Робоча програма дисципліни «Фахова англійська мова»

СПЕЦІАЛЬНІСТЬ 123 · КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

БАКАЛАВР

240

Годин

Загальний обсяг дисципліни

8

Кредити ЄКТС

Відповідно до стандарту

8

Модулі

Змістовних блоки курсу

Загальна інформація про дисципліну

Ідентифікація

Назва: Фахова англійська мова

Спеціальність: 123 Комп'ютерна інженерія

Освітня програма: Організація захисту інформації в інформаційно-комунікаційних системах

Ступінь: Бакалавр

Обсяг: 240 годин / 8 кредитів ЄКТС

Модулів: 8 змістовних блоків

Практичні: 120 год. | **Самостійна робота:** 120 год.

Призначення дисципліни

Дисципліна «Фахова англійська мова» формує у студентів комунікативну компетентність у галузі інформаційної безпеки та захисту інформації в інформаційно-комунікаційних системах. Курс розвиває навички читання, аналізу та продукування англомовних фахових текстів за тематикою кібербезпеки, криптографії, мережевого захисту та управління інформаційними ризиками.

Дисципліна є обов'язковою для підготовки бакалаврів зі спеціальності 123 «Комп'ютерна інженерія» освітньої програми «Організація захисту інформації в інформаційно-комунікаційних системах» та забезпечує формування загальних і фахових компетентностей, передбачених освітньо-професійною програмою.

Загальні компетентності

Іншомовна комунікація

Здатність до усної та письмової англомовної комунікації у фаховому середовищі: читання технічної документації, написання звітів, електронного листування та участь у міжнародних конференціях з кібербезпеки.

Аналітичне мислення

Здатність аналізувати та синтезувати англомовні фахові джерела з питань захисту інформації: порівняння стандартів, оцінка технічних рішень, формування обґрунтованих висновків.

Самоорганізація

Уміння самостійно опрацьовувати англомовні технічні тексти, планувати підготовку рефератів і презентацій, дотримуватися дедлайнів під час роботи з фаховою іноземномовною літературою.

Командна робота

Готовність до групової роботи над спільними англомовними проєктами, розподілу обов'язків під час підготовки кейсів з інформаційної безпеки та презентації результатів дослідження.

Студент повинен вміти: читати та розуміти англомовну технічну документацію зі спеціальності; продукувати фахові тексти англійською мовою; здійснювати усне спілкування в межах фахової тематики; самостійно поповнювати словниковий запас у галузі кібербезпеки та захисту інформації.

Фахові компетентності

Англомовна фахова лексика

Знання та коректне застосування термінологічного апарату з інформаційної безпеки, кіберзахисту та комп'ютерної інженерії англійською мовою: криптографія, аутентифікація, вразливість, брандмауер, шифрування, мережевий захист.

Читання технічної документації

Здатність читати, розуміти та реферувати англомовні стандарти (ISO/IEC 27001, NIST, GDPR), технічні специфікації, наукові статті та звіти з кібербезпеки. Виявлення ключових понять та критичний аналіз джерел.

Фахове письмо та презентація

Уміння оформлювати технічні звіти, анотації, есе та аналітичні записки англійською мовою з питань захисту інформаційно-комунікаційних систем; підготовка і проведення усних презентацій фахового змісту.

Міжнародні стандарти та нормативні документи

Орієнтування в англомовній нормативно-правовій базі та міжнародних стандартах у сфері захисту інформації; використання англомовних фахових ресурсів для формування обґрунтованих висновків у галузі ІКС.

Результати навчання

01

Фахова англомовна комунікація

Здійснювати усне та письмове спілкування англійською мовою в межах фахової тематики: кіберзахист, мережева безпека, захист інформації в ІКС, криптографія, управління інцидентами.

02

Аналіз англомовних текстів

Читати, розуміти та реферувати англомовну технічну літературу, нормативні документи та стандарти у сфері інформаційної безпеки; застосовувати методи порівняльного аналізу.

03

Продукування фахових текстів

Складати технічні звіти, анотації, реферати та аналітичні матеріали англійською мовою з питань організації захисту інформації в інформаційно-комунікаційних системах.

04

Робота з інформаційними ресурсами

Орієнтуватися в англомовних наукових та професійних ресурсах з кібербезпеки; використовувати фахові словники, бази даних та стандарти для підготовки обґрунтованих аналітичних матеріалів.

МОДУЛЬ 1

Основи фахової англійської мови в галузі IT та інформаційної безпеки

1

Тема 1.1

Вступ до фахової англійської мови. Термінологія комп'ютерної інженерії та інформаційних технологій.

2

Тема 1.2

Англомовна лексика з основ інформаційної безпеки. Ключові поняття: confidentiality, integrity, availability (CIA тріада).

3

Тема 1.3

Читання та аналіз англомовної технічної документації. Структура технічного тексту та стандарти ISO/IEC.

4

Тема 1.4

Фахове письмо: анотації, реферати та технічні звіти з питань захисту інформаційно-комунікаційних систем.

МОДУЛЬ 1 · ТЕМА 1.1

Вступ до фахової англійської мови в IT та кібербезпеці

Практичне заняття (4 год.)

Заняття 1: Введення до курсу. Фахова англійська мова та її роль у підготовці спеціаліста з захисту інформації. Особливості технічного стилю мовлення. Базова термінологія комп'ютерної інженерії: hardware, software, network, protocol, encryption, authentication, firewall, vulnerability.

Заняття 2: Читання та переклад англомовних фахових текстів рівня B1–B2. Техніки skimming та scanning. Лексичні вправи на засвоєння базового термінологічного апарату IT-галузі.

Ключові питання занять

- Специфіка фахового стилю в англомовній технічній документації
- Основна IT-термінологія та її відповідники в українській мові
- Структура та особливості технічного тексту
- Стратегії читання англомовних фахових матеріалів

Самостійна робота (8 год.)

Завдання 1. Опрацювання посібника: Тарнопольський О. Б. «Методика навчання іноземних мов у вищій школі» (2023) — розділ «Фахова іноземна мова в технічному ЗВО».

Завдання 2. Укладання глосарію англомовних термінів з комп'ютерної інженерії та інформаційної безпеки (не менше 50 одиниць).

Завдання 3. Письмовий переклад англомовного тексту за фахом (300–400 слів) з коментарем перекладацьких рішень.

