Силабус дисципліни «Фахова англійська мова»

СПЕЦІАЛЬНІСТЬ 123 · КОМП'ЮТЕРНА ІНЖЕНЕРІЯ · БАКАЛАВР · ОП «ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІКС»

240

Годин загальний обсяг дисципліни

8

Кредити ЄКТС відповідно до стандарту

8

Змістовних модулі курсу

Загальна інформація про дисципліну

Ідентифікація

Назва: Фахова англійська мова

Спеціальність: 123 Комп'ютерна інженерія

ОП: Організація захисту інформації в ІКС

Ступінь: Бакалавр

Обсяг: 240 годин / 8 кредитів ЄКТС

Модулів: 8 змістовних блоки курсу

Практичні: 120 годин

Самостійна робота: 120 годин

Мета дисципліни

Дисципліна «Фахова англійська мова» формує у студентів спеціальності «Комп'ютерна інженерія» систему знань, умінь і навичок читання, аудіювання, говоріння та письма англійською мовою у сфері інформаційних технологій, комп'ютерної інженерії та захисту інформації. Курс спрямований на опанування фахової лексики у галузі кібербезпеки та ІКС, розвиток навичок читання технічної документації, написання академічних текстів і усної фахової комунікації англійською мовою, а також підготовку до роботи з іноземними науковими джерелами та міжнародними стандартами інформаційної безпеки.

Форми навчання

- Практичні заняття — 120 годин
- Самостійна робота — 120 годин

Компетентності та результати навчання

Загальні компетентності

Здатність до іншомовної комунікації у сфері інформаційних технологій та кібербезпеки: розуміння автентичних англомовних текстів технічного та наукового характеру, ведення фахової дискусії, підготовки письмових матеріалів англійською мовою. Уміння самостійно розширювати словниковий запас, користуватися фаховими словниками, довідниками та онлайн-ресурсами для поповнення знань у сфері IT та інформаційної безпеки.

Здатність до усної та письмової фахової комунікації англійською мовою: чітко пояснювати технічні поняття, аргументовано обговорювати питання кібербезпеки, захисту інформації та комп'ютерної інженерії. Відповідальність та ініціативність у виконанні комунікативних завдань та роботі в групі.

- Аналізувати англомовні технічні та наукові тексти у сфері ІКС
- Планувати власну мовленнєву діяльність і дотримуватися дедлайнів
- Коректно спілкуватися іноземною мовою в академічному середовищі
- Брати участь у командній роботі над іноземномовними проєктами

Фахові компетентності

Розуміння фахової термінології в галузі комп'ютерної інженерії, кібербезпеки та захисту інформації англійською мовою: системна лексика з мережевих технологій, операційних систем, криптографії, протоколів безпеки та міжнародних стандартів ISO/IEC. Знання ключових фахових понять та вміння застосовувати їх в усній і письмовій англомовній комунікації.

Здатність читати та розуміти технічну документацію, стандарти, RFC-документи, наукові статті та звіти у сфері інформаційної безпеки, а також писати анотації, резюме, есе та технічні звіти англійською мовою.

- Читати й аналізувати англомовну технічну документацію та стандарти
- Вести усну фахову дискусію з тематики кібербезпеки англійською
- Писати анотації, резюме та технічні звіти англійською мовою
- Опрацьовувати міжнародні стандарти серії ISO/IEC 27000 мовою оригіналу
- Готувати та представляти фахові презентації англійською мовою

Результати навчання

Після успішного завершення курсу студент повинен демонструвати такі результати навчання:

1	2
Знання та розуміння Пояснювати сутність ключових понять фахової англійської мови у галузі комп'ютерної інженерії та кібербезпеки: cybersecurity, information security, network architecture, encryption, authentication, access control, vulnerability, threat, incident response. Розуміти й інтерпретувати автентичні англомовні тексти з технічної та наукової літератури у сфері захисту інформації в ІКС.	**Аналіз та оцінювання** Аналізувати англомовні технічні тексти, наукові статті та стандарти з точки зору змісту, структури та термінологічної коректності. Оцінювати рівень власного іноземномовного мовлення, виявляти прогалини у знаннях і самостійно їх усувати, використовуючи фахові словники та англомовні ресурси у відкритому доступі.
3	**4**
Застосування знань Застосовувати фахову англійську лексику та граматичні конструкції при складанні технічних документів, звітів, анотацій і презентацій у сфері захисту інформації в інформаційно-комунікаційних системах. Представляти результати досліджень і проєктів англійською мовою в усній і письмовій формах.	**Комунікація та рефлексія** Аргументовано викладати власну позицію з питань кібербезпеки та захисту інформації англійською мовою в академічному та професійному середовищі. Формувати готовність до участі в міжнародних конференціях, стажуваннях та взаємодії з іноземними колегами у сфері інформаційної безпеки.

