МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій, обліку та фінансів

ЗАТВЕРДЖЕНО

Голова приймальної комісії

_____Олександр КОВАЛЬЧУК

05.05 2026 р., протокол № 4

ПРОГРАМА

комплексного вступного випробування за фахом
для здобуття освітнього ступеня магістр
зі спеціальності F5 «Кібербезпека та захист інформації»
ОП «Кібербезпека»

Житомир – 2026

ВСТУП

Програма вступних випробувань до Поліського національного університету для здобуття освітнього ступеня «Магістр» спеціальності F5 «Кібербезпека та захист інформації» розроблена на підставі Законів України «Про освіту» та «Про вищу освіту», Положення про приймальну комісію Поліського національного університету на 2026 рік та складена відповідно до програми предметного тесту з інформаційних технологій і кібербезпеки єдиного фахового вступного випробування (ЄФВВ) для вступу на навчання для здобуття ступеня магістра на основі НРК 6, НРК 7 (затвердженої Наказом Міністерства освіти і науки України від 19.04.2024 р. № 552).

Програма передбачає оцінювання рівня засвоєних здобувачем спеціальних компетентностей, визначених Стандартом вищої освіти першого (бакалаврського) рівня вищої освіти галузі знань F «Інформаційні технології», спеціальності F5 «Кібербезпека та захист інформації» (затвердженого та введеного в дію відповідним Наказом Міністерства освіти і науки України).

Програма складається з переліку питань за темами, які відображають окремі аспекти спеціальності, та інтегрує знання з ключових фахових дисциплін бакалаврату. Мета фахового іспиту – оцінювання рівня здобутих професійних знань, умінь та навичок вступників.

СТРУКТУРА ПРОГРАМИ

РОЗДІЛ 1. Теоретичні основи кібербезпеки, нормативно-правове забезпечення та стандартизація

Сутність поняття кібербезпеки. Визначення та задачі захисту інформації (ЗІ). Структура та компоненти кіберпростору. Визначення понять: кіберзахист, кіберзагроза, вразливість, кібератака, кіберінцидент. Класифікація джерел кіберзагроз.

Класична тріада інформаційної безпеки: конфіденційність, цілісність, доступність інформації. Додаткові властивості: автентичність, підзвітність, незаперечність. Організаційно-технічні методи забезпечення КЦД. Інформація з обмеженим доступом (ІОД) та її законодавча класифікація. Поняття конфіденційної інформації, таємної інформації (державна, комерційна, банківська таємниця) та службової інформації. Персональні дані (ПД) як об'єкт захисту, особливості обробки та транскордонної передачі ПД.

Законодавство України у сфері ЗІ та кібербезпеки: Закони України «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про захист персональних даних». Національна система кібербезпеки. Державні та міжнародні стандарти. Роль інститутів стандартизації (НД ТЗІ, ДСТУ, ISO, NIST). Огляд базових сімейств стандартів інформаційної безпеки.

РОЗДІЛ 2. Менеджмент інформаційної безпеки, ризики та проєктування захищених систем

Поняття КСЗІ в інформаційно-комунікаційних системах (ІКС). Нормативно-правова база створення КСЗІ в Україні. Порядок та етапи розробки, впровадження й експлуатації КСЗІ. Стадії життєвого циклу системи захисту. Державна експертиза КСЗІ, отримання Атестата відповідності. Об'єкти інформаційної діяльності (ОІД) та їх паспортизація.

Класифікація автоматизованих систем (АС) за ознаками обробки інформації та архітектури (класи 1, 2, 3). Функціональний профіль захищеності (ФПЗ): критерії оцінки, послуги безпеки (конфіденційність, цілісність, доступність, спостережність), рівні гарантій за НД ТЗІ. Поняття моделі загроз та моделі порушника (внутрішній/зовнішній порушник, класифікація за рівнем можливостей та потенціалу).

Концепція та архітектура СУІБ. Стратегія та політика інформаційної безпеки підприємства: рівні формування, структура, вимоги до перегляду. Етапи та складові процесу побудови СУІБ відповідно до вимог міжнародного стандарту ISO/IEC 27001 (модель PDCA: Plan-Do-Check-Act, організаційний контекст, лідерство, планування, підтримка).

Поняття ризику інформаційної безпеки. Ідентифікація, аналіз та кількісна/якісна оцінка ризиків. Методології оцінки ризиків. Складові процесу управління ризиками відповідно до стандарту ISO/IEC 27005 (встановлення контексту, оцінювання ризиків, обробка ризиків, прийняття ризиків, комунікація та моніторинг). Сценарії обробки ризиків: зниження, прийняття, уникнення, передача.

