Робоча програма дисципліни «Фахова німецька 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 німецька мова

Спеціальність: 123 Комп'ютерна інженерія

ОП: Організація захисту інформації в ІКС

Ступінь: Бакалавр

Обсяг: 240 годин / 8 кредитів ЄКТС

Практичних: 120 год. | **СРС:** 120 год.

Модулів: 8 змістовних блоки

Призначення дисципліни

Дисципліна «Фахова німецька мова» формує у студентів комунікативну компетентність у сфері інформаційних технологій, захисту інформації та кібербезпеки на матеріалі сучасної фахової німецькомовної літератури. Курс охоплює лексику з комп'ютерних мереж, криптографії, кіберзагроз, нормативно-правового регулювання у сфері ІБ, а також розвиває навички читання технічної документації, ведення ділової кореспонденції та фахових переговорів.

Дисципліна є обов'язковою для підготовки бакалаврів зі спеціальності «Комп'ютерна інженерія» (ОП «Організація захисту інформації в ІКС») та забезпечує формування загальних і фахових компетентностей, передбачених освітньо-професійною програмою.

Загальні компетентності

Комунікативна компетентність

Здатність до усної та письмової комунікації німецькою мовою в академічному та професійному середовищі: ведення ділового листування, технічної документації, участь у конференціях та презентаціях у сфері IT та захисту інформації.

Аналітичне мислення

Здатність критично аналізувати, систематизувати та узагальнювати науково-технічну інформацію з фахових джерел, виявляти ключові поняття, порівнювати підходи різних авторів та формулювати обґрунтовані висновки.

Самоорганізація та навчання

Уміння самостійно навчатися, планувати роботу, організовувати виконання завдань у визначені строки, зокрема під час підготовки перекладів, анотацій, рефератів і науково-технічних проектів.

Командна взаємодія

Відповідальність, ініціативність та готовність працювати в команді під час групового аналізу фахових текстів, підготовки спільних презентацій та моделювання ситуацій ділового спілкування у сфері захисту інформації.

Студент повинен вміти: читати та розуміти фахові тексти з інформаційної безпеки та комп'ютерних технологій; перекладати науково-технічну документацію; вести ділове листування; здійснювати усну комунікацію з фахових питань; працювати з довідковою та лексикографічною літературою.

Фахові компетентності

Фахова лексика ІТ та ІБ

Володіння термінологічним апаратом у галузі комп'ютерних мереж, програмного забезпечення, криптографії, кіберзагроз та захисту інформаційно-комунікаційних систем на матеріалі оригінальних німецькомовних фахових текстів.

Перекладацька компетентність

Здатність здійснювати письмовий та усний переклад технічних текстів, інструкцій, стандартів і нормативної документації у сфері інформаційної безпеки з/на німецьку мову з дотриманням термінологічної точності та стилістичних норм.

Ділова комунікація

Знання норм і стандартів ділового листування, складання технічних звітів, резюме, заявок на конференції та листів-запитів німецькою мовою у контексті міжнародної співпраці в ІТ-секторі та сфері кібербезпеки.

Нормативно-правова база

Орієнтування в основних нормативно-правових актах ЄС у сфері інформаційної безпеки (GDPR, NIS Directive, BSI-Grundschutz) та здатність читати і аналізувати їх оригінальні тексти німецькою мовою.

Результати навчання

01

Читання та аналіз фахових текстів

Читати, розуміти та аналізувати оригінальні науково-технічні тексти з інформаційної безпеки, кібербезпеки та комп'ютерних мереж, написані сучасною фаховою німецькою мовою, виявляти ключові поняття та структуру аргументації.

02

Письмова продукція

Складати анотації, реферати, технічні звіти, ділові листи та документи відповідно до стандартів фахового письма; здійснювати письмовий переклад технічної документації з/на німецьку мову.

03

Усна комунікація

Вести ділові переговори, презентувати результати технічних досліджень, брати участь у дискусіях на фахові теми, пов'язані із захистом інформації та кіберзагрозами, у форматі монологу та діалогу.

04

Робота з ресурсами

Орієнтуватися у фахових онлайн-ресурсах, термінологічних базах даних та нормативних документах ЄС (BSI, ENISA); ефективно використовувати електронні словники та корпусні інструменти для підготовки перекладів і академічних текстів.

МОДУЛЬ 1

Вступ до фахової німецької мови. Комп'ютерна інженерія та IT-термінологія

1

Тема 1.1

Фонетичні та граматичні особливості фахової німецької мови. Складні іменники в технічній термінології.

2

Тема 1.2

IT-системи та комп'ютерна архітектура: базова лексика. Читання та переклад описових технічних текстів.

3

Тема 1.3

Програмне забезпечення та операційні системи: функціональна термінологія. Вживання пасивних конструкцій у фахових текстах.

4

Тема 1.4

Комп'ютерні мережі: протоколи, топологія, мережеве обладнання. Анотування та реферування технічних статей.

МОДУЛЬ 1 · ТЕМА 1.1

Фонетичні та граматичні особливості фахової мови

Практичне заняття (15 год.)

Заняття 1–2: Вимова та артикуляційні особливості фахових термінів. Складні іменники (Komposita): структура, словотвір, переклад. Відмінювання іменників у фахових конструкціях. Артиклі у технічних текстах.

Заняття 3–4: Речення з пасивним станом (Passiv): утворення, значення, вживання в описах технічних процесів. Інфінітивні конструкції. Атрибутивні звороти.

Заняття 5: Читання та переклад тексту «Grundlagen der Informatik» — виявлення структури тексту, ключових термінів, причинно-наслідкових зв'язків.

Ключові питання

- Структура складних іменників та стратегії їх перекладу
- Пасивний стан у науково-технічних описах
- Граматичні конструкції для характеристики обладнання
- Основні фонетичні труднощі для україномовних студентів

Самостійна робота (15 год.)

