МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСТИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ЗАТВЕРДЖУЮ
В.о. ректора НТУ «ХПІ»
_____Євген СОКОЛ
« 27 квітня » 2026 р.

ПРОГРАМА
ВСТУПНОГО ІСПИТУ ІЗ СПЕЦІАЛЬНОСТІ

F5 «Кібербезпека та захист інформації»

для вступу на навчання до аспірантури
для здобуття ступеня доктора філософії
(третій рівень вищої освіти)

освітньо-наукова програма «Кібербезпека»

Харків 2026

ЗМІСТ

РОЗРОБНИКИ ПРОГРАМИ

Гарант освітньої-наукової програми:

Погасій Сергій Сергійович, доктор технічних наук, доцент, професор кафедри кібербезпеки – гарант програми третього рівня вищої освіти.

Члени робочої групи ОНП :

1. Євсеєв Сергій Петрович, доктор технічних наук, професор, завідувач кафедри кібербезпеки;
2. Мілевський Станіслав Валерійович, доктор технічних наук, доцент, професор кафедри кібербезпеки.
3. Король Ольга Григорівна, кандидат технічних наук, доцент, професор кафедри кібербезпеки.
4. Дунаєв Сергій Владиславович, студент групи А-3523.

АНОТАЦІЯ

Програма складена відповідно до вимог Міністерства освіти і науки України, закону України від 06 вересня 2014 року «Про вищу освіту», постанови КМ України від 23 березня 2016 року. № 261 «Про затвердження Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах)» та наказу Міністерства освіти і науки України від 26 лютого 2026 року № 373 «Порядок прийому на навчання для здобуття вищої освіти в 2026 році», Положення про підготовку здобувачів вищої освіти ступеня доктора філософії в аспірантурі, правил прийому до аспірантури Національного технічного університету «Харківський політехнічний інститут» наказ № 119 ОД від 30 березня 2026 року.

Вступний іспит із спеціальності F5 «Кібербезпека та захист інформації» є формою вступного випробування для осіб, які вступають на навчання до аспірантури Національного технічного університету «Харківський політехнічний інститут» з метою здобуття ступеня доктора філософії (PhD) за відповідною освітньо-науковою програмою (ОНП).

Метою вступного іспиту є визначення рівня сформованості загальних і спеціальних компетентностей вступника за спеціальністю F5 «Кібербезпека та захист інформації», оцінювання його відповідності рівню підготовки випускників другого (магістерського) рівня вищої освіти, а також встановлення достатності наявних знань і навичок для успішного навчання на третьому рівні вищої освіти та провадження науково-дослідної діяльності.

Для організації та проведення вступних випробувань створюються предметні комісії, склад яких затверджується наказом проректора з наукової роботи НТУ «ХПІ».

Результати вступного іспиту враховуються під час розрахунку конкурсного балу вступника відповідно до Правил прийому до аспірантури НТУ «ХПІ» (Додаток 6 до Правил прийому на навчання для здобуття вищої освіти у Національному технічному університеті «Харківський політехнічний інститут» у 2026 році).

Програма вступного іспиту сформована відповідно до обсягу та змісту освітньої програми другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації».

1 ПОРЯДОК ОРГАНІЗАЦІЇ ТА ПРОВЕДЕННЯ ВСТУПНОГО ІСПИТУ

Організація та проведення вступного іспиту зі спеціальності F5 «Кібербезпека та захист інформації» здійснюються відповідно до Положення про приймальну комісію НТУ «ХПІ», Положення про вступні випробування (співбесіду) Національного технічного університету «Харківський політехнічний інститут» та Правил прийому до аспірантури НТУ «ХПІ» (Додаток 6 до Правил прийому на навчання для здобуття вищої освіти у Національному технічному університеті «Харківський політехнічний інститут» у 2026 році).

Вступний іспит зі спеціальності F5 «Кібербезпека та захист інформації» **проводиться очно в укриттях**, за винятком випадків, передбачених пунктом 4.5 Правил прийому до аспірантури НТУ «ХПІ», у **формі усного іспиту**.

Усний вступний іспит із спеціальності до аспірантури проводиться предметною комісією за екзаменаційними білетами.

Екзаменаційні білети вступного іспиту зі спеціальності F5 «Кібербезпека та захист інформації» формуються відповідно до програми підготовки здобувачів вищої освіти рівня магістра за цією спеціальністю та затверджуються рішенням Приймальної комісії НТУ «ХПІ».

Вступний іспит проводиться відповідно до Розкладу вступних випробувань, який схвалюється на засіданні Приймальної комісії НТУ «ХПІ», затверджується ректором університету та оприлюднюється на офіційному вебсайті НТУ «ХПІ» не пізніше ніж за три дні до початку приймання документів. **Інформація про дату, час і місце проведення іспиту** відображається в особистому **електронному кабінеті вступника**.