Модуль 1. Основи фахової англійської у сфері IT та кібербезпеки

ЗМІСТОВНИЙ МОДУЛЬ 1

Тема 1.1

Фахова лексика у сфері комп'ютерної інженерії. Термінологічна база комп'ютерної інженерії англійською мовою: hardware, software, network, operating system, architecture, processor, memory. Особливості технічного стилю мовлення. Читання та переклад фахових текстів з комп'ютерної тематики. Вправи на розширення термінологічного словника.

Тема 1.2

Граматичні конструкції у технічному тексті. Пасивний стан та його функції в технічних описах і документації. Інфінітивні та дієприкметникові звороти. Модальні дієслова у технічних інструкціях і стандартах. Практика читання та трансформації речень за моделями технічного тексту.

Модуль 2. Мережеві технології та архітектура ІКС

ЗМІСТОВНИЙ МОДУЛЬ 2

Тема 2.1

Лексика мережевих технологій та протоколів. Фахова термінологія мережевої архітектури: LAN, WAN, VPN, TCP/IP, DNS, DHCP, router, switch, firewall, proxy. Читання технічних описів мережевих топологій. Усне обговорення принципів роботи мережевих протоколів безпеки. Робота з автентичними англомовними RFC-документами.

Тема 2.2

Опис та характеристика інформаційно-комунікаційних систем. Лексика для опису компонентів і функцій ІКС англійською мовою. Типові граматичні моделі технічного опису: визначення, класифікація, порівняння. Письмові вправи зі складання технічних характеристик систем. Читання та аналіз технічних специфікацій.

Модуль 3. Кібербезпека та захист інформації: фахова лексика

ЗМІСТОВНИЙ МОДУЛЬ 3

Тема 3.1

Термінологія кібербезпеки та інформаційних загроз. Ключова лексика галузі: cybersecurity, threat, vulnerability, malware, ransomware, phishing, social engineering, intrusion detection, incident response. Читання оглядових статей із кібербезпеки. Обговорення сучасних загроз та методів захисту. Робота з глосарієм стандарту ISO/IEC 27001 мовою оригіналу.

Тема 3.2

Криптографія та методи захисту даних. Фахова лексика з криптографії та захисту даних: encryption, decryption, symmetric/asymmetric cryptography, digital signature, PKI, hashing, certificate. Читання технічної документації з криптографічних алгоритмів. Усний опис принципів роботи засобів криптографічного захисту.

Модуль 4. Міжнародні стандарти інформаційної безпеки

ЗМІСТОВНИЙ МОДУЛЬ 4

Тема 4.1

Читання та інтерпретація стандартів ISO/IEC серії 27000. Структура та мова міжнародних стандартів у сфері інформаційної безпеки. Ключові розділи стандартів ISO/IEC 27001, 27002, 27005. Лексика стандартизації: scope, requirement, control, risk assessment, policy, procedure, audit. Практика роботи з оригінальними текстами стандартів.

Тема 4.2

Фреймворки та регуляторні документи з інформаційної безпеки. Мова та структура NIST Cybersecurity Framework, GDPR, CIS Controls. Порівняльний аналіз фреймворків інформаційної безпеки: читання, анотування та обговорення положень документів англійською мовою. Складання коротких письмових оглядів нормативних документів.

Модуль 5. Академічне письмо та наукова комунікація

ЗМІСТОВНИЙ МОДУЛЬ 5

Тема 5.1

Структура та написання академічних текстів англійською мовою. Жанри академічного письма: abstract, essay, research paper, literature review, report. Структура наукової статті: introduction, methodology, results, discussion, conclusion. Типові лексичні та граматичні конструкції академічного стилю. Написання анотацій до фахових статей з кібербезпеки.

Тема 5.2

Написання технічних звітів та документації. Структура технічного звіту та документації у сфері захисту інформації. Лексика для опису методів, результатів і рекомендацій. Практика написання технічних звітів про тестування систем безпеки, інцидент-репортів та аналітичних записок англійською мовою. Правила оформлення посилань і бібліографії.

