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

ЗАТВЕРДЖУЮ
Голова приймальної комісії
Ректор
_____ Олександр НАЗАРЕНКО
«11» 05 2026 р.

ПРОГРАМА

ВСТУПНОГО ІСПИТУ

для конкурсного відбору вступників

на третій (освітньо-науковий) рівень вищої освіти

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

ОДЕСА – 2026

1. Загальні положення

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

Вступний іспит із спеціальності складається в обсязі програми рівня вищої освіти магістра з відповідної спеціальності (п. 17 Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого постановою Кабінету Міністрів України від 23 березня 2016 р. № 261 (в редакції постанови КМУ від 08.04.2025 № 426)).

Перелік питань для підготовки до вступних іспитів зі спеціальності F5 Кібербезпека та захист інформації укладено на підставі таких програм навчальних дисциплін:

1. Управління доступом до інформаційних ресурсів.
2. Моніторинг та аудит інформаційно-комунікаційних систем.
3. Криптологія.
4. Комплексні системи безпеки.
5. Моніторинг та аудит інформаційно-комунікаційних систем.

Згідно з чинними «Правил прийому на навчання до Державного університету інтелектуальних технологій і зв'язку» у 2026 році для охочих продовжити навчання на третьому рівні вищої освіти передбачено обов'язкове складання вступного іспиту зі спеціальності. Нижче наведена структура даного вступного іспиту та навчальні матеріали, які рекомендовані для опрацювання в ході підготовки до нього. Вступний іспит складається з 2-х теоретичних питань.

1. Перелік питань складено відповідно до спеціальності 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 на навчання до Державного університету інтелектуальних технологій і зв'язку».

2. Вступнику пропонується вибрати екзаменаційний білет для вступного іспиту, який складається із 2 питань. Максимальна кількість отриманих балів – 200. Питання для складання питань взято з відповідної програми навчальної дисципліни відповідно до програми підготовки магістрів вище вказаної спеціальності.

3. Перелік питань, покладених в основу вступного іспиту та наведених нижче представлено у відповідному розділі на сайті Університету (www.suitt.edu.ua).

4. При оцінюванні знань вступника під час вступного іспиту згідно «Правил прийому на навчання до Державного університету інтелектуальних технологій і зв'язку» у 2026 році використовується 200-бальна система оцінки, за якою оцінка «відмінно» відповідає 175-200 балам, оцінка 4 «добре» – 135-173 балам, оцінка «задовільно» – 100-133 балам, при отриманні менш ніж 100 балів вступник отримує оцінку «незадовільно».

2. Перелік питань для підготовки до фахового іспиту

1. Опишіть стандарт AES: його структуру, режими роботи (ECB, CBC, CFB, OFB, CTR), переваги та недоліки порівняно з DES та 3DES. Поясніть, чому AES став домінуючим стандартом для симетричного шифрування у сучасних системах.

2. Порівняйте алгоритми RSA та ECC за такими критеріями: математичні основи, довжина ключів для еквівалентного рівня безпеки, швидкодія та ресурсомісткість. Наведіть приклади практичного застосування кожного алгоритму.

3. Поясніть вимоги до стійкої криптографічної хеш-функції (односпрямованість, стійкість до колізій, лавинний ефект). Опишіть алгоритм SHA-256 та його застосування для забезпечення цілісності даних. Чим відрізняється SHA-3 від попередніх версій (SHA-1, SHA-2)?

4. Опишіть принцип роботи цифрового підпису на базі асиметричного шифрування. Порівняйте алгоритми ECDSA та RSA-PSS за критеріями безпеки, швидкодії та розміру підпису. Наведіть приклади застосування цифрового підпису в реальних системах (наприклад, SSL/TLS, електронні документи).

5. Опишіть протокол TLS 1.3: етапи встановлення з'єднання (handshake), механізми автентифікації та шифрування. Поясніть, які вразливості попередніх версій TLS (наприклад, Heartbleed, POODLE) були усунені в TLS 1.3 та які загрози залишаються актуальними.

6. Методи передавання, що забезпечують енергетичну прихованість сигнальних конструкцій в каналі. Шумоподібні сигнали та методи їх формування. Умови забезпечення енергетичної та структурної прихованості.

7. Основні параметри завадостійких кодів. Класифікація завадостійких кодів. Загальний принцип декодування з виявленням та виправленням помилок. Оцінка здатності кодів виявляти та виправляти помилки.

8. Взаємозв'язок між енергетичною та частотною ефективністю системи зв'язку при забезпеченні прихованості передавання сигнальних конструкцій. Забезпечення енергетичної прихованості пояснити на основі теореми Шеннона про пропускну здатність.

9. Технології доступу на основі радіочастотної ідентифікації NFC та RFID. Фізичні принципи взаємодії та протоколи передавання даних. Загрози та шляхи їх вирішення.

10. Захист інформації в умовах радіоелектронної боротьби. Завадозахищеність систем передавання. Поняття завадостійкості та прихованості. Енергетична, структурна та інформаційна прихованість.

11. Теорема Шеннона для каналу без завад. Методи ефективного кодування джерел дискретних повідомлень. Коди Шеннона-Фано, Хаффмана та арифметичні коди.