Передекзаменаційна консультація проводиться дистанційно із обов’язковим записом з використанням засобів аудіо- та відеозапису відповідно до затвердженого розкладу членами предметної комісії.

Допуск вступників до аудиторії, у якій проводиться вступний іспит, здійснюється виключно після ідентифікації особи вступника. Для цього вступник зобов’язаний прибути до пункту тестування з документом, що посвідчує особу.

Сторонні особи без дозволу голови Приймальної комісії до приміщень, у яких проводяться вступні іспити, не допускаються.

Іспит передбачає вибір екзаменаційного білета (вступник обирає його власноруч із запропонованих), 20-25 хвилин на підготовку, усну відповідь на питання та оцінювання результатів.

Вступник усно відповідає на питання екзаменаційного білета. Члени предметної комісії мають право ставити уточнюючі запитання в межах екзаменаційного білету. Після завершення відповідей комісія обговорює результати та оголошує оцінку вступнику в день проведення іспиту.

Загальна тривалість проведення однієї сесії вступного іспиту не може перевищувати 3 години. У разі необхідності після перерви може бути проведено другу сесію іспиту.

Оцінювання результатів вступного іспиту здійснюється за шкалою від 100 до 200 балів, після чого результати вносяться до екзаменаційної відомості.

Після завершення вступного іспиту голова предметної комісії передає заповнені та підписані екзаменаційні відомості до Приймальної комісії НТУ «ХПІ».

Під час проведення іспиту **забороняється**:

– користуватися мобільними телефонами, іншими ґаджетами;

– використовувати паперові носії інформації (якщо інше не передбачено правилами).

У разі порушення зазначених вимог вступник відсторонюється від участі у вступних випробуваннях, про що складається відповідний Акт, у якому зазначаються причина та час відсторонення.

Вступні випробування із спеціальності фіксуються в обов'язковому порядку з використанням відеозапису не менше ніж з двох камер відеоспостереження. Відеозаписи розміщуються на офіційному сайті НТУ «ХПІ», а посилання на відповідні матеріали вносяться до ЄДЕБО протягом трьох робочих днів після оприлюднення результатів оцінювання вступників. Відеоматеріали зберігаються у відкритому доступі протягом одного року у вигляді активних інтернет-посилань.

У разі незгоди вступника з отриманою оцінкою (кількістю балів) він особисто подає заяву на апеляцію до приймальної комісії відділу аспірантури не пізніше наступного робочого дня після оголошення екзаменаційної оцінки. Заяви на апеляцію, подані з порушенням установлених термінів, до розгляду не приймаються. Порядок розгляду апеляцій визначено Правилами прийому до аспірантури НТУ «ХПІ».

Офіційні результати вступного іспиту оприлюднюються на сайті відділу аспірантури та в особистому електронному кабінеті вступника у терміни, визначені Правилами прийому до аспірантури НТУ «ХПІ».

Особи, які **без поважних причин**, визнаних такими за рішенням Приймальної комісії, не з’явилися на вступні випробування у визначений розкладом час, а також особи, результати яких є **нижчими за встановлений мінімальний бал**, до участі в конкурсному відборі **не допускаються**. Повторне складання вступних випробувань **не передбачається**.

2 ЗМІСТ ПРОГРАМИ

Тема 1 “СПЕЦІАЛЬНІ РОЗДІЛИ МАТЕМАТИКИ”

1.1 Основи теорії чисел. Поняття подільності чисел. Ділення із залишком. НСД двох чисел. Знаходження НСД двох чисел. Спільне найменше кратне. Прості числа. Великі прості числа. Методи побудови “великих” простих чисел. Псевдопрості числа, головні методи їх побудови. Функція Ейлера. Узагальнена функція Ейлера. Визначення та головні властивості.

1.2 Основи теорії груп, кілець та полів. Групи, головні поняття та визначення. Мультиплікативні групи. Підстановки. Групи підстановок. Підгрупи. Кільця, визначення та властивості. Кільце з одиницею. Ізоморфні кільця. Поля, визначення та властивості. Прості та поширені поля. Еліптичні криві, визначення та властивості.

1.3 Теорія ймовірності та математична статистика. Дискретноймовірнісний простір. Події та ймовірності, їх визначення та властивості. Приклади розподілів. Випадкові величини. Мат. очікування. Незалежні випадкові величини. Основні поняття мат. статистики. Закони розподілу ймовірностей. Біноміальний, показовий, рівномірний та нормальний розподіл. Перевірка статистичних гіпотез. Схема іспитів Бернуллі, критерій знаків для однієї вибірки. Критерій згоди Колмогорова, x^2 – квадрат Пірсона.

1.4 Спеціальний розділ теорії інформації. Умовна та безумовна ентропія. Умовна апостеріорна ентропія. Середня взаємна інформація. Блокові та неблокові коди. Норми, метрики та кодові відстані. Лінійні коди, згорткові коди, збиткові коди. Псевдовипадкові послідовності. Лінійні та нелінійні рекурентні послідовності, їх властивості.

