МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ

ЗАТВЕРДЖУЮ
Голова приймальної комісії
Ректор
_____ Олександр НАЗАРЕНКО
«__11__» ___05___ 2026 р.

ПРОГРАМА

ФАХОВОГО ІСПИТУ

для конкурсного відбору вступників

на другий (магістерський) рівень вищої освіти

Галузь знань	**F Інформаційні технології**
Спеціальність	**F5 Кібербезпека та захист інформації**
Освітня програма	**Кібербезпека та захист інформації**

ОДЕСА – 2026

Загальні положення

Програма фахового іспиту є нормативним документом для проведення вступних випробувань осіб, що здобули освітньо-кваліфікаційний рівень бакалавра та проходять вступні випробування (тестування з фаху) для подальшого навчання за освітньою програмою «Кібербезпека та захист інформації» на другому (магістерський) рівні вищої освіти.

Згідно з чинними «Правилами прийому до Державного університету інтелектуальних технологій і зв'язку у 2026 році», для охочих продовжити навчання за освітнім ступенем «магістр» на основі другого рівня освіти передбачено обов'язкове складання фахового випробування (тестування) з фахової дисципліни. Нижче наведена структура даного випробування та навчальні матеріали, які рекомендовані для опрацювання в ході підготовки до нього. Фахове випробування складається з 50-ти тестових питань.

Перелік питань складено відповідно до рівня спорідненості, отриманої абітурієнтом, спеціальності освітньо-кваліфікаційного рівня «бакалавр» при вступі на перший курс навчання за другим (магістерським) рівнем вищої освіти в межах вакантних місць ліцензованого обсягу за спеціальностями (напрямами підготовки) відповідно до переліку спеціальностей (напрямів підготовки), за якими здійснювався набір на перший курс до Університету згідно «Правил прийому до Державного університету інтелектуальних технологій і зв'язку у 2026 році».

Абітурієнту пропонується лист тестування для фахового іспиту, який складається із 50-ти завдань. Кожне завдання має чотири варіанти відповідей, одна з яких є правильною, яка оцінюється в 4 бали. Максимальна кількість отриманих балів – 200. Питання для складання тестових задач взято з відповідної навчальної програми дисципліни відповідно до програми підготовки магістрів вище перелічених спеціальностей, які визначені згідно вступу абітурієнта на відповідний курс навчання.

При оцінюванні знань абітурієнта під час фахового випробування (тестування з фаху) використовується 200-бальна система оцінки, за якою оцінка «відмінно» відповідає 176-200 балам, оцінка 4 «добре» – 136-172 балам, оцінка «задовільно» – 100-132 балам, при отриманні менш ніж 100 балів абітурієнт отримує оцінку «незадовільно».

Перелік питань для підготовки до фахового іспиту

В основу тестових завдань покладено наступні теми:

1. Основні поняття кібербезпеки. Конфіденційність, цілісність та доступність.
2. Керування доступом. Авторизація, автентифікація, облік (аудит). Загальні принципи керування доступом.
3. Процес автентифікації – паролі, токени, біометрія.
4. Двофакторна автентифікація.
5. Протоколи автентифікації. Протокол Kerberos.
6. Права користувачів в операційній системі та мережі.
7. Основні моделі керування доступом.
8. Модель OSI.
9. Модель TCP/IP.
10. Основні мережеві протоколи.
11. Основі протоколи VPN-тунелювання.
12. Поняття PLS – Physical Layer Security.
13. Протоколи канального рівня та атаки на них.
14. Протоколи безпеки сеансового рівня.
15. Традиційні брандмауери.
16. Брадмауери наступного покоління (NGFW).
17. Системи виявлення та запобігання вторгнень (IDPS).
18. Елементи безпечної архітектури комп'ютерної мережі – VPN, NAT, BYOD.
19. Архітектура Zero Trust.
20. Захист від шкідливого програмного забезпечення.
21. Основні симетричні та асемитричні алгоритми шифрування.
22. Захист інформації у банківських системах.
23. Калсична архітектура фон Неймана.
24. Системи SSO.
25. Класичні атаки на інформаційні системи.
26. Соціальна інженерія. Основні механізми атак та захист від них.
27. Проксі-сервери.
28. Засоби захисту від IP-спуфінгу.
29. Відмінність IDS та IPS систем.
30. Основи хмарних обчислень та їх проблеми безпеки.
31. Основи контейнеризації. Архітектура CI/CD.
32. Забезпечення надійності паролю.
33. Що таке шина комп'ютера, і яка її роль у взаємодії компонентів системи?

34. Які компоненти входять у структуру комп'ютера згідно класичної архітектури фон Неймана?

35. Що таке кеш-пам'ять, і яку роль вона виконує в ієрархічній структурі пам'яті?

36. Що таке кіберпростір та інформаційний простір, і яка їх роль у сучасному світі?

37. Що таке кіберзагрози та кібератаки, і як вони можуть вплинути на системи та користувачів?

38. Що таке DDoS-атаки, і як вони можуть вплинути на роботу мережі?

39. Що таке фішинг та як він може бути небезпечним для інтернет-користувачів?

