Силабус дисципліни «Фахова німецька мова»

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

240

Годин загальний обсяг дисципліни

8

Кредитів ЄКТС відповідно до стандарту

8

Змістовних модулі 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 занять: 120 годин

Самостійна робота: 120 годин

Модулів: 8 змістовних блоки курсу

Мета дисципліни

Дисципліна «Фахова німецька мова» формує у студентів спеціальності «Комп'ютерна інженерія» систему знань, умінь і навичок у сфері іншомовної професійної комунікації з урахуванням специфіки галузі захисту інформації в інформаційно-комунікаційних системах. Курс спрямований на опанування німецькомовної фахової термінології у сфері кібербезпеки, комп'ютерних мереж та захисту інформації, розвиток навичок читання та перекладу технічної документації, а також усного та письмового спілкування в професійному контексті.

Форми навчання

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

Компетентності та результати навчання

Загальні компетентності

Здатність до аналізу, синтезу та критичного оцінювання фахової інформації у сфері кібербезпеки та захисту інформації, представленої німецькою мовою: виявлення суттєвих технічних вимог, порівняння нормативних і стандартизаційних підходів, формування обґрунтованих висновків. Уміння самостійно навчатися, планувати роботу та організовувати виконання мовних завдань у визначені строки, зокрема під час підготовки перекладів технічних текстів, анотацій та фахових презентацій.

Здатність до усної та письмової фахової комунікації німецькою мовою: чітко формулювати технічні вимоги, аргументовано обговорювати питання інформаційної безпеки та захисту даних. Відповідальність, ініціативність, дисциплінованість та готовність працювати в команді під час виконання комунікативних завдань.

- Аналізувати технічні тексти та нормативну документацію з ІБ німецькою мовою
- Планувати власну мовну діяльність і дотримуватися дедлайнів
- Коректно спілкуватися у фаховому контексті
- Брати участь у командній роботі та презентації результатів

Фахові компетентності

Розуміння системи фахової термінології у сфері комп'ютерної інженерії та захисту інформації в ІКС відповідно до стандартів і нормативних документів, виданих у німецькомовних країнах. Знання ключових понять, пов'язаних з кібербезпекою, мережевим захистом, шифруванням та управлінням інформаційними ризиками в контексті підготовки до роботи з міжнародними партнерами.

Здатність застосовувати мовні навички для роботи з технічною документацією, стандартами (зокрема BSI — Bundesamt für Sicherheit in der Informationstechnik), науковими публікаціями та звітами про інциденти ІБ, виданими у ФРН, Австрії та Швейцарії.

- Читати та перекладати фахові тексти з ІБ та комп'ютерних мереж
- Вести ділове листування та складати технічні документи
- Застосовувати фахову термінологію у сфері захисту інформації
- Здійснювати усну презентацію результатів фахових досліджень
- Розуміти та аналізувати стандарти BSI та документи DSGVO

Результати навчання

Після успішного завершення курсу студент повинен демонструвати такі результати навчання:

1

Знання та розуміння

Пояснювати сутність ключових понять фахової німецької мови у сфері ІКС: Datensicherheit, Informationssicherheit, Netzwerkschutz, Verschlüsselung, Firewall, Datenschutz, Cyberangriff, Authentifizierung. Характеризувати структуру та особливості функціонування фахового стилю технічної документації в німецькомовному середовищі.

2

Аналіз та оцінювання

Аналізувати технічні тексти, стандарти та нормативні документи з погляду вимог інформаційної безпеки, виявляти ключову термінологію та структурні особливості. Оцінювати рівень власного розуміння фахових текстів та визначати прогалини у знаннях технічної лексики.

3

Застосування знань

Застосовувати знання граматики і лексики при перекладі технічної документації, складанні ділових листів та анотацій до наукових публікацій з тематики захисту інформації в ІКС. Здійснювати усне спілкування у фаховому контексті: участь у семінарах, конференціях, технічних переговорах.

4

Комунікація та рефлексія

Аргументовано викладати власну позицію щодо технічних рішень у галузі захисту інформації в ІКС у форматі фахових дискусій, презентацій та письмових повідомлень. Формувати професійну відповідальність і готовність до міжнародного співробітництва у сфері кібербезпеки.