1.5 Алгоритмічні основи криптографії. Основні методи обчислень в багатослівній арифметиці та оцінка їх складності. Методи побудування “великих” простих чисел та незвідних поліномів, складність та реалізація алгоритмів. Афінний та проективний базиси скалярного множення в групі точок еліптичних кривих. Методи побудування системних параметрів для криптографічних додатків на еліптичних кривих. Методи розв’язку дискретних логарифмічних рівнянь в групі точок еліптичних кривих та порівняльна оцінка їх складності.

Рекомендована література до теми 1:

1. Кузнецов О.О., Євсеєв С.П., Кавун С.В., та Король О.Г. Сигнали і коди. Алгебраїчні методи синтезу. Монографія. Харків, Україна: Вид. ХНЕУ, 2009.

2. Кузнецов О.О., Євсеєв С.П., та Кавун С.В. Захист інформації та економічнабезпека підприємства. Монографія. Харків, Україна: Вид. ХНЕУ, 2009.

3. Теорія інформації: підручник для слухачів, курсантів та студентів вищих навчальних закладів / І.В. Рубан, С.І. Хмелевський, О.В. Сєвєрінов та ін. – Харків: ХНУПС, 2018. – 276 с.

4. Кузнецов О.О., Євсеєв С.П., Король О.Г. Захист інформації в ІС. Харків: Вид. ХНЕУ, 2011. –510 с.

Тема 2 “МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ. КРИПТОГРАФІЧНІ СИСТЕМИ”

2.1 Основи теорії захисту інформації. Моделі загроз та порушника. Фактори уразливості та канали витоку інформації, шляхи несанкціонованого доступу. Концепція захищеної комп'ютерної системи (мережі). Політики безпеки інформації та їх впровадження.

2.1.2. Основні функції криптографічних систем. Криптографія та криптографічний аналіз. Класифікація криптографічних систем по стійкості. Теоретично недешифруємі системи й умови їх реалізації. Обчислювальностійкі та доказово стійкі системи й умови їхньої реалізації. Інформаційні характеристики джерел повідомлень, криптограм і ключів. Класифікація шифрів. Симетричні та несиметричні алгоритми шифрування. Блокові та потокові алгоритми шифрування, та їх властивості. Генератори псевдовипадкових послідовностей. Несиметричні алгоритми шифрування та їх властивості. Умови реалізації та галузі застосування систем шифрування. Автентифікація. Погрози порушення автентичності. Модель взаємної довіри, взаємної недовіри та взаємного захисту. Методи автентифікації в потокових системах шифрування, оцінка їх ефективності. Цифровий підпис, оцінка ефективності електронних підписів. Класифікація методів криптографічного аналізу та умови здійснення.

2.2 Криптографічні системи. Класифікація та характеристика симетричних криптографічних систем. Основні вимоги та склад симетричних криптографічних систем. Основні принципи та режими симетричного

шифрування. Класифікація та характеристика несиметричних криптографічних систем. Основні протоколи встановлення таємниці та ключів. Аналіз рівнів безпеки. Алгоритми цифрового підпису та порівняльний аналіз їх властивостей. Алгоритм цифрового підпису в групі точок еліптичних кривих. Криптографічна стійкість та складність перетворень. Класифікація, суть та порівняльний аналіз стандартних алгоритмів та засобів гешування.

2.3 Проектування та використання систем і засобів захисту інформації. Нормативна база, яка визначає процеси розробки та створення комплексних систем захисту інформації. Вимоги до перспективних симетричних криптографічних систем. Стандарти симетричного блокового шифрування. Стійкість симетричних блокових криптосистем. Методика оцінки та порівняльного аналізу. Розробка програмних і апаратних засобів криптографічного захисту інформації. Основні вимоги. Принципи програмної та апаратної реалізації. Інфраструктури відкритих ключів, призначення, вимоги та принципи функціонування. Комплексні системи захисту центрів сертифікації ключів, вимоги до них, порядок створення і застосування.

2.4 Технічний захист інформації. Технічні канали витоку інформації. Радіоелектронні, вібро-акустичні та візуально-оптичні канали витоку інформації. Канали витоку інформації і їх структура та загальна характеристика. Сигнали як носії інформації. Способи і засоби отримання інформації по вібро-акустичному каналу. Лазерні системи акустичної розвідки (ЛСАР), їх структурна схема і принцип дії. Методи та засоби захисту мовної інформації. Засоби протидії підслуховуванню: інформаційне приховування та енергетичне приховування. Класифікація технічних засобів закриття. Аналогове скремблювання: частотна інверсія, часова і частотна перестановка, цифрове шифрування. Методи і радіотехнічні прилади запобігання витоку інформації за допомогою закладних приладів. Демаскуючі признаки закладних приладів. Апаратно-програмні комплекси викриття, ідентифікації та локалізації радіоакустичних закладних пристроїв. Основні характеристики і властивості радіоелектронного каналу витоку інформації. Джерела електромагнітних сигналів як носіїв інформації, їх властивості та особливості поширення. Побічні електромагнітні випромінювання технічних засобів. Екранування та заземлення технічних засобів передачі інформації. Вимоги та методи забезпечення захисту інформації від витоку по технічним каналам в АС 1 та АС2. Вимоги нормативних

документів та захист електронних засобів інформаційнотелекомунікаційних систем від зовнішнього впливу.