Очікуваний результат: студент розуміє специфіку фахової англійської мови, оперує базовою термінологією IT-галузі та вміє застосовувати техніки читання технічних текстів.

МОДУЛЬ 1 · ТЕМА 1.2

Англомовна лексика з основ інформаційної безпеки

1

Confidentiality

Конфіденційність: захист інформації від несанкціонованого доступу. Термінологія та контексти вживання.

2

Integrity

Цілісність: забезпечення достовірності та повноти даних. Ключові поняття та фахові тексти.

3

Availability

Доступність: забезпечення безперебійного доступу до інформаційних ресурсів для авторизованих користувачів.

4

Threats & Risks

Загрози та ризики: malware, phishing, DDoS, insider threat — термінологія та читання звітів про інциденти.

Практичне заняття (4 год.)

Опрацювання CIA-тріади як концептуальної основи інформаційної безпеки через англомовні тексти. Читання та аналіз витягів зі стандарту ISO/IEC 27001 (англійська версія). Лексичні та перекладацькі вправи: threats, vulnerabilities, risks, controls, policies, compliance.

Самостійна робота (8 год.)

СРС: Опрацювання: Ніколаєнко С. М., Луговська К. О. «English for Information Security Professionals» (2023) — розділ «Core Concepts of Information Security»; підготовка анотації (200 слів) до англомовного наукового джерела з тематики модуля.

МОДУЛЬ 1 · ТЕМИ 1.3–1.4

Технічна документація та фахове письмо

Тема 1.3 — Читання технічної документації (4 год.)

Структура та особливості англомовних стандартів і специфікацій у сфері ІБ: ISO/IEC 27001, NIST SP 800-53, GDPR. Методи роботи з нормативними документами: виявлення ключових вимог, визначення сфери застосування, реферування положень. Вправи на переклад нормативних формулювань.

СРС (8 год.): Опрацювання розділів стандарту NIST Cybersecurity Framework (оригінал, англ.); підготовка реферату «Основні вимоги ISO/IEC 27001 до системи управління інформаційною безпекою: англомовний аналіз».

Тема 1.4 — Фахове письмо (4 год.)

Жанри фахового письма англійською мовою: технічний звіт (technical report), анотація (abstract), резюме (executive summary), аналітична записка (analytical memo). Структура та мовні кліше академічного та технічного письма. Письмові вправи: складання анотацій до фахових статей з кібербезпеки.

СРС (8 год.): Опрацювання: Малецька О. В., Бережна С. В. «Academic and Professional Writing in English for IT Students» (2022) — розділ «Technical Reports and Memos»; підготовка технічного звіту (300–400 слів) за тематикою захисту інформації.

МОДУЛЬ 2

Мережева безпека та захист інформаційно-комунікаційних систем

Тема 2.1

Англомовна термінологія мережевої безпеки. Протоколи, архітектура мереж та засоби захисту: firewalls, VPN, IDS/IPS.

Тема 2.2

Читання та аналіз англомовних текстів про кіберзагрози: malware, ransomware, phishing, social engineering.

Тема 2.3

Англомовні стандарти та найкращі практики мережевої безпеки. Аналіз реальних кейсів кібератак англійською мовою.

Тема 2.4

Усна презентація англійською мовою на тему мережевої безпеки. Захист технічного проєкту перед аудиторією.

МОДУЛЬ 2 · ТЕМА 2.1

Англомовна термінологія мережевої безпеки

Практичне заняття (4 год.)

Лексичний та граматичний аналіз англомовних текстів про архітектуру комп'ютерних мереж і засоби захисту. Термінологія: network topology, packet filtering, stateful inspection, intrusion detection system, demilitarized zone (DMZ), proxy server, VPN tunnel, network segmentation.

Ключові питання

- Основна термінологія мережевої безпеки та її переклад
- Читання англомовних технічних схем та діаграм
- Опис архітектури захищеної мережі англійською
- Вживання пасивного стану у технічних описах

Самостійна робота (8 год.)

Завдання 1. Опрацювання: Котенко І. О., Яценко Н. В. «English for Network and Cybersecurity Engineers» (2023) — розділ «Network Security Fundamentals».

Завдання 2. Укладання тематичного глосарію «Мережева безпека» (англ./укр.) — не менше 40 термінів з прикладами вживання у реченнях.

Завдання 3. Написання технічного опису (200–250 слів) архітектури захищеної корпоративної мережі за поданою схемою.

Очікуваний результат: студент оперує термінологією мережевої безпеки, вміє читати та продукувати технічні описи мережевої інфраструктури англійською мовою.

МОДУЛЬ 2 · ТЕМА 2.2

Кіберзагрози: читання та аналіз англомовних текстів

Malware

Читання звітів про шкідливе програмне забезпечення. Типи, ознаки, методи виявлення.

Phishing

Аналіз англомовних кейсів фішингових атак. Термінологія та типові мовні конструкції звітів.

Ransomware

Читання реальних звітів про атаки-вимагачі (Incident Reports). Аналіз наслідків та заходів реагування.

APT

Advanced Persistent Threats: читання аналітичних матеріалів CERTs та провідних дослідницьких центрів.

Incident Report

Складання та читання звітів про інциденти інформаційної безпеки. Структура та мовні кліше.

Практичне заняття (4 год.)

Читання та аналіз реальних англомовних звітів про кіберінциденти (CERT-UA, ENISA, CISA). Обговорення прочитаного англійською мовою: опис загроз, аналіз векторів атак, рекомендовані заходи. Вправи на продукування тексту: складання короткого звіту про інцидент за шаблоном.

Самостійна робота (8 год.)

СРС: Опрацювання відкритих звітів CERT-UA та ENISA Threat Landscape (англ.); підготовка аналітичної записки (300 слів) англійською мовою «Analysis of a Recent Cybersecurity Incident» з описом загрози, наслідків та рекомендацій щодо захисту.

МОДУЛЬ 2 · ТЕМИ 2.3–2.4

Стандарти мережевої безпеки та усна презентація

Тема 2.3 — Стандарти та кейси (4 год.)

Читання та аналіз англомовних документів: NIST SP 800-94 (IDS/IPS), CIS Controls, OWASP Top 10. Порівняльний аналіз підходів до мережевої безпеки у різних стандартах. Переклад ключових вимог та рекомендацій. Аналіз реального кейсу кібератаки на основі англомовного звіту.