12. Поняття моделі керування доступом. Дискреційне, мандатне та рольове керування доступом.

13. Кіберсередовище. Кібербезпека та її задачі. Технології, служби, послуги та механізми кібербезпеки. Архітектура кібербезпеки. Політика безпеки.

14. Перелік загроз кібербезпеці за Рекомендаціями МСЕ-Т X.800, X.805. Порядок оцінки загроз. Аналіз вразливостей. Описання та аналіз загроз.

15. Структура безпеки мережі з кінця в кінець за Рекомендацією МСЕ-Т X.805. Вісім послуг безпеки, що захищають від атак та основних загроз безпеки.

16. Рівні ієрархії мережного обладнання: рівень безпеки інфраструктури, рівень безпеки послуг, рівень безпеки застосувань.

17. Вимоги гарантії конфіденційності, цілісності й точності (вірності) передавання даних мережею. Застосування шифрування та хешування інформації для забезпечення безпеки. Методи захисту між точками доступу локальної мережі.

18. Модель забезпечення безпеки центру управління мережею. Єдина структура захисту мережі. Послуги безпеки у технології безпеки управління мережею.

19. Визначення контролю доступу. Технології захисту периметра: фільтрація змісту даних, міжмережеві фільтри, приховування адрес мережі, шлюзи рівнів застосувань, проксі-застосування.

20. Віртуальна приватна мережа (VPN): віддалений доступ з VPN, типи VPN, VPN рівня 2, 3, 4, тунелі як тракти передачі даних, послуги безпеки VPN.

21. Автентифікація: методи автентифікації, категорії систем автентифікації – одно-факторні, двох-факторні, три-факторні системи автентифікації; смарт-картки; сильна автентифікація, що ґрунтується на шифруванні.

22. Ідентифікація: категорії ідентифікації, рольовий принцип ідентифікації, ідентифікація на основі правил.

23. Сканування на наявність вірусів. Антивірусні технології. Метод сигнатур. Методи забезпечення цілісності системи.

24. Методи віддаленого доступу. Основні загрози віддалених користувачів. Технології та послуги віддаленого доступу: комутованого доступу до централізованого вузлу підприємства, мережі VPN віддаленого доступу, мережі VPN на основі IPSec. Механізми захисту віддаленого доступу.

25. Вразливості мереж WLAN. Інфраструктура мереж WLAN. Загрози мережам WLAN. Механізми та вимоги до безпеки бездротової точки доступу. Багаторівневий підхід до організації захисту бездротових мереж LAN.

3. Критерії оцінювання

Критерії оцінювання відповіді вступника за шкалою від 0 до 200 балів. Екзаменаційний білет з вступного іспиту містить 2 теоретичних питання. Кожне відповідь оцінюється в 100 балів. Можуть бути задані додаткові питання. Максимальна кількість отриманих балів – 200.

4. Структура екзаменаційного білета

Державний університет інтелектуальних технологій і зв'язку

ВСТУПНИЙ ІСПИТ
Третій (освітньо-науковий) рівень вищої освіти
Спеціальність F5 Кібербезпека та захист інформації

ЕКЗАМЕНАЦІЙНИЙ БІЛЕТ № ___1___

1. Методи передавання, що забезпечують енергетичну прихованість сигнальних конструкцій в каналі. Шумоподібні сигнали та методи їх формування. Умови забезпечення енергетичної та структурної прихованості.
2. Кіберсередовище. Кібербезпека та захист інформації та її задачі. Технології, служби, послуги та механізми кібербезпеки. Архітектура кібербезпеки. Політика безпеки.

Голова фахової атестаційної комісії _____ Володимир КОРЧИНСЬКИЙ

5. Рекомендована література

1. В.А. Лахно, Є.В. Василіу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова, Методи та засоби захисту інформації. Навчальний посібник. Київ: ЦП «Компринт». 2021. 444 с.
2. Тарнавський Ю. А. Технології захисту інформації. Київ: КПІ ім. Ігоря Сікорського. 2018. 162 с.
3. Peter Stavroulakis, Mark Stamp. Handbook of Information and Communication Security. Berlin: Springer-Verlag. 2010. 863 p.
4. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник. Київ: «МК-Прес». 2005. 432 с.
5. Гребенюк А.М., Л.В. Рибальченко. Основи управління інформаційною безпекою. Навчальний посібник. Дніпро: Дніпроп. держ. унт внутріш.справ. 2020.
6. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. Захист інформації в автоматизованих системах управління. Навчальний посібник. Житомир: Вид-во ЖДУ ім. І. Франка. 2015. 226 с.
7. Кавун С. В., В. Носов, О. В. Манжай. Інформаційна безпека. Навчальний посібник. Ч.2. Харків: Вид. ХНЕУ. 2008. 196 с.
8. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник / За ред. Кривуци В.Р. Київ: ООО "Д.В.К.". 2004. 508с.
9. Fernando Maymi. Shon Harris. All-in-One Exam Guide 9-th Edition. 2020. 1320 с.
10. Darril Gibson. SSCP System Security Certified Practitioner Exam Guide Second Edition. 2016. 554 с.

Голова предметної комісії _____ Володимир КОРЧИНСЬКИЙ