2.5 Системи керування захистом інформації. Архітектура системи безпеки операційних систем (ОС). Диспетчер облікових записів (ДОЗ). Паролі, відновлення паролів. Захист файлів і компоненти (NTFS). Права доступу. Дозволи NTFS. Захист реєстру. Інформація про безпеку реєстру. Захист від локального та віддаленого доступу. Аудит реєстру.

Рекомендована література до теми 2:

1. Євсеєв С.П. Кібербезпека: основи кодування та криптографії: навчальний посібник / С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. "Новий Світ-2000", 2024. – 658 с.

2. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія: Теорія. Практика. Застосування: Підручник для вищих навчальних закладів. – Харків: Видавництво "Форт", 2013. – 880 с.

3. Горбенко Ю.І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія. - Частина 1: Методи побудування та аналізу, стандартизація та застосування криптографічних систем / За зат. ред. д.т.н., професора І.Д. Горбенка. – Харків : Видавництво "Форт", 2015. – 960 с.

4. Кузнецов О.О., Євсеєв С.П., Король О.Г. Захист інформації в ІС. Харків: Вид. ХНЕУ, 2011. –510 с.

5. Євсеєв С.П. Кібербезпека: сучасні технології захисту. / Євсеєв С.П, Остапов С.Е., Король О.Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: "Новий Світ- 2000", 2019. – 678.

6. Євсеєв С.П., Йохов О.Ю., та Король О.Г. Гешування даних в інформаційних системах. Монографія. Харків, Україна: Вид. ХНЕУ, 2013.

7. Задірака В., Олексик О. Комп'ютерна криптологія. – Київ, 2002. – 502 с.

8. Тимошенко Л.П. Схемотехніка пристроїв технічного захисту інформації: навч. посіб. [Ч.1] / Л.П. Тимошенко; за ред. В.М. Карташова. – Харків: СМІТ, 2012. – 340 с.

Тема 3 "ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ І МЕРЕЖАХ"

3.1 Стандартизація та сертифікація систем і засобів захисту інформації. Основні положення безпеки інформації. Сутність вимог основних стандартів по забезпеченню безпеки інформації. Призначення та ціль розробки стандарту.

Етапи розробки стандартів. Порядок сертифікації засобів захисту. Основні вимоги стандартів по управлінню ключами. Функції центрів управління та сертифікації ключів. Стандарти ЦП та їх застосування. Стандартні криптографічні протоколи розподілу таємниці. Властивості та реалізація. Стандарти гешування, властивості та застосування.

3.2 Захист інформації в комп'ютерних системах і мережах. Методи та засоби генерації та розподілу системних параметрів і ключів. Захист інформації із використанням цифрового підпису та коду автентифікації. Криптографічні методи та засоби захисту інформації в локальних та глобальних мережах. Криптографічні протоколи встановлення ключів та оцінка їх якості. Принципи забезпечення основних послуг – цілісності, конфіденційності, доступності й автентичності в локальних та глобальних мережах. Принципи побудування та функціонування інфраструктур з відкритими ключами. Порядок надання послуг з ЦП. Протоколи шифрування на мережевому рівні та їх основні властивості і характеристики.

Рекомендована література до теми 3:

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія: Теорія. Практика. Застосування: Підручник для вищих навчальних закладів. – Харків: Видавництво "Форт", 2013. – 880 с.

2. Горбенко Ю.І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія. - Частина 1: Методи побудування та аналізу, стандартизація та застосування криптографічних систем / За зат. ред. д.т.н., професора І.Д. Горбенка. – Харків : Видавництво "Форт", 2015. – 960 с.

3. Євсеєв С.П. Кібербезпека: сучасні технології захисту. / Євсеєв С.П, Остапов С.Е., Король О.Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: "Новий Світ- 2000", 2019. – 678.

4. Євсеєв С.П., Йохов О.Ю., та Король О.Г. Гешування даних в інформаційних системах. Монографія. Харків, Україна: Вид. ХНЕУ, 2013.

5. Задірака В., Олексик О. Комп'ютерна криптологія. – Київ, 2002. – 502 с.

6. Сенів М.М. Безпека програм та даних: навч. посіб. / М.М. Сенів, В.С. Яковина; М-во освіти і науки України, Нац. ун-т "Львівська політехніка". – Львів: Вид-во Львівської політехніки, 2015. – 256 с.