СРС (8 год.): Порівняльний аналіз NIST та ISO/IEC підходів до мережевої безпеки на основі оригінальних англомовних документів; підготовка реферату «Cybersecurity Best Practices for ICS: a Standards Overview».

Тема 2.4 — Усна презентація (4 год.)

Підготовка та проведення усної презентації англійською мовою на тему мережевої безпеки. Структура презентації: Introduction, Main Body, Conclusion, Q&A. Мовні кліше для презентацій. Типові помилки та їх виправлення. Рецензування презентацій одногрупників англійською мовою (peer review).

СРС (8 год.): Опрацювання: Тарнопольський О. Б., Кожушко С. П. «Методика навчання англійської мови для спеціальних цілей у технічних університетах» (2022); підготовка та репетиція презентації (7–10 хвилин) на тему захисту мережевої інфраструктури.

МОДУЛЬ 3

Криптографія та методи захисту даних: фахова мова

Тема 3.1

Англомовна термінологія криптографії. Симетричне та асиметричне шифрування, хеш-функції, цифровий підпис.

Тема 3.2

Читання англомовних наукових статей та технічних звітів з криптографічного захисту даних. Аналіз і реферування.

Тема 3.3

PKI (Public Key Infrastructure): англомовна документація, стандарти X.509, SSL/TLS. Читання специфікацій.

Тема 3.4

Написання технічного опису алгоритму шифрування англійською мовою. Академічне письмо в галузі криптографії.

МОДУЛЬ 3 · ТЕМА 3.1

Англомовна термінологія криптографії

Практичне заняття (4 год.)

Систематизація англомовної термінології криптографічного захисту: encryption, decryption, cipher, key, plaintext, ciphertext, hash function, digital signature, certificate, PKI, symmetric/asymmetric cryptography, AES, RSA, ECC. Читання та переклад технічних описів алгоритмів шифрування. Лексичні та граматичні вправи.

Ключові питання

- Базова термінологія криптографії англійською мовою
- Структура описів криптографічних алгоритмів
- Вживання пасивних конструкцій у технічних описах
- Читання математичних позначень та формул у тексті

Самостійна робота (8 год.)

Завдання 1. Опрацювання: Шевченко С. М., Яременко О. І. «Professional English for Cybersecurity and Data Protection» (2023) — розділ «Cryptography Fundamentals».

Завдання 2. Укладання термінологічного словника «Криптографія» (англ./укр.) — не менше 50 термінів.

Завдання 3. Підготовка реферату «Symmetric vs. Asymmetric Encryption: Key Differences and Applications» (300–350 слів) на основі англомовних джерел.

Очікуваний результат: студент оперує термінологією криптографії, вміє читати описи криптографічних алгоритмів і продукувати технічні тексти цієї тематики англійською мовою.

МОДУЛЬ 3 · ТЕМА 3.2

Читання наукових статей з криптографічного захисту

Практичне заняття (4 год.)

Структура англомовної наукової статті: Abstract, Introduction, Related Work, Methodology, Results, Conclusion, References. Стратегії читання наукових публікацій. Критичний аналіз наукового тексту. Написання структурованої анотації (structured abstract) до наукової статті з криптографії. Академічна доброчесність та правила цитування.

Самостійна робота (8 год.)

CPC: Самостійне опрацювання англомовної наукової статті з баз даних IEEE Xplore або Scopus за тематикою «Cryptographic protection in ICS»; підготовка критичної анотації (250 слів) із зазначенням мети, методів, результатів і висновків дослідження.

МОДУЛЬ 3 · ТЕМИ 3.3–3.4

PKI, SSL/TLS та академічне письмо з криптографії

Тема 3.3 — PKI та стандарти (4 год.)

Читання та аналіз англомовних специфікацій PKI, стандарту X.509 та RFC-документів щодо SSL/TLS. Розбір структури цифрового сертифіката. Переклад та реферування відповідних розділів RFC 5280 та RFC 8446 (TLS 1.3). Дискусія англійською мовою: «Why is certificate management critical for ICS security?»

СРС (8 год.): Читання та реферування RFC 8446 (вибрані розділи); підготовка технічного огляду «TLS 1.3: Key Improvements and Security Benefits» (300 слів) на основі оригінальних джерел.

Тема 3.4 — Академічне письмо (4 год.)

Написання технічного опису алгоритму шифрування англійською мовою: структура, мовні засоби, вживання пасивного стану та безособових конструкцій. Академічне письмо: how to describe an algorithm, a process, a system. Письмові вправи: опис роботи алгоритму AES або RSA. Рецензування письмових робіт одногрупників (peer review).

СРС (8 год.): Опрацювання: Малецька О. В., Бережна С. В. «Academic and Professional Writing in English for IT Students» (2022) — розділ «Describing Algorithms and Systems»; написання технічного есе «A Comparative Analysis of AES and RSA Algorithms» (350–400 слів).

МОДУЛЬ 4

Управління інформаційною безпекою: англомовний дискурс

Тема 4.1

Англомовна термінологія управління ризиками ІБ. Risk assessment, risk mitigation, security controls — читання стандартів.

Тема 4.2

Читання та аналіз англомовних політик і процедур інформаційної безпеки організацій. Security policy drafting.

Тема 4.3

Англомовна документація систем управління ІБ (ISMS). ISO/IEC 27001 у оригіналі: структура, вимоги, впровадження.

Тема 4.4

Написання та презентація плану управління інцидентами інформаційної безпеки (Incident Response Plan) англійською.

МОДУЛЬ 4 · ТЕМА 4.1

Управління ризиками ІБ: англомовна термінологія та тексти

Практичне заняття (4 год.)

Систематизація термінології управління ризиками англійською мовою: risk, threat, vulnerability, asset, impact, likelihood, risk assessment, risk treatment, residual risk, risk register, security controls, safeguards. Читання та аналіз розділів ISO/IEC 27005 (Risk Management) в оригіналі. Вправи на переклад та вживання у контексті.

Ключові питання

- Термінологічна база управління ризиками ІБ англійською
- Структура та мова стандарту ISO/IEC 27005
- Читання та заповнення реєстру ризиків (Risk Register) англійською
- Типові мовні конструкції у документах з управління ризиками

Самостійна робота (8 год.)

Завдання 1. Опрацювання: Ніколаєнко С. М., Луговська К. О. «English for Information Security Professionals» (2023) — розділ «Risk Management».

Завдання 2. Укладання тематичного глосарію «Управління ризиками ІБ» (англ./укр.) — 40 термінів з прикладами.