Модуль 1. Вступ до фахової мови. Комп'ютерна інженерія та IT-галузь

ЗМІСТОВНИЙ МОДУЛЬ 1

Тема 1.1

Фахова мова у сфері комп'ютерних технологій. Поняття та особливості фахової (технічної) мови. Відмінності між загальновживаною та фаховою лексикою. Структура фахового тексту в IT-галузі. Основна термінологія: Computer, Software, Hardware, System, Netzwerk, Programmierung. Стильові особливості технічної документації.

Тема 1.2

Граматичний мінімум для читання технічних текстів. Повторення граматичних основ: відмінювання іменників, дієслівні форми Präsens/Präteritum/Perfekt у технічних текстах. Складні іменники (Komposita) як особливість технічної мови: Datensicherheitssystem, Netzwerkschutzprotokoll. Пасивні конструкції у технічних описах і специфікаціях.

Тема 1.3

Структура комп'ютерних систем і мереж. Читання та переклад текстів про архітектуру комп'ютерних систем, мережеву топологію, протоколи передачі даних (TCP/IP, HTTP, FTP). Ключова лексика: Betriebssystem, Prozessor, Arbeitsspeicher, Übertragungsprotokoll, Netzwerktopologie. Вправи на переклад технічних описів.

Тема 1.4

IT-спеціаліст на ринку праці Німеччини. Лексика для пошуку роботи та ділового спілкування. Складання резюме (Lebenslauf) та супровідного листа для IT-компаній. Аналіз оголошень про вакансії у сфері Informationssicherheit, IT-Sicherheit, Cybersecurity. Ділова кореспонденція: структура та мовні кліше.

Модуль 2. Інформаційна безпека: основи та термінологія

ЗМІСТОВНИЙ МОДУЛЬ 2

Тема 2.1

Grundlagen der Informationssicherheit. Базова термінологія інформаційної безпеки: Vertraulichkeit, Integrität, Verfügbarkeit (CIA-Triade). Загрози ІБ: Bedrohung, Risiko, Schwachstelle, Angriff. Читання та переклад вступних розділів стандарту BSI IT-Grundschutz. Обговорення ключових понять у форматі діалогу.

Тема 2.2

Кіберзагрози та методи захисту. Лексика для опису кіберзагроз: Malware, Ransomware, Phishing, DDoS-Angriff, Social Engineering, Zero-Day-Exploit. Класифікація загроз та заходи захисту. Читання аутентичних текстів з порталу BSI. Вправи на перефразування та реферування технічних описів кіберінцидентів.

Тема 2.3

Захист персональних даних. DSGVO. Ключові положення Datenschutz-Grundverordnung (DSGVO): Personenbezogene Daten, Einwilligung, Datenschutzbeauftragter, Datenpanne, Betroffenenrechte. Порівняння DSGVO з українським законодавством про захист персональних даних. Переклад витягів з регламенту.

Модуль 3. Мережева безпека та криптографія

ЗМІСТОВНИЙ МОДУЛЬ 3

Тема 3.1

Netzwerksicherheit — безпека мереж. Термінологія мережевої безпеки: Firewall, VPN, Intrusion Detection System, Authentifizierung, Autorisierung, Verschlüsselung. Читання технічних описів конфігурацій захисту мереж. Порівняльний аналіз понять: Datensicherung vs. Datensicherheit. Переклад технічних специфікацій.

Тема 3.2

Kryptographie — основи криптографії. Фахова лексика: symmetrische/asymmetrische Verschlüsselung, digitale Signatur, Public-Key-Infrastruktur, Zertifikat, Hash-Funktion. Читання та реферування наукових статей з криптографічного захисту. Вправи на усний переказ технічних текстів. Дискусія про актуальність квантової криптографії.

Тема 3.3

Протоколи захисту даних у мережах. Протоколи: SSL/TLS, HTTPS, IPSec, SSH, PGP — фахова термінологія та функціональний опис. Читання технічних RFC-документів та їх анотування. Складання технічного звіту за результатами аналізу протоколів. Захист протоколу перед аудиторією.