Завдання 1. Опрацювання підручника: Вяхк І.А., Степанова І.С. «Німецька мова за професійним спрямуванням» — розділ «Граматичні основи фахового тексту».

Завдання 2. Складання власного глосарію базових ІТ-термінів (мінімум 50 одиниць) з перекладом та прикладами вживання у реченнях.

Завдання 3. Виконання граматичних вправ на пасивний стан і складні іменники (за збірником вправ Корнєєвої Н.О., 2023).

Очікуваний результат: студент вміє ідентифікувати та перекладати складні іменники, граматично коректно вживати пасивні конструкції в технічних контекстах.

МОДУЛЬ 1 · ТЕМИ 1.2–1.4

IT-системи, програмне забезпечення та комп'ютерні мережі

Тема 1.2 — Комп'ютерна архітектура (15 год. практики)

Апаратне забезпечення ПК: процесор, пам'ять, периферійні пристрої. Читання технічних специфікацій. Тексти типу «Beschreibung» та «Anleitung». Порівняльні конструкції у фахових текстах.

СРС (15 год.): Переклад уривку з технічної специфікації. Опрацювання: Левченко О.П., Паращук І.Ю. «Фахова іноземна мова (німецька) для IT-спеціальностей» (2022) — розділ «Комп'ютерна техніка».

Тема 1.3–1.4 — ПЗ та мережі (15 год. практики)

Операційні системи: функції, класифікація, термінологія у текстах. Мережеві протоколи: TCP/IP, DNS, HTTP/HTTPS. Топологія мереж. Реферування фахової статті з журналу «Datenschutz und Datensicherheit».

СРС (15 год.): Складання порівняльної таблиці «Операційні системи: функції та архітектура» на основі оригінальних текстів. Опрацювання: Когут У.П. «Практичний курс ділової німецької мови» (2023) — розділ «Мережеві технології».

МОДУЛЬ 2

Інформаційна безпека та захист даних: базова термінологія

Тема 2.1

Поняття «Informationssicherheit» та «Datenschutz»: розмежування термінів. Основні загрози та вразливості ІКС.

Тема 2.2

Класифікація кіберзагроз: шкідливе ПЗ, фішинг, атаки типу DDoS. Читання аналітичних звітів BSI.

Тема 2.3

Методи захисту інформації: шифрування, автентифікація, авторизація. Термінологія криптографії.

Тема 2.4

Управління інцидентами інформаційної безпеки. Аналіз оригінальних звітів про кіберінциденти.

МОДУЛЬ 2 · ТЕМА 2.1

Інформаційна безпека та захист даних: ключові поняття

Практичне заняття (15 год.)

Заняття 1–2: Читання та аналіз тексту «Was ist Informationssicherheit?» (джерело: BSI Grundschutz-Kompendium). Розмежування понять: Informationssicherheit, Datenschutz, IT-Sicherheit, Cybersicherheit. Виявлення дефінітивних конструкцій у тексті.

Заняття 3–4: Класифікація загроз: malware, phishing, social engineering, zero-day. Переклад уривку з «BSI-Lagebericht 2023». Вправи на відтворення тексту за ключовими словами.

Заняття 5: Написання анотації до фахової статті про загрози ІБ. Усна презентація результатів (2–3 хв.).

Ключові питання

- Розмежування Informationssicherheit і Datenschutz
- Класифікація кіберзагроз за звітом BSI
- Дефінітивні та класифікаційні конструкції в тексті
- Стратегії перекладу термінів-інтернаціоналізмів

Самостійна робота (15 год.)

Завдання 1. Опрацювання: Науменко Л.П., Гончаренко А.І. «Практичний курс перекладу з ділової та фахової мови» (2023) — розділ «Технічний переклад».

Завдання 2. Переклад розділу «Bedrohungslandschaft» зі звіту ENISA Threat Landscape (поточний рік). Складання двомовного глосарію термінів кіберзагроз (мінімум 30 одиниць).

Завдання 3. Реферат: «Основні поняття інформаційної безпеки в сучасній фаховій лексиці німецькомовних країн».

Очікуваний результат: студент вміє перекладати та коментувати фахові тексти про інформаційну безпеку, правильно вживати ключові терміни галузі.

МОДУЛЬ 2 · ТЕМИ 2.2–2.4

Кіберзагрози, криптографія та управління інцидентами

Тема 2.2 — Кіберзагрози (15 год. практики)

Читання аналітичного звіту BSI «Die Lage der IT-Sicherheit in Deutschland». Переклад розділу про актуальні кіберзагрози. Робота зі скороченнями та абревіатурами в технічних документах. Кейс: аналіз опису реальної кібератаки (ransomware) з офіційного джерела.

СРС (15 год.): Опрацювання: Шовковська Г.С. «Інформаційні технології та кібербезпека: посібник з фахової іноземної мови» (2022). Підготовка аналітичної нотатки «Топ-5 кіберзагроз за даними BSI».

Теми 2.3–2.4 — Криптографія та інциденти (15 год. практики)

Терміни шифрування: symmetrische/asymmetrische Verschlüsselung, digitale Signatur, Public-Key-Infrastruktur. Читання технічних стандартів. Управління інцидентами: Incident-Response-Prozess, CERT, Notfallplan. Аналіз реального звіту про кіберінцидент (кейс-стаді).

СРС (15 год.): Переклад витягу з ISO/IEC 27001 (офіційна версія). Підготовка реферату «Криптографічні методи захисту інформації: аналіз фахового тексту».

МОДУЛЬ 3

Нормативно-правове регулювання у сфері захисту інформації (ЄС)

Тема 3.1

GDPR (Datenschutz-Grundverordnung): структура, ключові поняття, права суб'єктів даних. Переклад статей регламенту.

Тема 3.2

Директива NIS2: сфера застосування, вимоги до безпеки, обов'язки операторів. Фахова лексика директив ЄС.