Модуль 6. Усна фахова комунікація та презентаційні навички

ЗМІСТОВНИЙ МОДУЛЬ 6

Тема 6.1

Усна фахова комунікація у сфері ІТ та кібербезпеки. Мовленнєві кліше та стратегії ведення фахових дискусій і переговорів англійською мовою. Презентація технічних рішень: структура виступу, аргументація, відповіді на запитання. Рольові ігри: технічні наради, обговорення захисту систем, демонстрація результатів аудиту безпеки.

Тема 6.2

Підготовка та представлення фахових презентацій. Структура ефективної наукової та технічної презентації англійською мовою. Лексика для опису графіків, діаграм, схем і результатів досліджень. Практика підготовки та захисту презентацій з тематики кібербезпеки та організації захисту інформації в ІКС. Зворотній зв'язок і самооцінювання.

Модуль 7. Читання та аналіз фахової літератури

ЗМІСТОВНИЙ МОДУЛЬ 7

Тема 7.1

Стратегії читання технічних та наукових текстів. Навички переглядового, вибіркового та вивчаючого читання технічних текстів англійською мовою. Розуміння структури наукових публікацій у галузі кібербезпеки. Конспектування та анотування англомовних джерел. Пошук та критичне оцінювання інформації у базах Scopus, Web of Science та IEEE Xplore.

Тема 7.2

Аудіювання та розуміння англомовного фахового мовлення. Сприйняття на слух технічних лекцій, подкастів і відеоматеріалів з кібербезпеки. Стратегії розуміння автентичного мовлення носіїв мови. Практика аудіювання доповідей з міжнародних конференцій DEF CON, RSA Conference, IEEE S&P. Конспектування почутого та відтворення основних думок.

Модуль 8. Фахова англійська для кар'єри та міжнародної співпраці

ЗМІСТОВНИЙ МОДУЛЬ 8

Тема 8.1

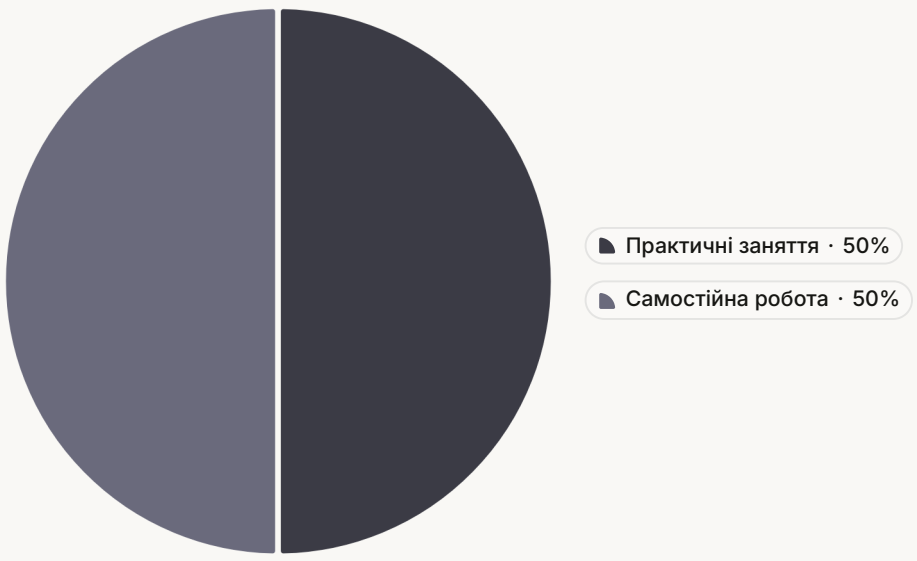
Ділова англійська у сфері IT та кібербезпеки. Написання ділових листів, електронних повідомлень, запитів та відповідей англійською мовою у контексті IT-галузі. Лексика для ведення ділового листування з питань безпеки інформаційних систем. Складання CV та мотиваційного листа для роботи у сфері кібербезпеки. Підготовка до технічного інтерв'ю англійською.

Тема 8.2

Участь у міжнародній науково-технічній комунікації. Підготовка тез та статей для міжнародних конференцій з інформаційної безпеки. Правила подання робіт до міжнародних видань. Peer review: рецензування та коментування англомовних технічних матеріалів. Огляд провідних міжнародних конференцій у сфері кібербезпеки та їх вимоги до авторів.