Модуль 4. Технічна документація та стандарти ІБ

ЗМІСТОВНИЙ МОДУЛЬ 4

Тема 4.1

BSI IT-Grundschutz як нормативна база. Структура та зміст методології IT-Grundschutz Федерального відомства з інформаційної безпеки Німеччини (BSI). Читання та переклад вибраних розділів каталогів IT-Grundschutz. Термінологія: Schutzbedarfsfeststellung, Risikoanalyse, Sicherheitskonzept, Maßnahmen. Порівняння з українськими стандартами у сфері захисту інформації.

Тема 4.2

ISO/IEC 27001 — міжнародний стандарт ІБ. Читання і переклад основних вимог стандарту в оригіналі (версія DIN EN ISO/IEC 27001). Фахова лексика: Informationssicherheitsmanagementsystem (ISMS), Risikobehandlung, Konformitätsbewertung, interne Revision. Аналіз структури та вимог стандарту для підготовки реферату.

Тема 4.3

Написання технічних звітів та анотацій. Структура та жанрові особливості Bericht, Zusammenfassung, Abstract, Stellungnahme у технічній сфері. Мовні засоби для опису методології, результатів та висновків. Практичне написання технічного звіту з питань безпеки ІКС за матеріалами BSI-Lageberichte (щорічний звіт BSI про стан ІБ).

Модуль 5. Операційні системи та програмне забезпечення

ЗМІСТОВНИЙ МОДУЛЬ 5

Тема 5.1

Betriebssysteme — операційні системи. Читання та переклад технічних описів операційних систем (Linux, Windows, macOS) та їх компонентів безпеки. Фахова лексика: Kernel, Treiber, Zugriffsrechte, Benutzerkonten, Systemprotokoll, Patch-Management. Аналіз технічних бюлетенів безпеки (Security Bulletins) відомих виробників ПЗ.

Тема 5.2

Антивірусне та захисне ПЗ. Лексика для опису засобів захисту: Antivirenprogramm, Intrusion-Prevention-System, Spam-Filter, Zwei-Faktor-Authentifizierung, Endpoint-Security. Читання документації та порівняльних оглядів засобів захисту від відомих виробників. Написання порівняльного огляду засобів захисту (Produktvergleich).

Тема 5.3

Управління інцидентами ІБ. Термінологія управління інцидентами: Sicherheitsvorfall, Incident Response, Notfallplan, Forensik, Beweissicherung, Wiederherstellung. Читання та реферування планів реагування на інциденти. Рольова гра: доповідь про інцидент ІБ перед керівництвом (auf Deutsch).

Модуль 6. Хмарні технології та захист даних

ЗМІСТОВНИЙ МОДУЛЬ 6

Тема 6.1

Cloud Computing та безпека хмарних середовищ. Фахова термінологія хмарних технологій: Cloud-Dienst, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Datenmigration, Mandantenfähigkeit. Читання технічних описів хмарних рішень від провідних виробників. Аналіз аспектів безпеки та конфіденційності хмарних сховищ.

Тема 6.2

Захист даних у хмарних середовищах. Законодавча база: Anforderungen an Cloud-Dienste згідно DSGVO та BSI C5 (Cloud Computing Compliance Criteria Catalogue). Читання і переклад вимог до хмарних провайдерів. Технічна лексика: Datenverschlüsselung in der Cloud, Zugriffsprotokoll, Datenlokalisierung, Auftragsdatenverarbeitung.

Тема 6.3

Ділова комунікація у хмарних проектах. Ведення технічних переговорів та листування з постачальниками хмарних рішень. Складання технічного завдання (Lastenheft) та специфікації вимог (Pflichtenheft) до хмарної системи. Практикум: телефонна та відеоконференція з питань впровадження хмарного рішення (рольова гра).

Модуль 7. Наукова комунікація та академічне письмо

ЗМІСТОВНИЙ МОДУЛЬ 7

Тема 7.1

Науковий стиль та академічне письмо. Особливості наукового стилю (Wissenschaftssprache) у галузі інформаційної безпеки. Структура наукової статті: Abstract, Einleitung, Methoden, Ergebnisse, Diskussion, Fazit. Мовні засоби аргументації та реферування. Написання анотації (Abstract) до власного дослідження з ІБ.