Тема 3.3

BSI-Grundschutz: методологія, каталоги, заходи. Читання та структурування технічних рекомендацій.

Тема 3.4

Стандарти ISO/IEC 27000: огляд серії, структура, ключові вимоги. Порівняння з нормативними актами України.

МОДУЛЬ 3 · ТЕМА 3.1

GDPR: Datenschutz-Grundverordnung

Практичне заняття (15 год.)

Заняття 1–2: Структура GDPR: преамбула, розділи, статті. Читання та переклад Ст. 4 (Begriffsbestimmungen): personenbezogene Daten, Verantwortlicher, Auftragsverarbeiter, Einwilligung. Вправи на розпізнавання юридичних конструкцій.

Заняття 3–4: Права суб'єктів даних: Recht auf Auskunft, Recht auf Löschung, Recht auf Datenübertragbarkeit. Переклад витягів зі статей 15–22. Порівняння з законодавством України.

Заняття 5: Рольова гра «Консультація з питань GDPR»: діалог між технічним спеціалістом та DPO (Data Protection Officer) у форматі ситуативного спілкування.

Ключові питання

- Ключові поняття GDPR та їх точний переклад
- Права суб'єктів персональних даних за регламентом
- Юридичні конструкції в текстах ЄС
- Відмінності між GDPR та Законом України «Про захист персональних даних»

Самостійна робота (15 год.)

Завдання 1. Опрацювання: Харченко В.С., Михайленко Т.О. «Юридично-технічна термінологія: посібник з перекладу для студентів IT-спеціальностей» (2023) — розділ «Нормативні акти ЄС».

Завдання 2. Переклад Ст. 32 GDPR «Sicherheit der Verarbeitung» та підготовка коментаря щодо технічних заходів захисту.

Завдання 3. Аналітична записка: «GDPR у роботі IT-підприємств: ключові вимоги та наслідки порушень».

Очікуваний результат: студент вміє перекладати та коментувати статті GDPR, орієнтується у правах суб'єктів даних та вимогах до технічного захисту.

МОДУЛЬ 3 · ТЕМИ 3.2–3.4

NIS2, BSI-Grundschutz та стандарти ISO/IEC 27000

Тема 3.2 — Директива NIS2 (15 год. практики)

Сфера застосування директиви NIS2 та її відмінності від NIS1. Обов'язкові суб'єкти (wesentliche und wichtige Einrichtungen). Вимоги до управління ризиками та звітування про інциденти. Читання та структурування статей директиви. Переклад Ст. 21 «Maßnahmen zum Risikomanagement».

СРС (15 год.): Опрацювання: Бойко Н.І. «Сучасна ділова іноземна мова: теорія і практика» (2024) — розділ «Право ЄС в IT-сфері».

Теми 3.3–3.4 — BSI та ISO (15 год. практики)

BSI-Grundschutz IT-Grundschutz-Methodik: баулауштайне, абсіхерунгсмасснамен. Читання структурованих технічних рекомендацій. Стандарти ISO 27001, 27002, 27005: сфера застосування, структура вимог, реалізація в організаціях. Порівняльний аналіз підходів BSI та ISO.

СРС (15 год.): Підготовка реферату «Порівняльний аналіз методологій BSI-Grundschutz та ISO/IEC 27001 як основи захисту інформації». Укладання глосарію стандартів.

МОДУЛЬ 4

Ділова комунікація у сфері IT та захисту інформації

Тема 4.1

Ділова кореспонденція: структура ділового листа, запит, відповідь на запит, рекламація в IT-контексті.

Тема 4.2

Технічні звіти та документація: структура Technischer Bericht, Sicherheitsaudit-Bericht, Risikoanalyse.

Тема 4.3

Резюме та супровідний лист для IT-компаній у DACH-регіоні. Особливості ринку праці у сфері кібербезпеки.

Тема 4.4

Ведення переговорів та нарад у сфері IT-безпеки. Презентація технічних рішень. Мова телефонних розмов та відеоконференцій.

МОДУЛЬ 4 · ТЕМА 4.1

Ділова кореспонденція в IT-середовищі

Практичне заняття (15 год.)

Заняття 1–2: Структура ділового листа за DIN 5008. Формули звертання та завершення листа. Типи листів: Anfrage (запит), Angebot (пропозиція), Bestellung (замовлення), Reklamation (рекламація). Аналіз зразків.

Заняття 3–4: Написання ділового листа-запиту щодо послуг з кібербезпеки. Відповідь на запит із технічними деталями. Редагування та коригування листів. Peer-review у парах.

Заняття 5: Ділова електронна переписка: Email-Etikette, формат і стиль. Написання Email-ланцюжка з питань технічного аудиту безпеки.

Самостійна робота (15 год.)

Завдання 1. Опрацювання: Когут У.П. «Практичний курс ділової німецької мови» (2023) — розділ «Ділова кореспонденція»; виконання вправ на написання листів за шаблонами та з опорою на ситуативні завдання.

Завдання 2. Написання повного комплекту документів: запит ↔️ відповідь ↔️ рекламація у ситуації «Придбання програмного забезпечення для захисту корпоративної мережі».

Завдання 3. Укладання власного шаблону ділового листа з поясненням усіх обов'язкових елементів.

Очікуваний результат: студент вміє складати ділові листи різних жанрів відповідно до норм DIN 5008, правильно добираючи стиль і формули ввічливості.

МОДУЛЬ 4 · ТЕМИ 4.2–4.4

Технічні звіти, резюме та ділові переговори

Тема 4.2 — Технічні звіти (15 год. практики)

Структура Sicherheitsaudit-Bericht: Zusammenfassung, Methodik, Befunde, Empfehlungen. Аналіз зразка звіту про аудит. Написання розділу «Risikobewertung». Логічний зв'язок між частинами звіту. Академічний стиль та об'єктивність.