7. ISO/IEC 11700-1, 2, 3. Information technology – Security techniques – Key management.

8. ISO/IEC 15946-1, 2, 3. Information technology – Security techniques – Cryptographic techniques based on elliptic curves.

9. ISO/IEC 9798-1, 2, 3, 4, 5. IT Security techniques – Entity authentication.

10. ISO/IEC 9797-1, 2, 3. Information technology – Security techniques – Message Authentication Codes (MACs).

11. ISO/IEC 13888-1.2.3. Information security – Non-repudiation.

12. ISO/IEC 14888- 1.2.3. IT Security techniques – Digital signatures with appendix.

13. ISO/IEC 9594-8. Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks.

14. ISO/IEC 18031. Information technology – Security techniques – Random bit generation.

15. ISO/IEC 18032. Information technology – Security techniques – Prime number generation.

16. ISO/IEC 18033 – 1, 2, 3, 4. Information technology – Security techniques – Encryption algorithms.

17. Edited by Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.

18. Hryshchuk R., Construction methodology of information security system of banking information in automated banking systems : monograph / R. Hryshchuk, S. Yevseiev, A.Shmatko //– Vienna.: Premier Publishing s. r. o., 2018. – 284 p.

Тема 4 “УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ”

4.1. Системи аналізу вразливостей та принципи етичного хакінгу.

4.2. Методи виявлення та аналізу шкідливого програмного забезпечення.

4.3. Стандарти, протоколи та процедури, що відповідають за перевірку та управління безпекою продукту.

4.4. Загальні вимоги та підходи до розробки моделі загроз програмного забезпечення; патерни безпеки: керування ідентифікацією, автентифікація, моделі доступу, керування сесіями та ін.

4.5. Аспекти адміністрування, аудит та безпека інформаційних служб Internet. 4.6. Методи проведення цифрової криміналістики.

Рекомендована література до теми 4:

1. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.
2. Богуш В.М. Інформаційна безпека держави: [навч. посіб.] / В.М. Богуш, О.К. Юдін. – К.: МК-Прес, 2005. – 432 с.
3. Бурячок В.Л., Грищук Р.В., та Хорошко В.О., під заг. ред. проф. В. О. Хорошка, “Політика інформаційної безпеки”, ПВП “Задруга”,. 2014.
4. Грищук Р.В., та Даник Ю.Г. Основи кібернетичної безпеки: Монографія /; за заг. ред. Ю. Г. Данника. Житомир: ЖНАЕУ, 2016.
5. ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій.
6. ДСТУ ISO/IEC TR 13335-2:2003 Інформаційні технології. Частина 2. Настанови з керування безпекою інформаційних технологій
7. ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій.
8. ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4. Вибирання засобів захисту
9. ДСТУ ISO/IEC TR 13335-5:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 5. Настанова з управління мережною безпекою
10. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD).
11. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Інформаційнітехнології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD)
12. Юдін О.К. “Інформаційна безпека. Нормативно-правове забезпечення”, К. : НАУ, 2011.
13. ISO/IEC 15408-1:1999 – Information technology – Security techniques – Evaluation criteria for IT security – Part1: Introduction and general model.
14. ISO/IEC 15408-2:2005– Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements.

15. ISO/IEC 15408-3:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements

16. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements

17. ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls.

18. ISO/IEC 27006:2015 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems

19. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity

20. ISO/IEC 27031:2011 Information Technology – Security Techniques – Guidelines for Information and Communication Technology Readiness for Business Continuity.

Тема 5 "МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ СИСТЕМ БЕЗПЕКИ"

5.1 Принципи побудови математичних моделей. Основні види моделювання. Формальні методи побудови моделей. Формальні методи побудови моделей: кібернетичний підхід, системна динаміка, теоретичномножинний підхід. Ідентифікація параметрів математичної моделі. Адекватність, чутливість, непротирічність моделі.

5.2 Математичні основи моделей безпеки. Поняття автомата. Елементи теорії графів. Алгоритмічно розв'язні і алгоритмічно нерозв'язні проблеми. Модель решітки. Основні види формальних моделей безпеки. Проблема адекватності реалізації моделі безпеки в реальному комп'ютерній системі.

5.3 Моделі з дискреційним управлінням доступу. Модель матриці доступив Харрісона-Руззо-Ульмана. Опис моделі. Аналіз безпеки систем ХРУ Модель типизированной матриці доступив. Модель поширення прав доступу Take-Grant. Основні положення класичної моделі Take-Grant. Розширена модель Take-Grant. Подання систем Take-Grant системами ХРУ. Дискреційні ДП-моделі. Базова ДП-модель. ДП-модель без кооперації довірених і недовірених суб'єктів.