Завдання 3. Підготовка реферату «Risk Assessment Methodologies for Information Systems» (300 слів) з аналізом підходів NIST та ISO.

Очікуваний результат: студент вміє читати та розуміти англомовні документи з управління ризиками ІБ, оперує відповідною термінологією, складає короткі аналітичні тексти цієї тематики.

МОДУЛЬ 4 · ТЕМИ 4.2–4.4

Політики ІБ, ISMS та Incident Response Plan

Тема 4.2 — Політики ІБ (4 год.)

Читання та аналіз англомовних зразків корпоративних політик інформаційної безпеки: Acceptable Use Policy, Password Policy, Data Classification Policy, Remote Access Policy. Виявлення типових мовних конструкцій нормативних текстів: «shall», «must», «is required to». Складання короткого проєкту політики ІБ англійською мовою.

СРС (8 год.): Розробка проєкту «Acceptable Use Policy for ICS» (400 слів) на основі зразків англомовних корпоративних документів.

Тема 4.3 — ISMS за ISO/IEC 27001 (4 год.)

Читання та реферування ключових розділів ISO/IEC 27001:2022 (оригінал). Структура ISMS: context, leadership, planning, support, operation, evaluation, improvement. Вправи на переклад та реферування вимог стандарту. Дискусія: «Challenges of implementing ISO 27001 in Ukrainian IT organizations».

СРС (8 год.): Підготовка аналітичного огляду «Key Requirements of ISO/IEC 27001:2022» (350 слів) на основі оригінального тексту стандарту.

Тема 4.4 — Incident Response Plan (4 год.)

Структура та написання Incident Response Plan (IRP) англійською мовою: Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned (модель PICERL). Читання зразків IRP відомих організацій. Групова робота: розробка IRP для гіпотетичної організації. Усна презентація та захист плану англійською мовою.

СРС (8 год.): Опрацювання: Котенко І. О., Яценко Н. В. «English for Network and Cybersecurity Engineers» (2023) — розділ «Incident Response»; розробка повного Incident Response Plan (600–700 слів) для умовного підприємства з обґрунтуванням рішень.

МОДУЛЬ 5

Захист персональних даних та правове регулювання: англомовний аспект

Тема 5.1

Англомовна термінологія захисту персональних даних. GDPR: читання оригінального тексту регламенту.

Тема 5.2

Англомовні правові тексти у сфері кібербезпеки. Читання та аналіз міжнародних конвенцій та директив ЄС.

Тема 5.3

Privacy by Design та Privacy by Default: читання методичних рекомендацій та написання огляду підходів англійською.

Тема 5.4

Написання та обговорення Privacy Impact Assessment (PIA) / Data Protection Impact Assessment (DPIA) англійською.

МОДУЛЬ 5 · ТЕМИ 5.1–5.2

GDPR та міжнародне правове регулювання кіберпростору

Тема 5.1 — GDPR (4 год.)

Читання та аналіз ключових статей GDPR (General Data Protection Regulation) в оригіналі. Термінологія: data subject, data controller, data processor, personal data, processing, consent, data breach, supervisory authority. Переклад та тлумачення ключових положень. Лексичні вправи. Дискусія: «How does GDPR affect Ukrainian IT companies?»

СРС (8 год.): Опрацювання ст. 5, 6, 13, 17, 25, 32–34 GDPR (оригінал); укладання термінологічного словника «GDPR» (40 термінів); підготовка реферату «Key Obligations under GDPR for IT Companies» (300 слів).

Тема 5.2 — Міжнародне правове регулювання (4 год.)

Читання та реферування англомовних міжнародних документів: Будапештська конвенція про кіберзлочинність (оригінал), NIS2 Directive (ЄС), Cybersecurity Act (ЄС). Виявлення ключових зобов'язань, визначень та механізмів. Порівняльний аналіз підходів до регулювання кіберпростору в різних документах.

СРС (8 год.): Опрацювання: Шевченко С. М., Яременко О. І. «Professional English for Cybersecurity and Data Protection» (2023) — розділ «Legal Frameworks»; аналітична записка «NIS2 Directive: Key Requirements and Implications for Critical Infrastructure» (350 слів).

МОДУЛЬ 5 · ТЕМИ 5.3–5.4

Privacy by Design та оцінка впливу на конфіденційність

Тема 5.3 — Privacy by Design (4 год.)

Читання англомовних методичних матеріалів EDPB (European Data Protection Board) щодо принципів Privacy by Design та Privacy by Default. Аналіз 7 принципів PbD (Ann Cavoukian). Написання структурованого огляду підходів англійською мовою. Дискусія: «Can Privacy by Design be fully implemented in modern ICS?»

СРС (8 год.): Читання EDPB Guidelines on Data Protection by Design and by Default (англ.); підготовка аналітичного огляду «Implementing Privacy by Design in Information Systems» (300 слів).

Тема 5.4 — DPIA (4 год.)

Структура та методологія проведення Data Protection Impact Assessment (DPIA) за вимогами GDPR ст. 35. Читання зразків DPIA-документів відомих організацій. Групова робота: розробка DPIA для умовного ІКС. Написання та презентація звіту DPIA англійською мовою із обґрунтуванням ризиків та заходів пом'якшення.

СРС (8 год.): Опрацювання шаблону DPIA від CNIL (французького регулятора, англ. версія); розробка проєкту DPIA (500–600 слів) для умовної системи управління доступом у корпоративній мережі.

МОДУЛЬ 6

Тестування безпеки та аудит ІКС: фахова мова

Тема 6.1

Англомовна термінологія тестування безпеки: penetration testing, vulnerability assessment, ethical hacking. Читання методологій OWASP, PTES.

Тема 6.2

Читання та написання звітів з тестування на проникнення (Penetration Testing Report) англійською мовою.

Тема 6.3

Аудит інформаційної безпеки: англомовні стандарти та звітність. Читання чеклістів аудиту ISO 27001.

Тема 6.4

Написання звіту про аудит безпеки ІКС англійською мовою. Структура, мова, рекомендації щодо усунення вразливостей.

МОДУЛЬ 6 · ТЕМИ 6.1–6.2

Тестування на проникнення: термінологія та звітність

Тема 6.1 — Термінологія PenTest (4 год.)