СРС (15 год.): Написання мінізвіту з аналізу вразливостей уявної корпоративної мережі на основі наданого шаблону. Опрацювання: Харченко В.С., Михайленко Т.О. «Юридично-технічна термінологія» (2023).

Теми 4.3–4.4 — Резюме та переговори (15 год. практики)

Lebenslauf (табличний та суцільний): структура, обов'язкові елементи, фото. Anschreiben до IT-компанії DACH-регіону. Підготовка до співбесіди: Stärken-Schwächen-Analyse. Переговори: аргументація, поступки, підсумовування. Презентація технічного рішення (захист системи) у форматі 5 хв.

СРС (15 год.): Складання власного Lebenslauf та Anschreiben для конкретної вакансії «IT-Security Analyst» у реальній або змодельованій компанії. Підготовка тез для презентації.

МОДУЛЬ 5

Технічний переклад у сфері захисту інформації

Тема 5.1

Теорія та практика технічного перекладу: стратегії, труднощі, інструменти. Перекладацькі трансформації в IT-текстах.

Тема 5.2

Переклад стандартів та нормативної документації: ISO, BSI, ENISA. Специфіка мови стандартів.

Тема 5.3

Переклад науково-технічних статей із журналів «Datenschutz und Datensicherheit», «IT-Security». Реферативний переклад.

Тема 5.4

Комп'ютерні засоби перекладу (CAT-tools): DeepL, SDL Trados, термінологічні бази. Постредагування МП-перекладів.

МОДУЛЬ 5 · ТЕМА 5.1

Стратегії та трансформації технічного перекладу

Практичне заняття (15 год.)

Заняття 1–2: Поняття еквівалентності та адекватності у технічному перекладі. Перекладацькі трансформації: калькування, транскрипція, описовий переклад, генералізація/конкретизація. Вправи на перетворення складних термінологічних конструкцій.

Заняття 3–4: Переклад уривку з технічної документації щодо налаштування міжмережевого екрана (Firewall-Konfigurationshandbuch). Аналіз труднощів: багатокомпонентні терміни, скорочення, неологізми.

Заняття 5: Порівняльний аналіз двох перекладів одного тексту: виявлення помилок, обговорення альтернатив. Укладання рекомендацій із перекладу конкретного жанру.

Самостійна робота (15 год.)

Завдання 1. Опрацювання: Науменко Л.П., Гончаренко А.І. «Практичний курс перекладу з ділової та фахової мови» (2023) — розділ «Технічний переклад: стратегії та труднощі».

Завдання 2. Письмовий переклад 1500 знаків фахового тексту з коментарями до прийнятих перекладацьких рішень (портфоліо-завдання).

Завдання 3. Укладання термінологічного міні-словника з 40 термінів (DE–UA) у сфері технічного захисту інформації.

Очікуваний результат: студент вміє застосовувати перекладацькі трансформації, аргументувати власний перекладацький вибір та редагувати переклади технічних текстів.

МОДУЛЬ 5 · ТЕМИ 5.2–5.4

Переклад стандартів, наукових статей та CAT-tools

Теми 5.2–5.3 — Стандарти та статті (15 год. практики)

Специфіка мови стандартів: модальні дієслова müssen/sollen/dürfen у вимогах, нумерація, cross-references. Переклад уривків ISO/IEC 27002 «Informationssicherheitskontrollen». Реферативний переклад статті з «Datenschutz und Datensicherheit» (DuD): складання структурованого реферату обсягом 250 слів.

СРС (15 год.): Підготовка реферативного перекладу повної наукової статті (4–6 стор.) з визначеного викладачем фахового видання.

Тема 5.4 — CAT-tools (15 год. практики)

Практична робота з DeepL Pro та SDL Trados: завантаження документу, налаштування пам'яті перекладів (Translation Memory), термінологічна база (Termbase). Постредагування автоматичного перекладу фахового тексту: виявлення типових помилок МП. Оцінка якості за шкалою MQM.

СРС (15 год.): Виконання комплексного завдання: автоматичний переклад → постредагування → коментований звіт про внесені правки.

МОДУЛЬ 6

Читання та реферування наукових текстів з кібербезпеки

Тема 6.1

Структура наукової статті (IMRaD) у контексті інформаційної безпеки. Стратегії читання: skimming, scanning, reading in depth.

Тема 6.2

Академічне письмо: анотація, реферат, рецензія на наукову роботу. Особливості наукового стилю в німецькомовних публікаціях.

Тема 6.3

Читання та аналіз звітів ENISA про стан кібербезпеки в ЄС. Порівняльний аналіз ситуації в Україні та Європі.

Тема 6.4

Підготовка та захист реферату за тематикою захисту інформації в ІКС. Критерії оцінювання академічних текстів.

МОДУЛЬ 6 · ТЕМА 6.1

Структура та стратегії читання наукових текстів

Практичне заняття (15 год.)

Заняття 1–2: Структура IMRaD (Einleitung, Methoden, Ergebnisse, Diskussion) у статті про кібербезпеку. Читання вступу та висновків (skimming). Виявлення мети дослідження, гіпотези, методів за маркерами дискурсу.

Заняття 3–4: Детальне читання (reading in depth) статті «Sicherheitsanalyse von IoT-Systemen». Виявлення аргументативної структури. Вправи на знаходження інформації за запитом (scanning).

Заняття 5: Складання розширеної анотації до прочитаної статті (150–200 слів). Групова дискусія: «Які виклики кібербезпеки IoT розглядаються у статті?»

Ключові питання

- Структура IMRaD та маркери кожного розділу
- Відмінності між анотацією та рефератом
- Мовні засоби для вираження мети, методів та висновків
- Стратегії читання залежно від комунікативної задачі

Самостійна робота (15 год.)

Завдання 1. Опрацювання: Левченко О.П., Паращук І.Ю. «Фахова іноземна мова (німецька) для ІТ-спеціальностей» (2022) — розділ «Академічне письмо та реферування».

