МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАВАТВЕРДЖУЮ
Голова Приймальної комісії
Державного університету
інформаційно - комунікаційних
технологій

Володимир ШУЛЬГА
«____» _____ 2026 р.

ПРОГРАМА
ДОДАТКОВОГО ВСТУПНОГО ВИПРОБУВАННЯ
ЗІ СПЕЦІАЛЬНОСТІ
F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

для здобуття третього (освітньо-наукового) рівня вищої освіти

Київ – 2026

Розробники:

Завідувач кафедри — Галина ГАЙДУР

Професор кафедри — Світлана КАЗМІРЧУК

Гарант:

Професор кафедри УКБЗІ — Віталій САВЧЕНКО

Завідувач кафедри СТКБ — Галина ГАЙДУР

Директор ННКБЗІ — Євгенія ІВАНЧЕНКО

Завідувач відділу аспірантури та докторантури Наукового центру — Юрій ПОКАНЄВИЧ

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Програма додаткового вступного випробування для здобуття освітньонаукового ступеня доктора філософії за спеціальністю F5 Кібербезпека та захист інформації розроблена на базі освітньо-кваліфікаційного рівня магістра або спеціаліста, здобутого за іншою спеціальністю.

Абітурієнти, які вступають на навчання для здобуття освітньо-наукового ступеня доктора філософії на основі освітньо-кваліфікаційного рівня магістра або спеціаліста, здобутого за іншою спеціальністю, попередньо складають додаткове вступне випробування.

Додаткове вступне випробування проводиться з метою перевірки якості загально-професійної й спеціальної підготовки потенційних аспірантів і дозволяє виявити й оцінити готовність вступника до вирішення професійних завдань та до науково-практичної діяльності.

Програма і форма додаткового вступного випробування є єдиною для всіх осіб, які не мають фахової освіти зі спеціальності F5 Кібербезпека та захист інформації.

1. Зміст дисциплін, які виносяться для кандидатів на навчання в аспірантурі за спеціальністю F5 Кібербезпека та захист інформації

Прикладна криптологія – математичні основи криптології; симетричні криптосистеми; асиметричні криптосистеми; методи автентифікації інформації; цифровий підпис; криптографічний аналіз.

Захист інформації в інформаційно-комунікаційних системах і мережах - комплекси засобів захисту інформаційно-комунікаційних систем; механізми та засоби захисту операційних систем; механізми та засоби захисту систем управління базами даних; механізми та засоби захисту від потенційно небезпечних програм; механізми та засоби захисту розподілених обчислювальних мереж і середовищ; механізми та засоби захисту програм та електронного документообігу; перспективні напрями розвитку комплексів засобів захисту.

Технічний захист інформації – технічний захист інформації, суб'єкти системи технічного захисту інформації, матеріально-технічна база системи технічного захисту інформації, оцінювання захищеності інформації, інформація з обмеженим доступом, комплекс технічного захисту інформації, об’єкт інформаційної діяльності, комплексна система захисту інформації.

Система управління інформаційною безпекою (СУІБ) – частина загальної системи управління, яка ґрунтується на підході, що враховує ризики інформаційної безпеки як бізнес-ризики, призначена для розроблення,

впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

2. Форма додаткового вступного випробування

Додаткове вступне випробування проводиться у формі тесту. Складання тесту відбувається протягом однієї академічної години.

3. Теми, які виносяться на випробування

Тема 1. Основні поняття криптології.

Тема 2. Основи побудови комплексів засобів захисту для інформаційнотелекомунікаційних систем та мереж.

Тема 3. Основи технічного захисту інформації.

Тема 4. Основи управління інформаційною безпекою.

4. Критерії оцінювання фахового вступного випробування

Програму додаткового вступного випробування (іспиту) зі спеціальності складено на підставі програм рівня вищої освіти магістра зі спеціальності F5 Кібербезпека та захист інформації у Державному університеті телекомунікацій.

Додаткове вступне випробування зі спеціальності проводиться у письмовій формі.

Додаткове вступне випробування складається з тестових завдань. Кожне запитання оцінюється в 200 балів (Таблиця 1) .

