МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій, обліку та фінансів

ЗАТВЕРДЖЕНО

Голова приймальної комісії

_____ Олег СКИДАН

16.07.2025 р., протокол № 4

П Р О Г Р А М А

комплексного вступного випробування за фахом
при зарахуванні на навчання на основі освітнього ступеня бакалавр,
освітньо-кваліфікаційного рівня спеціаліст, освітнього ступеня магістр
для здобуття освітнього ступеня магістр
зі спеціальності F5 «Кібербезпека та захист інформації»
ОП «Кібербезпека»

Житомир – 2025

Перелік питань, які виносяться на фахове вступне випробування

1. Сутність поняття кібербезпеки та визначення захисту інформації.
2. Поняття комплексної системи захисту інформації, порядок її створення.
3. Нормативно-правові документи у сфері кібербезпеки та захисту інформації.
4. Державні та міжнародні стандарти у сфері кібербезпеки та захисту інформації.
5. Базові категорії криптографії: алфавіт, ключ, текст, шифрування, дешифрування. Вимоги до криптосистем.
6. Класифікація криптосистем.
7. Технічні канали витоку інформації: визначення та їх класифікація.
8. Класи автоматизованих систем, функціональні послуги безпеки та профіль захищеності.
9. Поняття стеганографії, її класифікація та алгоритми.
10. Категорії конфіденційність, цілісність, доступність інформації. Методи їх забезпечення.
11. Сутність та визначення цифрового підпису.
12. Прості хеш-функції і сильна хеш-функція *MD5*.
13. Система управління (менеджменту) інформаційної безпеки.
14. Визначення кіберпростору, кіберзахисту, кіберзагрози та кібератаки.
15. Поняття ризику інформаційної безпеки та методики його оцінки.
16. Поняття інформації з обмеженим доступом, її класифікація.
17. Поняття конфіденційної інформації, персональних даних та їх захисту.
18. Поняття несанкціонованого доступу до інформації. Принципи захисту інформації від несанкціонованого доступу.
19. Поняття ідентифікації, аутентифікації та авторизації користувача.
20. Поняття стратегії та політики інформаційної безпеки.
21. Сутність моделей розмежування доступу: дискреційна, мандатна, рольова.
22. Поняття моделі загрози і моделі порушника.
23. Поняття режимне приміщення. Порядок побудови комплексу технічного захисту інформації.
24. Визначення об’єкта інформаційної діяльності.
25. Організація захисту баз даних та їх адміністрування.
26. Основні мережеві моделі та протоколи.
27. Поняття шкідливого програмного забезпечення в операційних системах та їх класифікація.

28. Види антивірусного програмного забезпечення та його застосування в системах безпеки.
29. Протоколи побудови віртуальних приватних мереж.
30. Особливості системи захисту комп'ютерної мережі з використанням міжмережевих екранів.
31. Проблеми та можливості забезпечення безпеки баз даних.
32. Складові процесу управління ризиками інформаційної безпеки відповідно до ISO/IEC 27005.
33. Складові процесу побудови системи управління інформаційної безпеки відповідно до ISO/IEC 27001.
34. Асиметричні криптографічні системи шифрування.
35. Класифікація атак криптографічного аналізу.
36. Методи та способи організації захисту web-додатків.
37. Етапи проектування захищених інформаційних систем.
38. Симетричні алгоритми блокового шифрування даних.
39. Засоби та способи забезпечення безпеки операційних систем.
40. Визначення та особливості розподілу ключів в інформаційних системах.

Порядок проведення та оцінювання результатів фахового вступного іспиту

На фаховому вступному іспиті абітурієнт отримує письмове завдання, бланк результатів іспиту та титульний аркуш зі штампом Приймальної комісії університету. Фаховий вступний іспит проводиться в письмовій формі або на основі індивідуальної усної співбесіди. Перед вступним іспитом представники приймальної комісії проводять інструктаж щодо порядку виконання фахового вступного іспиту.

На бланку результатів абітурієнт вказує за номером питання та надає письмово правильну відповідь. Виправлення, декілька позначень і відсутність результату відповіді за питанням зараховуються як невірна відповідь. Не допускаються будь-які умовні позначки на бланку результатів іспиту та титульному аркуші.

Письмове завдання містить 3 питання на які потрібно надати правильну відповідь. Кожна правильна відповідь оцінюється у 60 балів. Максимально можлива кількість набраних балів після складання фахового іспиту – 180. Кількість балів необхідна для участі в конкурсі повинна дорівнювати або бути більшою за 100.

Тривалість іспиту – 120 хвилин.

Зарахування для навчання до Поліського національного університету здійснюється за рейтинговою системою.

Список рекомендованої літератури для самостійної підготовки вступника до фахового вступного випробування

1. Молодецька К. В. Захист інформації в автоматизованих системах управління : навч. посіб. / К. В. Молодецька, Н. М. Лобанчикова, І. А. Пількевич. – Житомир : вид-во ЖДУ ім. І. Франка, 2015. – 170 с.

2. Прикладна криптологія : системи шифрування [Текст] : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с.

3. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія / Корченко О.Г., Казмірчук С.В., Ахметов Б.Б. – Київ, ЦП «Компринт», 2017. – 435 с

4. Горбенко І. Д. Прикладна криптологія. Теорія. Практика. Застосування / І. Д. Горбенко, Ю. Д. Горбенко. – Х.: Форт, 2012. – 870 с.

5. Захист інформації в комп'ютерних системах та мережах : навч. посібник / С. Г. Семенов [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : НТУ "ХПІ", 2014. – 251 с.

6. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

7. Основи захисту інформації / Даник Ю. Г., Вдовенко С. Г., Шестаков В. І., Писарчук О. О., Грищук Р. В., Куликівський М. В., Ходаківський В. М. – Житомир : ЖВІ ДУТ, 2015. – 202 с.

8. Бурячок В. Л. Політика інформаційної безпеки : підручник / В. Л. Бурячок, Р. В. Грищук, В. О. Хорошко / За заг. ред. докт. техн. наук, проф. В. О. Хорошка. – Київ : ПВП “Задруга“, 2014. – 222 с.

9. Юдін О.І., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних – К.: Вид-во ТОВ «НВП» Інтерсервіс», 2014. – 716 с.

10. Грищук Р. В. Основи кібернетичної безпеки / Р. В. Грищук, Ю. Г. Даник; за заг. ред. проф. Ю.Г. Даника. – Житомир: ЖНАЕУ, 2016. – 636 с.

11. Основи кіберпростору, кібербезпеки та кіберзахисту / Богуш В.М., Богуш В.В., Бровко В.Д., Настрадін В.П. – Ліра-К, 2020. – 554 с.

12. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К.: Видавнича група BHV

13. Корченко О.Г. Охорона конфіденційної інформації підприємства [Текст]: навчальний посібник / О.Г. Корченко, Ю.О. Дрейс. – Житомир: ЖВІ НАУ, 2011. – 172 с.

14. Менеджмент інформаційної безпеки: навч. пос./ О. Г. Корченко, М. Є. Шелест, С. В. Казмірчук, Ю. М. Ткач, Є. В. Іванченко. – Ніжин: «Орхідея», 2019. – 408 с.