5.4 Моделі ізольованого програмного середовища. Суб'єктноорієнтована модель ізольованого програмного середовища. Коректність суб'єктів в ДП-моделях КС з дискреційним управлінням доступом. ДПмодель з функціонально асоційованими з суб'єктами сутностями. ДП-модель для політики безпечного

адміністрування. ДП-модель для політики абсолютного поділу адміністративних і призначених для користувача повноважень. ДП-модель з функціонально або параметрично асоційованими з суб'єктами сутностями. Застосування ФАС ДП-моделі для аналізу безпеки веб-систем.

5.5 Моделі з мандатним управлінням доступу. Модель Бела-ЛаПадули. Модель мандатної політики цілісності інформації Віба. Модель систем військових сполучень. Загальні положення та основні поняття. Неформальне опис моделі СВС. Формальний опис моделі СВС. Мандатна ДП-модель.

5.6 Моделі безпеки інформаційних потоків. Автоматна модель безпеки інформаційних потоків. Програмна модель контролю інформаційних потоків. Імовірнісна модель безпеки інформаційних потоків. ДП-моделі безпеки інформаційних потоків за часом. ДП-модель з блокуючими доступами довірених суб'єктів. Мандатна ДП-модель з блокуючими доступами довірених суб'єктів. Мандатна ДП-модель з ототожненням породжених суб'єктів.

5.7 Моделі рольового управління доступом. Базова модель рольового управління доступом. Модель адміністрування рольового управління доступом. Основні положення. Адміністрування множин авторизованих ролей користувачів. Адміністрування множин прав доступу, якими володіють ролі. Адміністрування ієрархії ролей. Модель мандатної рольового управління доступом. Захист від загрози конфіденційності інформації. Захист від загроз конфіденційності та цілісності інформації. Мандатна сутніснорольова ДП-модель управління доступом та інформаційними потоками в операційних системах сімейства Linux.

Рекомендована література до теми 5:

1. Грищук Р.В., та Даник Ю.Г. Основи кібернетичної безпеки: Монографія /; за заг. ред. Ю. Г. Данника. Житомир: ЖНАЕУ, 2016.
2. Кібербезпека мереж наступного покоління : навч. посіб. / О. О. Вараксін, Є. В. Василіу, С. М. Горохов и др. ; за ред. В. Г Кононовича ; М-во освіти і науки України, Одеська нац. академія зв'язку ім. О. С. Попова. – Одеса : ОНАЗ ім. О. С. Попова, 2013. – 240 с.
3. Математичне моделювання телекомунікаційних систем та мереж: навчальний посібник [Текст] / Є.М. Чернихівський. – Львів: Видавництво Львівської політехніки, 2011. – 272 с

4. Махней О. В. Математичне моделювання : навчальний посібник / О. В.Махней. – Івано-Франківськ : Супрун В. П., 2015. – 372 с.

5. Олейніков А.М. Методи та засоби захисту інформації. Навчальнийпосібник для студентів вищих навчальних закладів // Харків: НТМТ, 2014. – 298 с.

Тема 6 "ЗАХИСТ ІНФОРМАЦІЇ В ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМАХ"

6.1 Централізовані та децентралізовані мережі. Принципи формування систем безпеки. Технологія блокчейн. Технології майнінга. Моделі знаходження консенсусу. Криптографічні протоколи гешування.

6.2. Основи смарт-контрактів. Принципи формування смарт-контрактів. Принципи токенізації. Принципи формування та особливості Bitcoin Script. Принципи формування протоколу Bitshares. Формування SmartCoins. Облікова система Atomic Swap. Принципи створення Stablecoin. Проведення транзакцій та формати ключів у BitCoin.

Рекомендована література до теми 6:

1. Кравченко П., Скрябін Б. Блокчейн та децентралізовані системи. Ч. 1. Харків: Промарт, 2018. – 400 с.

2. Кравченко П. Блокчейн і децентралізовані системи. Ч. 2 – Харків: ПРОМАРТ, 2019. – 452 с.

3. Кравченко П. Блокчейн і децентралізовані системи. Ч. 3 – Харків: ПРОМАРТ, 2020. – 306 с.

4. Горбенко Ю.І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія. - Частина 1: Методи побудування та аналізу, стандартизація та застосування криптографічних систем / За зат. ред. д.т.н., професора І.Д. Горбенка. – Харків : Видавництво "Форт", 2015. – 960 с.

5. Євсеєв С.П. Кібербезпека: сучасні технології захисту. / Євсеєв С.П, Остапов С.Е., Король О.Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: "Новий Світ- 2000", 2019. – 678.