Розподіл навчального часу — 240 годин

Модуль	Тема	Практичні (год.)	Самостійна робота (год.)
Модуль 1	Тема 1.1 — Фахова лексика у сфері комп'ютерної інженерії	8	7
	Тема 1.2 — Граматичні конструкції у технічному тексті	7	8
Модуль 2	Тема 2.1 — Лексика мережевих технологій та протоколів	8	7
	Тема 2.2 — Опис та характеристика інформаційно-комунікаційних систем	7	8
Модуль 3	Тема 3.1 — Термінологія кібербезпеки та інформаційних загроз	8	7
	Тема 3.2 — Криптографія та методи захисту даних	7	8
Модуль 4	Тема 4.1 — Читання та інтерпретація стандартів ISO/IEC 27000	8	7
	Тема 4.2 — Фреймворки та регуляторні документи з ІБ	7	8
Модуль 5	Тема 5.1 — Структура та написання академічних текстів	8	7
	Тема 5.2 — Написання технічних звітів та документації	7	8
Модуль 6	Тема 6.1 — Усна фахова комунікація у сфері IT	8	7
	Тема 6.2 — Підготовка та представлення фахових презентацій	7	8
Модуль 7	Тема 7.1 — Стратегії читання технічних та наукових текстів	8	7
	Тема 7.2 — Аудіювання та розуміння англомовного фахового мовлення	7	8
Модуль 8	Тема 8.1 — Ділова англійська у сфері IT та кібербезпеки	8	7
	Тема 8.2 — Участь у міжнародній науково-технічній комунікації	7	8
Разом		**120**	**120**



Структура навчального часу

Загальний обсяг — **240 годин (8 кредитів ЄКТС)** — розподілено між двома формами роботи для забезпечення балансу між практичним відпрацюванням навичок та самостійним поглибленням знань.

- **Практичні заняття (120 год. — 50%):** відпрацювання мовних навичок, аналіз текстів, дискусії та презентації
- **Самостійна робота (120 год. — 50%):** поглиблене вивчення, читання літератури, підготовка письмових завдань

Рівний розподіл між практичними заняттями та самостійною роботою забезпечує **максимальне занурення в мовне середовище** та відповідальність студента за власний мовленнєвий розвиток.

Самостійна робота студентів та методи викладання

Форми самостійної роботи

Опрацювання літератури

Поглиблене вивчення фахової англійської мови за навчальними посібниками для IT-спеціальностей, читання автентичних технічних текстів, наукових статей у базах IEEE Xplore, ACM Digital Library та Scopus. Конспектування ключових термінів, порівняння перекладацьких підходів різних авторів.

Індивідуальні завдання

Виконання письмових завдань: написання анотацій до англомовних статей з кібербезпеки, підготовка есе та технічних звітів, складання глосаріїв з тематики захисту інформації в ІКС, переклад фрагментів стандартів ISO/IEC 27001.

Робота з інформаційними ресурсами

Опрацювання англомовних ресурсів: NIST (**nist.gov**), ENISA (**enisa.europa.eu**), IEEE Xplore (**ieeexplore.ieee.org**). Аналіз технічних звітів, стандартів та наукових публікацій у відкритому доступі.

Підготовка до занять

Підготовка до практичних занять: читання заданих текстів, вивчення нової лексики, підготовка усних відповідей; систематичне повторення граматичного матеріалу; підготовка до тестувань із фахової термінології та мовних конструкцій.

Методи викладання

→ Практичні заняття

Комунікативний підхід: відпрацювання мовних навичок через виконання автентичних завдань — читання, обговорення, письмо, аудіювання та говоріння з фахової тематики IT та кібербезпеки.

→ Кейс-стаді

Аналіз реальних англомовних звітів про кіберінциденти (CERT, ENISA, NIST); студенти аналізують текст, виявляють ключові терміни, формулюють висновки та презентують їх англійською.

→ Рольові ігри та симуляції

Ділові переговори, технічні наради, захист проєктів — усі ситуативні вправи відтворюють реальні комунікативні сценарії фахівця з кібербезпеки у міжнародному середовищі.

→ Робота з автентичними текстами

Читання та аналіз стандартів ISO/IEC, NIST SP, технічних RFC-документів, наукових статей IEEE та ACM; формування навичок критичного читання англомовної фахової документації.

→ Самостійне дослідження

Підготовка анотацій, есе та презентацій з обраної теми у сфері кібербезпеки; розвиток навичок самостійного пошуку й систематизації англомовних наукових і технічних джерел.