Завдання 2. Самостійне читання однієї наукової статті (обсяг 5–8 стор.) з визначеного переліку та складання структурованого конспекту за планом: тема → мета → методи → результати → висновки.

Завдання 3. Написання анотації (150 слів) та реферату (400 слів) до самостійно обраної статті з журналу «Informatik Spektrum» або «DuD».

Очікуваний результат: студент вміє структурувати свою роботу з науковим текстом, застосовувати різні стратегії читання та складати анотації й реферати відповідно до академічних стандартів.

МОДУЛЬ 6 · ТЕМИ 6.2–6.4

Академічне письмо, звіти ENISA та захист реферату

Теми 6.2–6.3 — Письмо та звіти (15 год. практики)

Написання рецензії (Rezension) на наукову статтю: структура, критерії оцінювання, мовні кліше. Звіти ENISA Threat Landscape: читання виконавчого резюме, аналіз статистики, виявлення тенденцій. Порівняльний аналіз загроз: ЄС та Україна у цифровому просторі. Підготовка таблиці «Топ-10 кіберзагроз за ENISA».

СРС (15 год.): Написання рецензії на одну зі статей, прочитаних у модулі 6.1–6.2. Опрацювання: Бойко Н.І. «Сучасна ділова іноземна мова» (2024) — розділ «Академічні жанри».

Тема 6.4 — Захист реферату (15 год. практики)

Написання та оформлення наукового реферату (Fachreferat, 8–10 стор.) за самостійно обраною темою з галузі захисту інформації. Підготовка презентації (10 слайдів). Захист перед групою: усний виступ 7–10 хв., відповіді на запитання.

СРС (15 год.): Фінальне редагування та оформлення реферату відповідно до вимог (цитування, список літератури, титульна сторінка). Підготовка усного виступу та відповідей на можливі запитання.

МОДУЛЬ 7

Усна комунікація та презентації в IT-середовищі

Тема 7.1

Структура публічного виступу та наукової доповіді. Мовні кліше для вступу, переходів та завершення.

Тема 7.2

Презентація технічного рішення у сфері кібербезпеки. Використання наочності та технічних схем при виступі.

Тема 7.3

Дискусія та аргументація: стратегії переконання, вираження згоди/незгоди, запит уточнень у фаховому контексті.

Тема 7.4

Ділові переговори та технічні наради (Besprechung): порядок денний, протокол, підведення підсумків. Рольові ігри.

МОДУЛЬ 7 · ТЕМА 7.1

Структура та мовне оформлення публічного виступу

1

Вступ (Einleitung)

Привітання, формулювання теми та мети, анонс структури, залучення аудиторії.

2

Основна частина (Hauptteil)

Логічна послідовність аргументів, зв'язкові фрази, посилання на джерела, ілюстрація прикладами.

3

Висновки (Schluss)

Резюмування ключових тез, висновок, заклик до дії або постановка питань для дискусії.

4

Q&A-сесія

Відповіді на запитання: прийом, перефразування, чітка відповідь або коректне відхилення.

Практичне заняття (15 год.)

Аналіз структури зразкових доповідей. Відпрацювання кліше для кожного етапу виступу. Мікропрезентації (3 хв.) за темами: «Актуальні кіберзагрози», «Технологія VPN», «Двофакторна автентифікація». Взаємне рецензування за чітко визначеними критеріями.

Самостійна робота (15 год.)

Опрацювання: Когут У.П. «Практичний курс ділової німецької мови» (2023) — розділ «Презентація та доповідь». Підготовка повноцінної презентації (10 слайдів) на тему «Захист персональних даних у сучасних ІКС» для виступу в модулі 7.2.

МОДУЛЬ 7 · ТЕМИ 7.2–7.4

Технічні презентації, дискусія та ділові переговори

Теми 7.2–7.3 — Презентація та дискусія (15 год. практики)

Захист технічної презентації (підготовленої у 7.1): виступ 7–10 хв. з демонстрацією слайдів. Відповіді на технічні запитання аудиторії. Дискусія: Für- und Contra-Argumente щодо актуальних питань кібербезпеки (зокрема: «Чи є повна анонімність в Інтернеті можливою і бажаною?»).

СРС (15 год.): Опрацювання: Бойко Н.І. «Сучасна ділова іноземна мова» (2024) — розділ «Дискусія та аргументація». Підготовка аргументованої позиції для наступного заняття.

Тема 7.4 — Ділові наради (15 год. практики)

Рольова гра «Засідання комітету з ІБ»: розподіл ролей (голова, технічний директор, юрист, DPO), розгляд порядку денного, прийняття рішень щодо усунення вразливостей. Написання протоколу наради (Sitzungsprotokoll). Підведення підсумків модуля.

СРС (15 год.): Підготовка власного Sitzungsprotokoll на основі запису або транскрипту ділової наради. Самооцінювання комунікативних умінь за портфоліо-листом.

МОДУЛЬ 8

Сучасні виклики кібербезпеки: мовний та фаховий аспект

Тема 8.1

Штучний інтелект у кібербезпеці: можливості та ризики. Читання та переклад актуальних публікацій BSI та ENISA.

Тема 8.2

Захист критичної інформаційної інфраструктури (KRITIS): правове регулювання, технічні вимоги, мовне оформлення документів.

Тема 8.3

Хмарна безпека (Cloud Security) та DSGVO: аналіз вимог до хмарних провайдерів у контексті захисту персональних даних.

Тема 8.4

Підсумковий проект: комплексний аналіз фахового тексту, переклад, усний захист. Підсумкове узагальнення курсу.

МОДУЛЬ 8 · ТЕМА 8.1

Штучний інтелект у кібербезпеці: мовний аспект

Практичне заняття (15 год.)

Заняття 1–2: Читання публікації BSI «Künstliche Intelligenz — Chancen und Risiken für die Cybersicherheit» (2023). Виявлення ключових тверджень. Лексика: maschinelles Lernen, neuronale Netze, adversarial attacks, deepfake. Переклад уривку з коментарями.

