкалу 100–200 балів.

Мінімальна сума балів, з якою вступник допускається до участі у конкурсі складає 100 балів.

У разі не набрання мінімальної кількості балів ухвалюється рішення про негативну оцінку («незадовільно»).

Таблиця переведення балів з фахового іспиту до шкали 100–200 балів

Тестовий бал	Бал за шкалою 100–200
1 2 3 4	0
5	100
6	105
7	110

8	115
9	120
10	125
11	130
12	135
13	140
14	145
15	150
16	155
17	160
18	165
19	170
20	175
21	180
22	185
23	190
24	195
25	200

Голова комісії **Віктор БОЙКО**