Тема 7.2

Реферування та переклад наукових текстів. Методика реферування наукових публікацій з кібербезпеки та захисту інформації. Технічний переклад: особливості передачі термінів та скорочень. Практична робота: реферат наукової статті з журналу «Datenschutz und Datensicherheit» (DuD) або видань Fraunhofer-Institut.

Тема 7.3

Фахова презентація результатів дослідження. Структура усної презентації (Vortrag/Präsentation) у науковому та діловому контексті. Мовні засоби для введення, переходів та висновків. Підготовка та захист власної презентації (10–15 хвилин) з тематики безпеки ІКС або захисту даних. Оцінювання презентацій однокурсників.

Модуль 8. Інтегрований практикум та підсумковий контроль

ЗМІСТОВНИЙ МОДУЛЬ 8

Тема 8.1

Комплексний переклад технічної документації. Практичний переклад комплексу технічних документів: технічне завдання, специфікація, звіт про аудит ІБ, інструкція з безпеки. Редагування та рецензування перекладів. Оцінювання якості перекладу за галузевими стандартами. Використання термінологічних баз і CAT-інструментів.

Тема 8.2

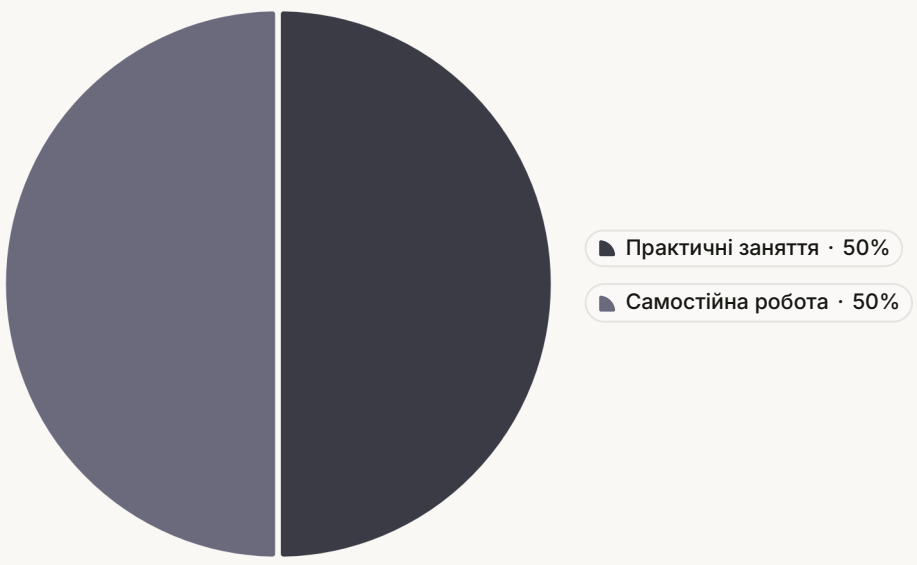
Ділова гра: міжнародний проєкт з кібербезпеки. Симуляція роботи у міжнародній команді (Deutsch-ukrainisches IT-Sicherheitsprojekt): розподіл ролей, ведення нарад (Besprechungsprotokoll), написання статус-звітів, підготовка підсумкового звіту про стан ІБ ІКС. Розвиток міжкультурної компетентності та розуміння ділової культури Німеччини.

Тема 8.3

Узагальнення та систематизація навчального матеріалу. Повторення та систематизація фахової термінології за всіма модулями. Підготовка до підсумкового контролю: комплексне тестування лексики та граматики, переклад, усна відповідь. Самооцінювання рівня мовних компетентностей відповідно до шкали CEFR (B1–B2).