Англомовна термінологія тестування безпеки: black-box, white-box, grey-box testing; reconnaissance, scanning, exploitation, post-exploitation, reporting; CVE, CVSS score, zero-day, payload, exploit, shell, privilege escalation. Читання та аналіз методологій OWASP Testing Guide та PTES (Penetration Testing Execution Standard) в оригіналі.

СРС (8 год.): Укладання глосарію «Penetration Testing» (50 термінів); читання та реферування розділу «Information Gathering» з OWASP Testing Guide.

Тема 6.2 — Звіт з PenTest (4 год.)

Структура та написання звіту з тестування на проникнення англійською мовою: Executive Summary, Scope, Methodology, Findings (з CVSS-оцінками), Recommendations, Conclusion. Читання зразкових звітів. Написання розділу «Findings» для гіпотетичного тесту: опис вразливості, вплив, докази (evidence), рекомендації.

СРС (8 год.): Опрацювання: Котенко І. О., Яценко Н. В. «English for Network and Cybersecurity Engineers» (2023) — розділ «Security Testing Reports»; написання повного Penetration Test Executive Summary (400 слів) для умовної системи.

МОДУЛЬ 6 · ТЕМИ 6.3–6.4

Аудит інформаційної безпеки ІКС

Тема 6.3 — Стандарти аудиту ІБ (4 год.)

Читання та аналіз англомовних стандартів аудиту ІБ: ISO/IEC 27007 (Guidelines for Information Security Management Systems Auditing), ISAE 3402. Структура та мова чеклістів аудиту. Реферування ключових вимог. Дискусія: «Internal vs. External Audit: pros and cons for information security management».

СРС (8 год.): Читання та реферування ISO/IEC 27007 (вибрані розділи); укладання аудиторського чеклісту (Audit Checklist) для перевірки відповідності ISO 27001 (15–20 пунктів, англійською мовою).

Тема 6.4 — Звіт з аудиту (4 год.)

Написання звіту про аудит безпеки ІКС англійською мовою: Audit Scope, Objectives, Criteria, Findings, Non-Conformities, Recommendations, Conclusion. Мовні кліше звіту про аудит. Групова робота: розробка звіту за результатами умовного аудиту. Усна презентація результатів аудиту перед «керівництвом» (рольова гра, англійська мова).

СРС (8 год.): Підготовка повного звіту про аудит безпеки умовного підприємства (600–700 слів) з висновками та рекомендаціями щодо усунення невідповідностей вимогам ISO/IEC 27001.

МОДУЛЬ 7

Хмарна безпека та захист розподілених систем: мова фаху

Тема 7.1

Англомовна термінологія хмарних технологій та безпеки: IaaS, PaaS, SaaS, cloud security, shared responsibility model.

Тема 7.2

Читання та аналіз англомовних документів з хмарної безпеки: CSA Cloud Controls Matrix, AWS/Azure Security Best Practices.

Тема 7.3

Безпека IoT та промислових систем управління (ICS/SCADA): фахова англійська мова та відповідні стандарти.

Тема 7.4

Написання технічного проєкту «Security Architecture for Cloud-based ICS» англійською мовою. Захист проєкту.

МОДУЛЬ 7 · ТЕМИ 7.1–7.2

Хмарна безпека: термінологія та документація

Тема 7.1 — Хмарні технології (4 год.)

Англомовна термінологія хмарних обчислень та безпеки: cloud computing, deployment models (public, private, hybrid, multi-cloud), service models (IaaS, PaaS, SaaS), shared responsibility model, cloud access security broker (CASB), zero-trust architecture, identity and access management (IAM). Читання офіційної документації AWS/Azure/GCP з безпеки.

СРС (8 год.): Укладання глосарію «Cloud Security» (45 термінів); читання та реферування CSA Cloud Controls Matrix (вибрані домени).

Тема 7.2 — Хмарна документація (4 год.)

Читання та критичний аналіз англомовних документів: NIST SP 800-144 «Guidelines on Security and Privacy in Public Cloud Computing», CSA Security Guidance for Critical Areas of Focus in Cloud Computing. Визначення ключових ризиків, заходів безпеки та відповідальності сторін. Написання порівняльного аналізу підходів двох стандартів (300 слів).

СРС (8 год.): Опрацювання: Шевченко С. М., Яременко О. І. «Professional English for Cybersecurity and Data Protection» (2023) — розділ «Cloud Security»; підготовка реферату «Top Cloud Security Risks and Mitigation Strategies» (300 слів).

МОДУЛЬ 7 · ТЕМИ 7.3–7.4

Безпека IoT, ICS/SCADA та технічний проєкт

Тема 7.3 — Безпека IoT та ICS (4 год.)

Англомовна термінологія промислових систем управління та IoT-безпеки: SCADA, PLC, HMI, operational technology (OT), IT/OT convergence, air-gap, industrial protocol (Modbus, DNP3). Читання стандарту IEC 62443 (Industrial Cybersecurity) в оригіналі. Аналіз кейсів атак на промислові системи (Stuxnet, Industroyer) на основі англомовних звітів.

СРС (8 год.): Читання та реферування IEC 62443 (вибрані розділи); аналіз англомовного звіту про кіберінцидент в промисловій інфраструктурі; підготовка есе «Securing Industrial Control Systems: Challenges and Best Practices» (300 слів).

Тема 7.4 — Технічний проєкт (4 год.)

Написання та захист технічного проєкту «Security Architecture for a Cloud-based Information System» англійською мовою. Структура проєктного документа: Executive Summary, System Description, Threat Model, Security Controls, Compliance Mapping, Recommendations. Усна презентація (7–10 хвилин) та відповіді на запитання англійською мовою.

СРС (8 год.): Розробка повного технічного проєкту (700–800 слів) із підготовкою слайдів презентації та репетицією усного захисту англійською мовою.

МОДУЛЬ 8

Професійна комунікація та кар'єра в галузі кібербезпеки

Тема 8.1

Англомовне резюме, мотиваційний лист та LinkedIn-профіль спеціаліста з захисту інформації. Пошук роботи в IT.

Тема 8.2

Ділова переписка та усне ділове спілкування: електронні листи, наради, переговори у сфері кібербезпеки.

Тема 8.3

Академічне письмо: написання наукової статті у галузі захисту інформації. Структура, вимоги, подання до журналу.

Тема 8.4

Підсумкова презентація: захист індивідуального дослідницького проєкту англійською мовою. Підсумок курсу.