40. Які заходи безпеки можуть бути використані для захисту від шкідливого програмного забезпечення?

41. Що таке комп'ютерна мережа?

42. Топології комп'ютерних мереж.

43. Які основні рівні ієрархії протоколів в моделі ISO/OSI та моделі TCP/IP?

44. Що таке Інтернет Речей?

45. Які основні функції виконує DNS (Domain Name System) у Інтернеті?

46. Що означає поняття "відмовостійкість" у контексті операційних систем?

47. Яка різниця між логічною та фізичною організацією файлів?

48. Які типи файлових систем використовуються в сучасних комп'ютерних системах?

49. Які технології використовуються в сучасних операційних системах для захисту від вторгнень та забезпечення безпеки користувачів?

50. Які основні функції виконує операційна система?

Критерії оцінювання

Критерії оцінювання відповіді вступника за шкалою від 0 до 200 балів. Тест з вступних випробувань складається з 50-ти тестових завдань. Кожне з 50-ти тестових завдань має чотири варіанти відповідей, одна з яких є правильною, яка оцінюється в 4 бали. Максимальна кількість отриманих балів – 200.

4. Структура екзаменаційного білета або тестового завдання

ВКЛАДКА

ШИФР _____

ЗАТВЕРДЖУЮ
Голова приймальної комісії
ректор ДУІТЗ
_____Олександр НАЗАРЕНКО
„ _____ ” _____ 2026 р.

УВАГА! Підписувати, робити будь-які помітки, що розшифровують роботу, ЗАБОРОНЯЄТЬСЯ !

ЛИСТ ТЕСТУВАННЯ ДЛЯ ФАХОВОГО ІСПИТУ

(для здобуття другого (магістерський) рівня вищої освіти)

ВАРІАНТ № ___

Тест з фахових вступних випробувань складається із 50-ти задач. Кожна задача має чотири варіанти відповідей, одна з яких є правильною, яка оцінюється в 4 бали. Максимальна кількість отриманих балів – 200. В таблиці відповідей необхідно в клітці, що знаходиться на перетині номеру задачі та букви визначеної Вами правильної відповіді (А, Б, В, Г), зробити позначку: **Х**

Відповідь	Номер завдання																								
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
А																									
Б																									
В																									
Г																									

Відповідь	Номер завдання																								
	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
А																									
Б																									
В																									
Г																									

1. Які три елементи безпекової тріади?

А) Автентифікація, авторизація та облік;
Б) Конфіденційність, цілісність та доступність;
В) Ідентифікація, автентифікація та авторизація;
Г) Конфіденційність, цілісність та авторизація.

2. Що таке ААА інформаційної безпеки?

А) Автентифікація, доступність та авторизація;
Б) Облік, автентифікація та доступність;
В) Автентифікація, авторизація та облік;
Г) Доступність, облік та авторизація.

3. Який тип послуг надає Kerberos?

А) Автентифікацію;
Б) Облік;
В) Доступність;
Г) Підзвітність.

4. Який метод аутентифікації вважається найбільш захищеним?

А) Парольна автентифікація
Б) Двофакторна автентифікація (2FA)
В) Використання PIN-коду
Г) Вхід без пароля

Рекомендована література

1. Методи та засоби захисту інформації : навч. посіб. / В. А. Лахно, Є. В. Василіу, В. М. Гладких та ін. Київ : ЦП «Компринт», 2021. 444 с.
2. Тарнавський Ю. А. Технології захисту інформації : навч. посіб. / Ю. А. Тарнавський. Київ : КПІ ім. Ігоря Сікорського, 2018. 162 с.
3. Stavroulakis P., Stamp M. Handbook of Information and Communication Security. Berlin : Springer-Verlag, 2010. 863 p.
4. Богуш В. М., Юдін О. К. Інформаційна безпека держави : навч. посіб. / В. М. Богуш, О. К. Юдін. Київ : МК-Прес, 2005. 432 с.
5. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою : навч. посіб. / А. М. Гребенюк, Л. В. Рибальченко. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2020. 144 с.
6. Пількевич І. А., Лобанчикова Н. М., Молодецька К. В. Захист інформації в автоматизованих системах управління : навч. посіб. / І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. Житомир : Вид-во ЖДУ ім. І. Франка, 2015. 226 с.
7. Кавун С. В., Носов В., Манжай О. В. Інформаційна безпека : навч. посіб. / С. В. Кавун, В. Носов, О. В. Манжай. Харків : Вид. ХНЕУ, 2008. Ч. 2. 166 с.
8. Інформаційна безпека: термінологічний навчальний довідник / В. М. Богуш, В. Г. Кривуца, А. М. Кудін ; за ред. В. Г. Кривуци. Київ : Д.В.К., 2004. 508 с.
9. Maymi F., Harris S. CISSP All-in-One Exam Guide. 9th ed. New York : McGraw-Hill Education, 2021. 1320 p.
10. Gibson D. SSCP Systems Security Certified Practitioner Exam Guide. 2nd ed. New York : McGraw-Hill Education, 2016. 554 p.

Голова фахової атестаційної комісії Володимир КОРЧИНСЬКИЙ