Форми контролю знань

1

Поточний контроль

Завдання: словниковий диктант, усна відповідь, читання та переклад фахового тексту за темою змістовного модуля. Оцінюються регулярність виконання завдань, якість мовлення і рівень засвоєння фахової лексики. Поточний контроль формує накопичувальну оцінку протягом семестру. Включає усні відповіді, тести на знання термінології, виконання граматичних вправ та участь у дискусіях з кібербезпеки.

2

Проміжний контроль

Самостійна робота — письмове завдання або усна презентація за темами змістовних модулів (написання анотації, есе або технічного звіту, захист підготовленої презентації з тематики захисту інформації в ІКС). Оцінюються повнота відповіді, правильність використання термінів та мовна коректність. Проводиться після кожного парного змістовного модуля.

3

Підсумковий контроль

Залік / іспит відповідно до навчального плану. Форма проведення — тестування фахової лексики, читання та аналіз автентичного тексту, усна відповідь з тематики курсу. Підсумкова оцінка враховує результати поточного, проміжного та підсумкового контролю відповідно до 100-бальної системи з переведенням у національну шкалу та ЄКТС (A, B, C, D, E, FX, F).

Усі методи контролю спрямовані на формування іншомовної комунікативної компетентності, передбаченої освітньо-професійною програмою «Організація захисту інформації в ІКС» спеціальності 123 «Комп'ютерна інженерія».

Рекомендована література та ресурси

Навчальна та наукова література (2022–2024)

1. Новікова Г. В., Денисенко І. В. English for Information Technology: навч. посіб. — Київ : НаУКМА, 2022. — 87 с.
2. Ковальчук О. С., Мартиненко О. В. Англійська мова для фахівців з інформаційної безпеки: навч. посіб. — Київ : КПІ ім. Ігоря Сікорського, 2023. — 196 с.
3. Бондаренко Н. І., Кравченко Т. М. Фахова англійська мова для ІТ-спеціальностей: навч. посіб. — Харків : ХНУРЕ, 2022. — 210 с.
4. Петрук О. М., Сидоренко В. В. Англійська мова у сфері інформаційних та комп'ютерних технологій: навч. посіб. — Львів : Видавництво Львівської політехніки, 2023. — 224 с.
5. Ромась Н. О., Шевченко Л. Б. Академічне письмо англійською мовою для технічних спеціальностей: навч. посіб. — Київ : НТУУ «КПІ ім. Ігоря Сікорського», 2022. — 178 с.
6. Грищенко А. В., Назаренко О. С. Основи наукової комунікації англійською мовою: навч. посіб. — Херсон : ХДУ, 2023. — 156 с.
7. Дяченко Т. Ю., Король О. П. Ділова англійська мова у сфері кібербезпеки та ІТ: навч. посіб. — Київ : Університет «Україна», 2024. — 184 с.
8. Лисенко І. М., Харченко В. М. English for Cybersecurity and Computer Engineering: навч.-метод. посіб. — Київ : МЄУ, 2023. — 144 с.
9. Мельник Т. В., Зінченко О. Л. Технічний переклад та фахова комунікація в галузі захисту інформації: навч. посіб. — Одеса : ОДЕКУ, 2024. — 168 с.
10. Гаврилюк А. В., Іванченко С. М. Англійська мова для студентів спеціальності «Комп'ютерна інженерія»: навч. посіб. — Житомир : ЖНАЕУ, 2022. — 190 с.

Офіційні інтернет-ресурси та бази даних

1. IEEE Xplore Digital Library — бази наукових публікацій з ІТ та кібербезпеки. — URL: **https://ieeexplore.ieee.org/**
2. NIST — Національний інститут стандартів і технологій США (стандарти кібербезпеки). — URL: **https://www.nist.gov/**
3. ENISA — Агентство ЄС з кібербезпеки (звіти, рекомендації, глосарії). — URL: **https://www.enisa.europa.eu/**
4. ACM Digital Library — база публікацій з комп'ютерних наук. — URL: **https://dl.acm.org/**
5. Національна бібліотека України ім. В. І. Вернадського. — URL: **https://nbuv.gov.ua/**
6. Науково-технічний журнал «Кібербезпека: освіта, наука, техніка». — URL: **https://csecurity.kubg.edu.ua/**
7. Кембриджський онлайн словник англійської мови. — URL: **https://dictionary.cambridge.org/**
8. Державна служба спеціального зв'язку та захисту інформації України (англомовний розділ). — URL: **https://cip.gov.ua/**

Рекомендована література охоплює видання **2022–2024 років** українських авторів відповідно до вимог актуальності навчально-методичного забезпечення ОП «Організація захисту інформації в ІКС».