МОДУЛЬ 8 · ТЕМИ 8.1–8.2

Кар'єрна комунікація та ділова англійська в кібербезпеці

Тема 8.1 — Кар'єрні документи (4 год.)

Написання англомовного CV/resume для спеціаліста з інформаційної безпеки: структура, мовні засоби, ключові слова для ATS. Написання Cover Letter / мотиваційного листа. Заповнення LinkedIn-профілю англійською мовою. Огляд англомовних вакансій: читання job descriptions, розуміння вимог роботодавців (CISM, CISSP, CEH, Security+).

СРС (8 год.): Опрацювання: Тарнопольський О. Б., Кожушко С. П. «Методика навчання англійської мови для спеціальних цілей у технічних університетах» (2022) — розділ «Professional Communication»; написання власного CV та Cover Letter (обидва документи — англійською).

Тема 8.2 — Ділова комунікація (4 год.)

Ділова переписка у сфері кібербезпеки: структура та мовні кліше англомовних службових листів (Inquiry, Complaint, Report, Meeting Request). Усне ділове спілкування: проведення зустрічей, звіти про статус проєкту, телефонні дзвінки та відеонаради в IT-компанії. Рольові ігри: «Security incident meeting» та «Client briefing on data breach».

СРС (8 год.): Написання серії ділових листів (4 листи різних жанрів) англійською мовою за сценарієм «Reporting and managing a data breach incident in an IT company».

МОДУЛЬ 8 · ТЕМИ 8.3–8.4

Академічне письмо та підсумковий проєкт

Тема 8.3 — Наукова стаття (4 год.)

Структура та написання наукової статті у галузі захисту інформації: Title, Abstract, Keywords, Introduction, Related Work, Methodology, Results & Discussion, Conclusion, References. Вимоги міжнародних журналів (IEEE, Springer, Elsevier). Академічна доброчесність: плагіат, цитування, список літератури (APA, IEEE style). Написання власної наукової статті або розширеного реферату (Short Paper) за фаховою тематикою.

СРС (8 год.): Написання Short Paper (600–800 слів) англійською мовою на тему «An Analysis of [Chosen Security Topic] in Information and Communication Systems» з повним оформленням відповідно до вимог.

Тема 8.4 — Підсумковий проєкт (4 год.)

Захист індивідуального дослідницького проєкту англійською мовою. Презентація результатів Short Paper або технічного проєкту перед аудиторією (10–12 хвилин + Q&A). Оцінювання за критеріями: зміст і точність інформації, якість мовлення, структура, відповіді на запитання. Рефлексія на курс: підсумкове обговорення «What have we learned?» — особисті цілі та подальший розвиток у фаховій англійській мові.

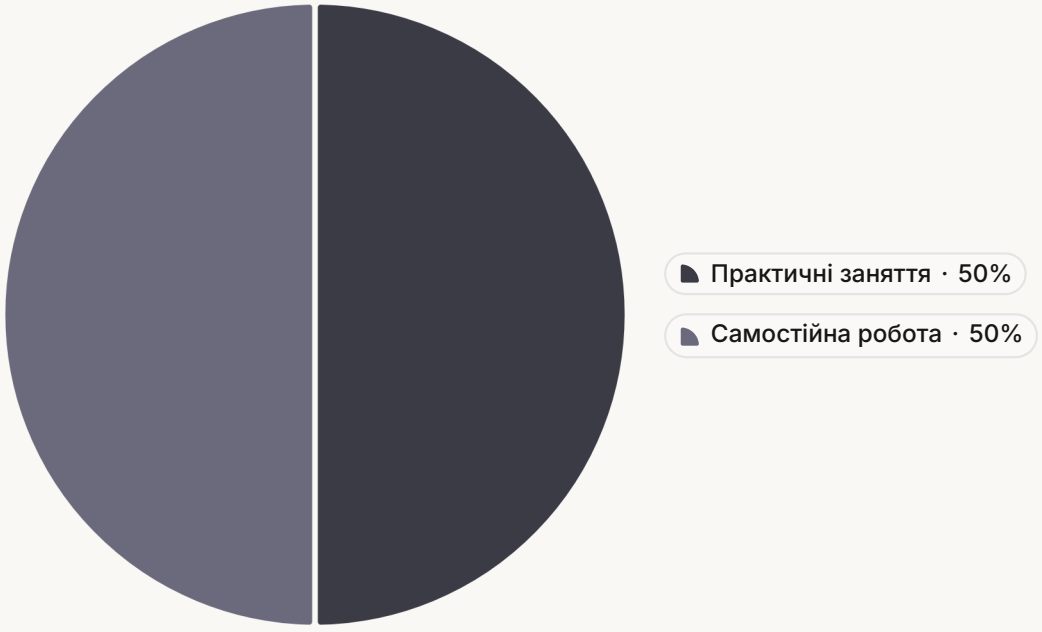
СРС (8 год.): Підготовка фінальної версії дослідницького проєкту, оформлення слайдів, репетиція презентації; самооцінка прогресу за критеріями CEFR (B2–C1 для фахової мови).

Розподіл навчального часу — 240 годин

Модуль	Тема	Практичні (год.)	СРС (год.)	Разом (год.)
Модуль 1	Тема 1.1 — Вступ до фахової англійської	4	8	12
	Тема 1.2 — Лексика ІБ (CIA-тріада)	4	8	12
	Тема 1.3 — Технічна документація	4	8	12
	Тема 1.4 — Фахове письмо	4	8	12
Модуль 2	Тема 2.1 — Мережева безпека: термінологія	4	8	12
	Тема 2.2 — Кіберзагрози: читання текстів	4	8	12
	Тема 2.3 — Стандарти мережевої безпеки	4	8	12
	Тема 2.4 — Усна презентація	4	8	12
Модуль 3	Тема 3.1 — Термінологія криптографії	4	8	12
	Тема 3.2 — Наукові статті з криптографії	4	8	12
	Тема 3.3 — PKI, SSL/TLS	4	8	12
	Тема 3.4 — Академічне письмо (крипто)	4	8	12
Модуль 4	Тема 4.1 — Управління ризиками ІБ	4	8	12
	Тема 4.2 — Політики інформаційної безпеки	4	8	12
	Тема 4.3 — ISMS, ISO/IEC 27001	4	8	12
	Тема 4.4 — Incident Response Plan	4	8	12
Модуль 5	Тема 5.1 — GDPR	4	8	12
	Тема 5.2 — Міжнародне правове регулювання	4	8	12
	Тема 5.3 — Privacy by Design	4	8	12
	Тема 5.4 — DPIA	4	8	12
Модуль 6	Тема 6.1 — Термінологія PenTest	4	8	12
	Тема 6.2 — Звіт з тестування на проникнення	4	8	12
	Тема 6.3 — Стандарти аудиту ІБ	4	8	12
	Тема 6.4 — Звіт з аудиту ІБ	4	8	12
Модуль 7	Тема 7.1 — Хмарна безпека: термінологія	4	8	12
	Тема 7.2 — Хмарна документація	4	8	12
	Тема 7.3 — Безпека IoT та ICS/SCADA	4	8	12
	Тема 7.4 — Технічний проєкт (Cloud ICS)	4	8	12
Модуль 8	Тема 8.1 — Кар'єрні документи	4	8	12
	Тема 8.2 — Ділова комунікація	4	8	12
	Тема 8.3 — Академічне письмо / наукова стаття	4	8	12
	Тема 8.4 — Підсумковий проєкт	4	8	12
Разом	**32 теми / 8 модулів**	**120**	**120**	**240**