Таблиця 1

Порядок нарахування балів

Рівень знань	Бали	Критерії оцінювання знань
Початковий	100-107	Абітурієнт називає загрози інформаційній безпеці
	108-115	Абітурієнт називає класифікує загрози інформаційній безпеці; вибирає правильний варіант відповіді на рівні «так-ні»
	116-123	Абітурієнт двома-трьома словами має розповісти про об'єкти захисту інформації
Середній	124-132	Абітурієнт репродуктивно відтворює невелику частину навчального матеріалу, пояснюючи

		терміни у сфері управління інформаційною безпекою
	133-141	Абітурієнт з допомогою викладача відтворює основний зміст навчальної теми, визначає властивості інформації
	124-150	Абітурієнт самостійно відтворює фактичний матеріал теми, дає стислу характеристику системі управління інформаційною безпекою
Достатній	151-159	Абітурієнт послідовно і логічно відтворює навчальний матеріал теми, виявляє розуміння термінології, характеризує вразливості інформаційної системи (причини, наслідки, значення), відокремлює деякі ознаки явищ та процесів
	160-168	Абітурієнт володіє навчальним матеріалом і використовує знання за аналогією, дає правильні визначення, аналізую можливі загрози інформаційній безпеці, визначає причинно-наслідкові зв'язки між ними
	169-177	Абітурієнт оперує навчальним матеріалом, формує нескладні висновки, обґрунтовуючи їх конкретними фактами; самостійно встановлює причинно-наслідкові зв'язки між вразливостями та загрозами інформаційній безпеці
Високий	178-185	Абітурієнт використовує набуті знання для вирішення нової навчальної проблеми; виявляє розуміння системи управління інформаційною безпекою; робить аргументовані висновки, спираючись на широку джерельну базу
	168-193	Абітурієнт володіє глибокими знаннями, може вільно та аргументовано висловлювати власні судження щодо розробки основних документів з питань управління інформаційною безпекою
	194-200	Абітурієнт системно володіє навчальним матеріалом; виявляє особисту позицію щодо розробки системи управління інформаційною безпекою організації; уміє відокремити проблему і визначити шляхи її розв'язання; користується джерелами інформації, аналізує та узагальнює їх.

ЛІТЕРАТУРА

1. Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology. - April 16, 2018. – 55p. [Електронний ресурс] – Режим доступу: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
2. ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines/ ISO, IEC. - 2019. -76p.
3. Kutub Thakur Cybersecurity Fundamentals: A Real-World Perspective / Thakur Kutub, Pathan Al-Sakib Khan // CRC Press. – 2020. – 305p. ISBN 13:9780367476489
4. Leslie F. Sikos (Editor) AI in Cybersecurity. Springer. – 2018. – 215p.
5. Scott E. Enterprise Cybersecurity Study Guide/ Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, Abdul Aslam // Apress. 2018. – 737p. ISBN-13 (pbk): 978-1-4842-3257-6
6. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект / В.Л. Бурячок, В. Б.Толубко, С.В. Дорошенко: К.: ДУТ, 2015 - 298 с.
7. Гребенніков В. Комплексні системи захисту інформації. Проектування, впровадження, супровід / В. Гребенніков – «Издательские решения», 2018. – 249 с.
8. ДСТУ 33960-96. Захист інформації. Технічний захист інформації. Основні положення. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38911&cat_id=38836
9. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38911&cat_id=38836
10. Закон України «Про доступ до публічної інформації».
11. Закон України «Про електронні документи та електронний документообіг». https://zakon.rada.gov.ua/laws/ show /851-15
12. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
13. Закон України «Про інформацію» https://zakon.rada.gov.ua/laws/main/2657-12
14. Закон України «Про основні засади забезпечення кібербезпеки України». https://zakon.rada.gov.ua/laws/main/2163-19

ПОРЯДОК ПРОВЕДЕННЯ ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

Склад предметної комісії визначається додатковим наказом ректора Державного університету телекомунікацій «Про створення предметних комісій з приймання вступних іспитів до аспірантури». Робота комісії та порядок проведення вступного випробування регламентується Правилами прийому до аспірантури для здобуття наукового ступеня доктора філософії у Державному університеті телекомунікацій на навчальний рік.

Програму обговорено та схвалено на засіданні кафедри Систем та технологій кібербезпеки.

Протокол № 8/2 від «30» квітня 2025 р.

Гарант освітньої програми

доктор технічних наук, професор Віталій САВЧЕНКО