Заняття 3–4: Аналіз звіту ENISA про застосування ШІ в кіберзахисті. Реферат за прочитаним (250 слів). Дискусія: «Чи є ШІ більшою загрозою чи засобом захисту в кіберпросторі?».

Заняття 5: Написання аргументативного есе (300 слів) «KI als Sicherheitsrisiko oder Schutzwerkzeug: eine Abwägung».

Самостійна робота (15 год.)

Завдання 1. Опрацювання: Шовковська Г.С. «Інформаційні технології та кібербезпека: посібник з фахової іноземної мови» (2022) — розділ «Штучний інтелект та захист даних».

Завдання 2. Читання та конспектування оригінальної статті з журналу «Informatik Spektrum» або «DuD» за темою ШІ та кібербезпеки.

Завдання 3. Підготовка до підсумкового проекту (тема 8.4): вибір тексту, попередній переклад, укладання глосарію.

Очікуваний результат: студент вміє читати та аналізувати актуальні фахові тексти про ШІ та кібербезпеку, висловлювати аргументовану позицію письмово та усно.

МОДУЛЬ 8 · ТЕМИ 8.2–8.4

KRITIS, хмарна безпека та підсумковий проект

Теми 8.2–8.3 — KRITIS та Cloud Security (15 год. практики)

Захист критичної інфраструктури: Gesetz zur Umsetzung der NIS2-Richtlinie (2023/2024). Перелік KRITIS-секторів. Переклад та аналіз технічних вимог. Хмарна безпека та DSGVO: вимоги до хмарних договорів (Auftragsverarbeitungsvertrag). Кейс: вибір хмарного провайдера для корпоративної системи захисту.

СРС (15 год.): Підготовка аналітичної записки «Вимоги до хмарних провайдерів за DSGVO та NIS2: порівняльний аналіз».

Тема 8.4 — Підсумковий проект (15 год. практики)

Комплексний проект: (1) вибір оригінального фахового тексту (8–10 стор.) з тематики захисту інформації, (2) письмовий переклад з перекладацьким коментарем, (3) підготовка анотації та реферату, (4) усний захист перед комісією (10 хв. виступ + 5 хв. Q&A). Фінальне узагальнення курсу: компетентності та перспективи.

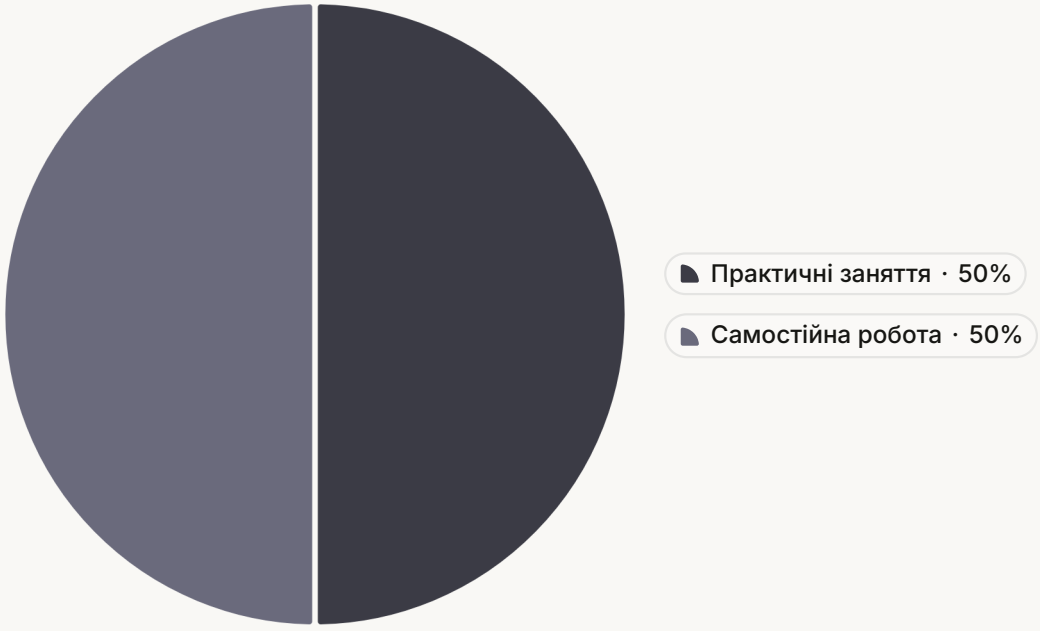
СРС (15 год.): Остаточне оформлення підсумкового проекту. Самостійна рефлексія над розвитком мовних компетентностей упродовж курсу (learning diary).

Розподіл навчального часу — 240 годин

Модуль	Тема	Практичні (год.)	СРС (год.)	Зміст
Модуль 1	Теми 1.1–1.4	15+15	15+15	IT-термінологія, мережі, ПЗ
Модуль 2	Теми 2.1–2.4	15+15	15+15	Інформаційна безпека, кіберзагрози
Модуль 3	Теми 3.1–3.4	15+15	15+15	GDPR, NIS2, BSI, ISO/IEC 27000
Модуль 4	Теми 4.1–4.4	15+15	15+15	Ділова комунікація, резюме, переговори
Модуль 5	Теми 5.1–5.4	15+15	15+15	Технічний переклад, CAT-tools
Модуль 6	Теми 6.1–6.4	15+15	15+15	Читання, реферування, захист реферату
Модуль 7	Теми 7.1–7.4	15+15	15+15	Усна комунікація, презентації
Модуль 8	Теми 8.1–8.4	15+15	15+15	ШІ, KRITIS, підсумковий проект
Разом	**32 теми (8 модулів)**	**120**	**120**	**Загалом: 240 год. / 8 кредитів**

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

Структура навчального часу



Коментар до розподілу

Загальний обсяг — **240 годин (8 кредитів ЄКТС)** — розподілено між двома формами роботи для забезпечення балансу між аудиторною практикою та самостійним опрацюванням.