Загальний обсяг: 240 годин = 8 кредитів ЄКТС. Розподіл є орієнтовним і може коригуватися відповідно до специфіки навчального процесу та рівня підготовки групи.

Структура навчального часу



Коментар до розподілу

Загальний обсяг — **240 годин (8 кредитів ЄКТС)** — розподілено між практичними заняттями та самостійною роботою для забезпечення балансу між аудиторною та позааудиторною формами навчання.

Практичні заняття — 120 год. (50%)

Відпрацювання навичок читання та аналізу англомовних фахових текстів, усне спілкування, написання технічних документів, розгляд кейсів та захист проєктів. Кожне заняття — 4 академічні години.

Самостійна робота — 120 год. (50%)

Поглиблене вивчення фахової термінологічної бази, опрацювання англомовних стандартів та наукової літератури, підготовка завдань і дослідницьких проєктів. Самостійна робота становить **50% обсягу дисципліни**.

Самостійна робота студентів — Детальний опис

Опрацювання літератури

Поглиблене вивчення фахової англійської мови за навчальними посібниками українських авторів, міжнародними стандартами, науковими статтями у галузі кібербезпеки та захисту інформації. Студент конспектує ключові терміни та конструкції, укладає особисті глосарії.

Індивідуальні завдання

Виконання перекладацьких, аналітичних та творчих завдань: написання анотацій, технічних звітів, аналітичних записок, реферативних оглядів англомовних стандартів і наукових статей з тематики захисту ІКС.

Робота з інформаційними ресурсами

Опрацювання офіційних англомовних ресурсів: **NIST Cybersecurity Framework**, **ENISA**, **ISO.org**, **OWASP**, **CERT-UA**. Пошук та аналіз англомовних наукових публікацій у базах IEEE Xplore та Scopus.

Підготовка до занять та контролю

Підготовка до практичних занять (опрацювання текстів, словникова робота); підготовка до тестувань за ключовими термінами кожного модуля; підготовка до модульних контрольних робіт (систематизація знань, типові завдання).

Форми контролю знань

1	2	3
Поточний контроль	Проміжний контроль	Підсумковий контроль
Завдання: тестові вправи на перевірку засвоєння термінологічного мінімуму кожної теми (15–20 питань), контрольне читання фахового тексту з виконанням завдань (True/False, Multiple Choice, Short Answer), оцінювання усних відповідей. Проводиться на кожному практичному занятті або після кожних 2 тем.	Модульна контрольна робота після завершення кожного змістовного модуля: читання англомовного тексту з завданнями, переклад фахового фрагменту, лексичний тест за термінологією модуля, написання короткого тексту (150–200 слів) за заданою ситуацією. Оцінюється повнота, точність та мовна грамотність виконання.	Залік (або іспит) відповідно до навчального плану: усна частина (презентація підсумкового проєкту або бесіда за фаховою тематикою) + письмова частина (читання з завданнями, письмовий твір або технічний документ). Підсумкова оцінка враховує поточний, проміжний та підсумковий контроль: **100-бальна система** з переведенням в національну шкалу та ЄКТС (A, B, C, D, E, FX, F).

Методи викладання

Викладання дисципліни «Фахова англійська мова» поєднує комунікативні, проєктні та інтерактивні методи, що забезпечує формування реальних мовних компетентностей для роботи в англомовному фаховому середовищі кібербезпеки та захисту ІКС.

Комунікативний метод

Усні дискусії, рольові ігри, дебати та презентації фахових тем кібербезпеки англійською мовою; розвиток спонтанного мовлення в реалістичних ситуаціях.

Робота з автентичними текстами

Опрацювання оригінальних англомовних документів: стандартів ISO/NIST, звітів CERT-UA/ENISA, наукових публікацій IEEE; розвиток навичок критичного читання.

Кейс-стаді

Аналіз реальних кіберінцидентів, документів з управління ІБ та звітів з аудиту на основі англомовних джерел; формування навичок прийняття рішень у фаховому контексті.

Проєктна робота

Розробка групових та індивідуальних проєктів (IRP, Security Architecture, Audit Report) англійською мовою; інтеграція мовних, технічних і дослідницьких навичок.

Взаємооцінювання (Peer Review)

Рецензування письмових робіт та усних презентацій одногрупників за чіткими критеріями; розвиток навичок критичного аналізу та конструктивного зворотного зв'язку.

Академічне письмо

Навчання написанню технічних звітів, наукових статей, анотацій та ділових листів відповідно до міжнародних академічних стандартів; систематичне відпрацювання письмових жанрів.

Рекомендована література — Основні навчальні посібники (2022–2024 рр.)

1. Тарнопольський О. Б., Кожушко С. П. Методика навчання англійської мови для спеціальних цілей у технічних університетах. — Дніпро : Університет імені Альфреда Нобеля, 2022. — 296 с.