6. Wanjala Peter. A Beginner's Journey to Ethereum's Smart Contracts. [Peter Namisiko Wanjala], 2018. – 189 p.

7. Vaneetvelde Kenny. Ethereum Projects for Beginners (code).Packt Publishing,2018. – 92 p.

8. Skvorc Bruno. Learn Ethereum: The Collection. SitePoint, 2018. – 447 p.

3 ПЕРЕЛІК ЗАПИТАНЬ ВСТУПНОГО ІСПИТУ

1. Знаходження НСД двох чисел. Методи побудови “великих” простих чисел.
2. Кільця, визначення та властивості.
3. Поля, визначення та властивості. Прості та поширені поля. Критерій згоди Колмогорова, x^2 – квадрат Пірсона.
4. Еліптичні криві, визначення та властивості. Методи побудування системних параметрів для криптографічних додатків на еліптичних кривих.
5. Дискретно-ймовірнісний простір. Події та ймовірності, їх визначення та властивості.
6. Основні методи обчислень в багатослівній арифметиці та оцінка їх складності.
7. Моделі загроз та порушника. Фактори уразливості та канали витоку інформації, шляхи несанкціонованого доступу.
8. Класифікація шифрів. Класифікація криптографічних систем по стійкості.
9. Симетричні та несиметричні алгоритми шифрування. Блокові та потокові алгоритми шифрування, та їх властивості.
10. Несиметричні алгоритми шифрування та їх властивості.
11. Методи автентифікації, оцінка їх ефективності. Стандарти гешування, властивості та застосування.
12. Цифровий підпис, оцінка ефективності електронних підписів. Стандарти ЦП та їх застосування.
13. Основні принципи та режими симетричного шифрування. Класифікація та характеристика несиметричних криптографічних систем. 14. Алгоритм цифрового підпису в групі точок еліптичних кривих.
15. Криптографічна стійкість та складність перетворень. Класифікація, суть та порівняльний аналіз стандартних алгоритмів та засобів гешування.
16. Вимоги до перспективних симетричних криптографічних систем
17. Стандарти симетричного блокового шифрування. Стандартні криптографічні протоколи розподілу таємниці.
18. Інфраструктури відкритих ключів, призначення, вимоги та принципи функціонування.
19. Комплексні системи захисту центрів сертифікації ключів, вимоги до них, порядок створення і застосування.

20. Технічні канали витоку інформації.
21. Канали витоку інформації і їх структура та загальна характеристика.
22. Лазерні системи акустичної розвідки (ЛСАР), їх структурна схема і принцип дії.
23. Методи та засоби захисту мовної інформації.
24. Класифікація технічних засобів закриття.
25. Методи і радіотехнічні прилади запобігання витоку інформації за допомогою закладних приладів.
26. Основні характеристики і властивості радіоелектронного каналу витоку інформації.
27. Архітектура системи безпеки операційних систем.
28. Сутність вимог основних стандартів по забезпеченню безпеки інформації.
29. Методи та засоби генерації та розподілу системних параметрів і ключів.
30. Захист інформації із використанням цифрового підпису та коду автентифікації.
31. Криптографічні протоколи встановлення ключів та оцінка їх якості.
32. Принципи побудування та функціонування інфраструктур з відкритими ключами.
33. Протоколи шифрування на мережевому рівні та їх основні властивості і характеристики.
34. Системи аналізу вразливостей та принципи етичного хакінгу.
35. Методи виявлення та аналізу шкідливого програмного забезпечення.
36. Стандарти, протоколи та процедури, що відповідають за перевірку та управління безпекою продукту.
37. Загальні вимоги та підходи до розробки моделі загроз програмного забезпечення.
38. Аспекти адміністрування, аудит та безпека інформаційних служб Internet.
39. Методи проведення цифрової криміналістики.
40. Формальні методи побудови моделей: кібернетичний підхід, системна динаміка, теоретично-множинний підхід.
41. Математичні основи моделей безпеки. Поняття автомата. Елементи теорії графів.
42. Моделі з дискреційним управлінням доступу.
43. Моделі ізольованого програмного середовища.

44. Моделі з мандатним управлінням доступу. Модель Бела-ЛаПадули.
45. Моделі безпеки інформаційних потоків. Автоматна модель безпеки інформаційних потоків.
46. Мандатна ДП-модель з блокуючими доступами довірених суб'єктів.
47. Мандатна ДП-модель з ототожненням породжених суб'єктів.
48. Модель адміністрування рольового управління доступом. Основні положення.
49. Модель мандатної рольового управління доступом.
50. Мандатна сутнісно-рольова ДП-модель управління доступом та інформаційними потоками в операційних системах сімейства Linux.
51. Централізовані та децентралізовані мережі. Принципи формування систем безпеки.
52. Технологія блокчейн. Технології майнінга. Моделі знаходження консенсусу.
53. Базова модель рольового управління доступом.
54. Принципи майнінга та знаходження консенсусу. Криптографічні протоколи гешування.
55. Основи смарт-контрактів. Принципи формування смарт-контрактів.
56. Принципи токенізації. Принципи формування та особливості Bitcoin Script.
57. Принципи формування протоколу Bitshares. Формування SmartCoins.
58. Облікова система Atomic Swap.
59. Принципи створення Stablecoin.
60. Проведення транзакцій та формати ключів у BitCoin.
61. Мережа Фейстеля. Її архітектура та функціонування.
62. Модульна арифметика у криптографії. Порівняння за модулем. Основні операції у модульній арифметиці.
63. Зведення в ступінь у модульній арифметиці. Мала теорема Ферма.
64. Поняття про односторонні функції. Приклади. Використання в несиметричних криптосистемах.
65. Вимоги до криптографічних геш-функцій.