Практичні заняття — 120 год. (50%)

Відпрацювання мовних навичок, переклад текстів, аналіз нормативних документів, рольові ігри, кейс-стаді, захист проектів і рефератів. Практична спрямованість забезпечує формування активних комунікативних та перекладацьких умінь.

Самостійна робота — 120 год. (50%)

Поглиблене вивчення лексики, виконання перекладів, написання академічних текстів, робота з онлайн-ресурсами та фаховою літературою. Самостійна робота **становить 50% обсягу дисципліни**.

Самостійна робота студентів — Детальний опис

Опрацювання літератури

Поглиблене вивчення теоретичного та практичного матеріалу за посібниками з фахової німецької мови (Вяхк, Левченко, Когут, Бойко та ін.), нормативними актами ЄС, звітами BSI та ENISA. Студент конспектує ключові лексичні одиниці, виконує вправи та порівнює термінологічні рішення різних авторів.

Індивідуальні завдання

Виконання письмових перекладів (1 000–2 000 знаків) з коментарями; написання анотацій, рефератів, ділових листів та аналітичних записок; ведення глосаріїв фахових термінів; підготовка есе на актуальні теми кібербезпеки.

Робота з інформаційними ресурсами

Опрацювання офіційних сайтів: BSI (**bsi.bund.de**), ENISA (**enisa.europa.eu**), GDPR-повний текст (**gdpr-info.eu**), Informatik Spektrum (**springer.com**). Використання CAT-tools та термінологічних баз (IATE, DeepL).

Підготовка до занять та контролю

Підготовка до практичних занять (попереднє читання текстів, виконання підготовчих вправ); підготовка до тестувань (лексика, граматика, переклад); підготовка до контрольних робіт за кожним модулем (систематизація знань, типові завдання).

Форми контролю знань

1	2	3
Поточний контроль	**Проміжний контроль**	**Підсумковий контроль**
Виконання практичних завдань та тестування за темами кожного змістовного модуля. Оцінюються якість перекладу, лексична точність, граматична коректність та комунікативна активність. Поточний контроль формує накопичувальну оцінку протягом семестру. Проводиться після кожної теми у формі тестування (10–15 питань), усного опитування або письмового завдання.	Комплексне модульне завдання — переклад фахового тексту з коментарями або захист реферату, що охоплює теми відповідного змістовного модуля. Оцінюються повнота виконання, термінологічна точність, аргументованість та якість усного захисту. Проводиться після завершення кожного з 8 модулів.	Іспит відповідно до навчального плану. Форма — комплексне завдання: письмовий переклад тексту (1 000 знаків) + виконання лексико-граматичного тесту + усна відповідь. Підсумкова оцінка враховує результати поточного, проміжного та підсумкового контролю відповідно до встановленої шкали: **100-бальна система** з переведенням у національну шкалу та ЄКТС (A, B, C, D, E, FX, F).

Методи викладання

Викладання дисципліни «Фахова німецька мова» поєднує сучасні комунікативні та інтерактивні методи, що забезпечує формування як практичних мовних навичок, так і фахової компетентності у сфері захисту інформації, необхідної для майбутньої професійної діяльності бакалавра з комп'ютерної інженерії.

Читання та аналіз

Опрацювання оригінальних фахових текстів (BSI, ENISA, ISO, GDPR); формування навичок критичного читання та виявлення ключових ідей.

Переклад

Письмовий та усний переклад технічних текстів, нормативних документів та наукових статей; формування перекладацьких компетентностей та термінологічної культури.

Кейс-стаді

Аналіз реальних ситуацій кіберінцидентів, нормативних вимог та технічних рішень; студенти виявляють проблему, пропонують рішення та обґрунтовують висновки мовою оригіналу.

Дискусії та рольові ігри

Моделювання ситуацій ділового спілкування: переговори, наради, захист проектів; розвиток критичного мислення, аргументації та усного мовлення.

Самостійне дослідження

Підготовка перекладів, анотацій, рефератів та аналітичних записок за самостійно обраними текстами; розвиток навичок пошуку і систематизації фахової інформації.

Цифрові інструменти

Практична робота з CAT-tools (DeepL, SDL Trados), термінологічними базами (IATE, TERMDAT), фаховими корпусами; розвиток цифрових компетентностей перекладача та фахівця з ІБ.

Усі методи спрямовані на формування компетентностей, передбачених ОП «Організація захисту інформації в ІКС» спеціальності 123 «Комп'ютерна інженерія».

Рекомендована література — Підручники та посібники (2022–2024 рр.)

1. Вяхк І.А., Степанова І.С.
Німецька мова за професійним спрямуванням: навч. посіб. для студентів ІТ-спеціальностей ЗВО. — Київ : Центр учбової літератури, 2022. — 240 с.

2. Когут У.П.
Практичний курс ділової німецької мови: навч.-метод. посіб. — Луцьк : Волинський національний університет ім. Лесі Українки, 2023. — 196 с.

3. Левченко О.П., Паращук І.Ю.
Фахова іноземна мова (німецька) для ІТ-спеціальностей: навч. посіб. — Львів : Видавництво Львівської політехніки, 2022. — 224 с.

4. Бойко Н.І.
Сучасна ділова іноземна мова: теорія і практика: навч. посіб. для студентів технічних ЗВО. — Харків : НТУ «ХПІ», 2024. — 210 с.

5. Науменко Л.П., Гончаренко А.І.
Практичний курс перекладу з ділової та фахової мови (німецька — українська): навч. посіб. — Вінниця : Нова книга, 2023. — 304 с.

6. Шовковська Г.С.
Інформаційні технології та кібербезпека: посібник з фахової іноземної мови (німецька): навч.-метод. посіб. — Київ : КПІ ім. Ігоря Сікорського, 2022. — 178 с.