2. Ніколаєнко С. М., Луговська К. О. English for Information Security Professionals : навч. посіб. — Київ : Академвидав, 2023. — 288 с. *Рекомендується для модулів 1–4.*

3. Шевченко С. М., Яременко О. І. Professional English for Cybersecurity and Data Protection : навч. посіб. — Харків : НТМТ, 2023. — 312 с. *Рекомендується для модулів 3–7.*

4. Малецька О. В., Бережна С. В. Academic and Professional Writing in English for IT Students : навч. посіб. — Київ : КПІ ім. Ігоря Сікорського, 2022. — 256 с. *Рекомендується для модулів 1, 3, 8.*

5. Котенко І. О., Яценко Н. В. English for Network and Cybersecurity Engineers : навч. посіб. — Київ : Ліра-К, 2023. — 320 с. *Рекомендується для модулів 2, 6, 7.*

6. Тарнопольський О. Б. Методика навчання іноземних мов у вищій школі : підручник. — 2-ге вид., переробл. — Дніпро : Університет імені Альфреда Нобеля, 2023. — 344 с.

7. Луговська К. О., Шаповалова О. В. English for Computer Engineers: Technical Reading and Writing : навч. посіб. — Київ : Наукова думка, 2024. — 272 с. *Рекомендується для модулів 1–2.*

8. Яременко О. І., Бондаренко В. С. Фахова іноземна мова для спеціальності «Захист інформації» : навч.-метод. посіб. — Київ : НАУ, 2024. — 240 с. *Рекомендується для модулів 4–5.*

Додаткова література та нормативні документи

9. Бережна С. В., Ковтун О. М.

English for IT Security: Vocabulary and Reading Comprehension. — Київ : Знання, 2022. — 198 с. *Рекомендується для модулів 1–3 (термінологічний мінімум).*

10. ISO/IEC 27001:2022

Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. — ISO, 2022. *Основний стандарт для модулів 4 та 6 (оригінал, англійська мова).*

11. NIST Cybersecurity Framework v2.0

National Institute of Standards and Technology. Cybersecurity Framework 2.0. — NIST, 2024. — Режим доступу: **nist.gov/cyberframework**. *Рекомендується для модулів 1–4.*

12. Луговська К. О., Прокопенко А. І.

Ділова англійська мова у сфері інформаційних технологій : навч. посіб. — Харків : ХНУ імені В. Н. Каразіна, 2023. — 228 с. *Рекомендується для модуля 8.*

Нормативно-правова база та міжнародні стандарти

- Закон України «Про освіту» від 05.09.2017 № 2145-VIII

  Визначає засади освітньої діяльності, у т.ч. вимоги до вивчення іноземних мов у закладах вищої освіти. **zakon.rada.gov.ua**

- Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII

  Визначає правові засади забезпечення кібербезпеки — базовий нормативний документ для фахового контексту курсу. **zakon.rada.gov.ua**

- Стандарт вищої освіти зі спеціальності 123 «Комп'ютерна інженерія»

  Перший (бакалаврський) рівень вищої освіти. МОН України, 2019 (чинна редакція). Визначає компетентності та результати навчання. **mon.gov.ua**

- GDPR — Regulation (EU) 2016/679

  General Data Protection Regulation. Основний регуляторний документ для вивчення англомовної правової термінології захисту персональних даних (Модуль 5). **gdpr-info.eu**

- Budapest Convention on Cybercrime (ETS No. 185)

  Будапештська конвенція про кіберзлочинність. Рада Європи, 2001 (оригінал, англ.). Ратифікована Україною. Матеріал для Модуля 5. **coe.int**

Офіційні англомовні ресурси та фахові видання

NIST (США)

nist.gov — стандарти кібербезпеки, NIST CSF, NIST SP 800-серія. Основний ресурс для модулів 1–4, 6–7.

ENISA (ЄС)

enisa.europa.eu — щорічний звіт про кіберзагрози (ETL), методичні матеріали з ІБ, рекомендації для критичної інфраструктури.

OWASP

owasp.org — OWASP Top 10, Testing Guide, SAMM. Відкриті англомовні методичні матеріали для модулів 2 та 6.

CERT-UA

cert.gov.ua — офіційні звіти про кіберінциденти в Україні (англійська версія сайту). Актуальний матеріал для модулів 2 та 4.

IEEE Xplore

ieeexplore.ieee.org — провідна база англомовних наукових публікацій з комп'ютерної інженерії, кібербезпеки та захисту інформації.

ISO Online Browsing Platform

iso.org/obp — офіційний доступ до міжнародних стандартів серії ISO/IEC 27000 в оригіналі.

Національна бібліотека України

nbuv.gov.ua — електронні ресурси, наукові статті та монографії з фахової іноземної мови та інформаційної безпеки.

МОН України

mon.gov.ua — освітні стандарти, навчальні програми, методичні рекомендації МОН щодо вивчення іноземних мов у ЗВО.

Зв'язок дисципліни зі спеціальністю та ОП

Чому фахова англійська для захисту інформації?

Дисципліна «Фахова англійська мова» є невід'ємною складовою підготовки бакалаврів за ОП «Організація захисту інформації в інформаційно-комунікаційних системах». Провідні міжнародні стандарти (ISO, NIST, IEC), наукові публікації та технічна документація провідних виробників рішень ІБ — переважно англійською мовою.

Сучасний фахівець з кіберзахисту, який не володіє фаховою англійською, позбавлений доступу до 90% актуальних знань і позбавлений конкурентоздатності на міжнародному ринку праці в IT-галузі.

Практичне значення для кар'єри

- Читання та застосування міжнародних стандартів ІБ (ISO/IEC 27001, NIST, GDPR) в оригіналі
- Участь у міжнародних конференціях та проєктах з кібербезпеки
- Підготовка документації для міжнародних замовників та партнерів
- Доступ до найновіших англомовних досліджень, CVE-баз та звітів з кіберзагроз
- Отримання міжнародних сертифікатів (CISSP, CISM, CEH, CompTIA Security+)
- Кар'єрні можливості в міжнародних IT-компаніях та організаціях ЄС/НАТО

Ключові компетентності курсу — Підсумок

Курс охоплює всі ключові тематичні напрями захисту інформації в ІКС через призму фахової англійської мови — від базової термінології до написання наукових статей і захисту технічних проєктів на міжнародному рівні.

Бажаємо успіхів у вивченні фахової англійської мови!

240

Годин

Загальний обсяг дисципліни

8

Кредити ЄКТС

Відповідно до стандарту

32

Теми

У 8 змістовних модулях

12

Джерел

Рекомендованої літератури 2022–2024 рр.

> «Language is the road map of a culture. It tells you where its people come from and where they are going.» — Rita Mae Brown

Спеціальність 123 · Комп'ютерна інженерія · Бакалавр · 8 кредитів ЄКТС · ОП: Організація захисту інформації в ІКС