РОЗДІЛ 3. Прикладна криптографія та стеганографія

Математичні та логічні основи криптографії. Основні поняття: алфавіт, відкритий текст, шифротекст, ключ, шифрування, дешифрування. Критерії надійності криптосистем: ідеальна стійкість, практична стійкість. Принцип Керкгоффса. Класифікація криптосистем (симетричні, асиметричні, гібридні). Класифікація атак криптографічного аналізу (атака на основі лише шифротексту, відомого відкритого тексту, обраного відкритого тексту тощо).

Симетрична криптографія: потокові та блокові шифри. Принципи функціонування блокових шифрів (перестановка, підстановка, мережа Фейстеля, SP-мережа). Режими роботи блокових шифрів (ECB, CBC, CFB, OFB, CTR). Огляд стандартів (AES, DES, 3DES, Калина). Асиметрична криптографія (криптосистеми з відкритим ключем). Односторонні функції з секретом. Алгоритми RSA, Діффі-Гелмана, ЕЦП на еліптичних кривих (ECDSA, ДСТУ 4145).

Криптографічні хеш-функції: призначення, властивості (стійкість до пошуку першого та другого прообразу, стійкість до колізій). Огляд алгоритмів хешування (MD5, SHA-1, SHA-2, SHA-3, Купина). Сутність, архітектура та математичні схеми генерації і перевірки цифрового підпису. Проблема розподілу та генерації ключів в ІКС. Концепція інфраструктури відкритих ключів (PKI): сертифікати ключів, центри сертифікації (CA).

Поняття комп'ютерної стеганографії. Відмінності між стеганографією та криптографією. Класифікація стеганографічних систем за типом контейнера (аудіо, відео, зображення, текстові файли, мережеві пакети). Стеганографічні алгоритми приховування даних (метод найменшого значущого біта — LSB, просторові та частотні методи). Поняття стегоаналізу.

РОЗДІЛ 4. Безпека операційних систем, комп'ютерних мереж та баз даних

Еталонні мережеві моделі OSI та TCP/IP. Аналіз вразливостей базових мережевих протоколів (IP, TCP, UDP, DNS, ARP). Концепція захисту комп'ютерних мереж. Міжмережеві екрани (Firewalls): класифікація (пакетні фільтри, шлюзи сеансового рівня, прикладні шлюзи, NGFW), архітектура

підключення, правила фільтрації трафіку. Технологія віртуальних приватних мереж (VPN): призначення, архітектура, базові тунелюючі та захищені протоколи (IPsec, SSL/TLS, OpenVPN, WireGuard, L2TP).

Поняття несанкціонованого доступу (НСД) до інформації в ОС. Комплекс засобів захисту від НСД. Процедури доступу: ідентифікація, автентифікація (фактори автентифікації: паролі, токени, біометрія), авторизація. Моделі розмежування доступу: дискреційна (DAC), мандатна (MAC), рольова (RBAC), атрибутивна (ABAC). Загальні механізми безпеки ОС (журналювання, аудит, керування пам'яттю, ізоляція процесів).

Визначення та класифікація шкідливого програмного забезпечення (ШПЗ) в ОС (віруси, хробаки, троянські програми, руткіти, шпигунське ПЗ, вимагачі-шифрувальники Ransomware). Механізми розповсюдження та функціонування ШПЗ в сучасних середовищах. Види антивірусного програмного забезпечення (сканери, монітори, ревізори диска, евристичні аналізатори, поведінкові блокувальники). Організація антивірусного захисту на підприємстві.

Архітектура захисту систем управління базами даних (СУБД). Загрози безпеці баз даних (ін'єкції коду, витік даних, несанкціоновані запити). Організація захисту та адміністрування БД: автентифікація користувачів, розмежування прав доступу на рівні таблиць і стовпців, шифрування даних «на льоту» (TDE), аудит операцій з БД. Захист вебдодатків: аналіз топ-загроз (OWASP Top 10), методи протидії атакам (SQL-ін'єкції, XSS, CSRF), застосування Web Application Firewalls (WAF).

РОЗДІЛ 5. Технічний та інженерний захист інформації

Поняття технічного захисту інформації (ТЗЗІ). Категорування та архітектура об'єктів інформаційної діяльності (ОІД). Поняття та вимоги до «режимного приміщення». Складові комплексів ТЗЗІ на об'єкті: системи контролю та управління доступом (СКУД), відеоспостереження, охоронно-пожежна сигналізація. Контроль фізичного доступу до серверного обладнання та комунікаційних вузлів.

Визначення та класифікація технічних каналів витоку інформації (ТКВІ). Акустичні, віброакустичні, оптичні канали витоку. ПЕМВН (побічні електромагнітні випромінювання та наводки): сутність явища, канали витоку через ланцюги живлення, заземлення та навколишні металеві конструкції. Засоби та методи захисту від ТКВІ: звукоізоляція, екранування приміщень та кабельних ліній, активне та пасивне зашумлення, використання сертифікованого захищеного обладнання.

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.