4 СТРУКТУРА ЕКЗАМЕНАЦІЙНОГО БІЛЕТУ ТА КРИТЕРІЇ ОЦІНКИ ВСТУПНОГО ІСПИТУ

Екзаменаційний білет складається з трьох питань з однаковим рівнем складності за вищезазначеними темами з переліку наведеного у розділі 3.

Нижче наведено структуру екзаменаційного білета.

ЗРАЗОК ЕКЗАМЕНАЦІЙНОГО БІЛЕТУ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”

Вступний іспит зі спеціальності F5 – “Кібербезпека та захист інформації”

Білет № 3

1. Модульна арифметика у криптографії. Порівняння за модулем. Основні операції у модульній арифметиці.

2. Симетричні та несиметричні алгоритми шифрування. Блокові та потокові алгоритми шифрування, та їх властивості.

3. Моделі загроз та порушника. Фактори уразливості та канали витоку інформації, шляхи несанкціонованого доступу.

Предметна комісія колегіально оцінює відповідь вступника на кожне питання білету за 200-бальною шкалою (максимальна кількість – 200 балів, мінімальна кількість – 100 балів). У разі відсутності відповіді або надання неправильної відповіді на питання результат оцінювання цього питання визначається як «незадовільно» та дорівнює нулю балів. При оцінці знань за основу слід брати повноту і правильність відповіді.

Основні критерії оцінювання відповіді вступника на питання наведено у таблиці 1.

Загальна оцінка за вступний іспит визначається як середнє арифметичне балів, отриманих вступником за всі питання екзаменаційного білета (якщо середній бал має дробове значення, його округлюють у бік збільшення до цілого числа). Предметна комісія встановлює загальний результат за шкалою 100–200 балів або ухвалює рішення про негативний результат вступного випробування («незадовільно»).

Вступники, які за результатами вступного іспиту отримали менше 100 балів, вважаються такими, що не склали вступне випробування, та не допускаються до подальшої участі в конкурсному відборі.

Таблиця 1 – Критерії оцінювання кожного окремого питання білету

Оцінка за 100-200 бальною шкалою	Характеристика відповіі
165-200	Вступник: - досконало володіє теоретичним навчальним матеріалом для ґрунтовної відповіді на поставлені питання; - глибоко і повно оволодів понятійним апаратом, вільно та аргументовано висловлює власні думки; - демонструє культуру спеціальної мови і використовує сучасну технологічну термінологію, цілісно, системно, у логічній послідовності дає відповідь на поставлені запитання; - творчо використовує знання для розв'язання практичних завдань.
135-164	Вступник: - володіє теоретичним навчальним матеріалом для відповіді на поставлені питання; - здатний застосовувати вивчений матеріал на рівні стандартних ситуацій; наводити окремі власні приклади на підтвердження певних тверджень; - грамотно викладає відповідь, але зміст і форма відповіді мають окремі неточності, припускає 2-3 непринципові помилки, які вміє виправити, добираючи при цьому аргументи для підтвердження певних дій.
100-134	Вступник: - частково володіє навчальним матеріалом, здатний логічно відтворити значну його частину; - виявляє знання і розуміння основних положень навчального матеріалу, але викладає його неповно, непослідовно, припускається неточностей у визначеннях понять, у застосуванні знань для вирішення практичних задач, не вміє доказово обґрунтувати свої думки; - завдання виконує, але припускає методологічні помилки.
Незадовільно	Вступник: - має розрізнені безсистемні знання; - володіє матеріалом на елементарному рівні засвоєння, викладає його безладно, уривчастими реченнями; - припускає помилки у визначенні термінів, які приводять до викривлення їх змісту; - припускає принципові помилки при вирішенні практичних завдань; - не відповідає (або дає неповні, неправильні відповіді) на основні та додаткові питання.

Гарант ОНП зі спеціальності
F5 «Кібербезпека та захист інформації»_____Сергій ПОГАСІЙ

Затверджено на засіданні кафедри “Кібербезпека” від «23» березня 2026 р., протокол № 12.

Завідувач кафедри “Кібербезпека” _____ Сергій ЄВСЕЄВ

Затверджено на засіданні інституту ННІ КНІТ № КНІТ-4 від 21.04.2026

Директор ННІ КНІТ _____ Михайло ГОДЛЕВСЬКИЙ

Завідувач аспірантури НТУ «ХПІ» _____ Віктор ШАЙДА

Відповідальний секретар Центральної
приймальної комісії НТУ «ХПІ» _____ Сергій ВИРОВЕЦЬ