7. Харченко В.С., Михайленко Т.О.
Юридично-технічна термінологія: посібник з перекладу для студентів ІТ-спеціальностей. — Дніпро : ДДУВС, 2023. — 192 с.

8. Корнєєва Н.О.
Збірник вправ з граматики фахової німецької мови для студентів технічних спеціальностей: навч.-метод. посіб. — Запоріжжя : ЗНУ, 2023. — 148 с.

Додаткова література та фахові ресурси

9. Козак Л.В., Федорів Я.Р.

Українсько-німецький термінологічний словник з комп'ютерних технологій та інформаційної безпеки. — Тернопіль : ТНТУ ім. І. Пулюя, 2023. — 256 с. *Рекомендується до всіх модулів курсу.*

10. Олійник М.В., Петренко С.І.

Академічне письмо іноземною мовою для технічних спеціальностей: навч. посіб. — Київ : Академвидав, 2023. — 220 с. *Рекомендується для модулів 5–6.*

11. BSI — Bundesamt für Sicherheit in der Informationstechnik

Die Lage der IT-Sicherheit in Deutschland 2023. — Bonn : BSI, 2023. — 120 S. Доступно: **bsi.bund.de**. *Рекомендується для модулів 2, 3, 8.*

12. ENISA — European Union Agency for Cybersecurity

ENISA Threat Landscape 2023. — Heraklion : ENISA, 2023. Доступно: **enisa.europa.eu**. *Рекомендується для модулів 2, 6, 8.*

Нормативно-правова база

→ Verordnung (EU) 2016/679 — DSGVO (GDPR)

Datenschutz-Grundverordnung. Офіційний текст ЄС про захист фізичних осіб у зв'язку з обробкою персональних даних. **gdpr-info.eu**

→ Richtlinie (EU) 2022/2555 — NIS2

Директива про заходи щодо забезпечення високого загального рівня кібербезпеки в Союзі. **eur-lex.europa.eu**

→ ISO/IEC 27001:2022

Міжнародний стандарт систем управління інформаційною безпекою. Оригінальний текст доступний через ISO. **iso.org**

→ Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI

Основний нормативний акт України у сфері захисту персональних даних. **zakon.rada.gov.ua**

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

Визначає правові та організаційні основи забезпечення кібербезпеки України. **zakon.rada.gov.ua**

Офіційні ресурси та фахові видання

BSI — Bundesamt für Sicherheit

bsi.bund.de — офіційні звіти, рекомендації, IT-Grundschutz-Kompendium, публікації з актуальних кіберзагроз.

ENISA

enisa.europa.eu — щорічні звіти про загрози, аналітика, стандарти кібербезпеки ЄС, доступні для навчального опрацювання.

GDPR повний текст

gdpr-info.eu — зручний інтерфейс для читання статей DSGVO з гіперпосиланнями та офіційними мовними версіями.

Держспецзв'язку України

cip.gov.ua — офіційний сайт Державної служби спеціального зв'язку та захисту інформації України.

Журнал «Datenschutz und Datensicherheit» (DuD)

springer.com — провідне фахове видання з питань захисту даних та інформаційної безпеки у DACH-регіоні.

Журнал «Informatik Spektrum»

springer.com — журнал Gesellschaft für Informatik, публікує наукові та оглядові статті з IT та кібербезпеки.

Термінологічна база IATE (EU)

iate.europa.eu — офіційна міжінституційна термінологічна база ЄС, незамінний ресурс для перекладу нормативних актів.

Міністерство освіти і науки України

mon.gov.ua — освітні стандарти, навчальні програми, методичні матеріали для ЗВО.

Зв'язок дисципліни зі спеціальністю 123 «Комп'ютерна інженерія» (ОП: Організація захисту інформації в ІКС)

Чому «Фахова німецька мова» для фахівців з ІБ?

Дисципліна «Фахова німецька мова» є невід'ємною складовою підготовки бакалаврів зі спеціальністю 123 «Комп'ютерна інженерія» (ОП «Організація захисту інформації в ІКС»). Знання фахової мови відкриває доступ до першоджерел нормативного регулювання ЄС — GDPR, NIS2, BSI-Grundschutz — у оригіналі.

DACH-регіон (Німеччина, Австрія, Швейцарія) є одним із лідерів у розробці стандартів і технологій кібербезпеки. Партнерство з компаніями та установами цього регіону потребує прямої мовної компетентності, не обмеженої перекладами.

Практичне значення для майбутньої кар'єри

- Читання оригінальних технічних стандартів BSI, ISO та директив ЄС без посередників
- Можливість стажування та працевлаштування в IT та ІБ-компаніях DACH-регіону
- Участь у міжнародних проектах, конференціях та дослідженнях кібербезпеки
- Ведення технічної документації та ділового листування для міжнародних партнерів
- Критичне читання аналітики BSI/ENISA для прийняття обґрунтованих рішень у сфері ІБ
- Конкурентна перевага на ринку праці у сфері кібербезпеки та захисту інформації

Ключові компетентності курсу — Підсумок

Курс охоплює всі ключові аспекти фахової німецької мови у сфері захисту інформації — від базової IT-термінології до перекладу нормативних актів ЄС та усного захисту технічних проектів — і формує у студентів цілісну комунікативну та перекладацьку компетентність, необхідну для успішної міжнародної кар'єри у сфері кібербезпеки.

Бажаємо успіхів у вивченні Фахової німецької мови!

240

Годин

Загальний обсяг дисципліни

8

Кредити ЄКТС

Відповідно до стандарту

8

Модулів

Змістовних блоків курсу

8

Джерел

Рекомендованої літератури 2022–2024 рр.

> «Wer fremde Sprachen nicht kennt, weiß nichts von seiner eigenen.» — Johann Wolfgang von Goethe
> «Хто не знає іноземних мов, той нічого не знає про свою власну.» — Йоганн Вольфганг фон Ґете

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