Розподіл навчального часу — 240 годин

Модуль	Тема	Практичні (год.)	Самостійна робота (год.)	Разом (год.)
Модуль 1	Теми 1.1–1.4 — Вступ до фахової мови	14	14	28
Модуль 2	Теми 2.1–2.3 — Інформаційна безпека: основи	14	14	28
Модуль 3	Теми 3.1–3.3 — Мережева безпека та криптографія	16	16	32
Модуль 4	Теми 4.1–4.3 — Технічна документація та стандарти	14	14	28
Модуль 5	Теми 5.1–5.3 — Операційні системи та ПЗ	16	16	32
Модуль 6	Теми 6.1–6.3 — Хмарні технології та захист даних	14	14	28
Модуль 7	Теми 7.1–7.3 — Наукова комунікація	16	16	32
Модуль 8	Теми 8.1–8.3 — Інтегрований практикум	16	16	32
Разом		**120**	**120**	**240**



Структура навчального часу

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

- **Практичні заняття (120 год. — 50%):** відпрацювання мовних навичок, робота з фаховими текстами, рольові ігри, презентації, переклад
- **Самостійна робота (120 год. — 50%):** поглиблене вивчення лексики, підготовка завдань, читання автентичних текстів, написання рефератів

Курс розраховано на рівень **B1–B2 CEFR** — студенти розвивають здатність до самостійного опрацювання фахових матеріалів з ІБ та ІКС.

Самостійна робота студентів та методи викладання

Форми самостійної роботи

Опрацювання фахової літератури

Поглиблене вивчення теоретичного матеріалу за навчальними посібниками з фахової німецької мови та термінологічними словниками з IT та кібербезпеки. Конспектування ключових термінів, складання глосаріїв, порівняльний аналіз лексичних систем у технічних текстах.

Індивідуальні завдання

Виконання перекладів технічних текстів (250–400 слів), написання анотацій до наукових статей, реферування матеріалів BSI, підготовка термінологічних глосаріїв з тематики кожного модуля, написання ділових листів і звітів з безпеки ІКС.

Робота з інформаційними ресурсами

Опрацювання офіційних сайтів: BSI (**www.bsi.bund.de**), DSGVO-Portal (**dsgvo-gesetz.de**), Fraunhofer SIT (**sit.fraunhofer.de**). Читання автентичних новин і статей з IT-безпеки (Heise Security, c't Magazin, BSI Lagebericht).

Підготовка до занять

Підготовка до практичних занять шляхом опрацювання лексичного та граматичного матеріалу; підготовка до тестувань через вивчення термінологічних глосаріїв; систематизація знань перед контрольними роботами та підсумковими заходами.

Методи викладання

→ Комунікативні вправи

Парні та групові вправи з відпрацювання фахового мовлення: діалоги, дискусії, рольові ігри з тематики кібербезпеки та захисту інформації; студенти розвивають навички спонтанного та підготовленого мовлення.

→ Кейс-стаді

Аналіз реальних кіберінцидентів за матеріалами BSI та Heise Security: студенти опрацьовують автентичні тексти, виявляють термінологічні конструкції та обговорюють технічні рішення.

→ Перекладацькі вправи

Переклад технічної документації, стандартів та фахових статей з IT-безпеки. Редагування та взаємооцінювання перекладів. Робота з термінологічними базами та онлайн-словниками.

→ Презентації та доповіді

Підготовка та захист усних презентацій з тематики ІБ та ІКС. Формування навичок публічного мовлення, аргументації та відповідей на запитання аудиторії німецькою мовою.

→ Самостійне дослідження

Підготовка термінологічних глосаріїв, рефератів і перекладів за обраною темою; розвиток навичок самостійного пошуку та опрацювання автентичних джерел з кібербезпеки.

Форми контролю знань

1

Поточний контроль

Завдання: лексичні та граматичні тести, переклад мікротекстів, усні відповіді на запитання за темою. Оцінюються регулярність виконання завдань, якість перекладів і рівень засвоєння термінології. Поточний контроль формує накопичувальну оцінку протягом семестру. Включає усні опитування, письмові вправи, термінологічні диктанти та участь у рольових іграх і дискусіях.

2

Проміжний контроль

Самостійна робота — комплексне практичне завдання або реферат, що охоплює теми змістовних модулів (переклад технічного тексту, написання анотації, усна презентація). Оцінюються повнота перекладу, коректність використання термінології та обґрунтованість власних суджень. Проводиться після кожного парного модуля (після 2, 4, 6 та 8 модулів).

3

Підсумковий контроль

Іспит відповідно до навчального плану. Форма проведення — комплексний екзамен: тестування з лексики та граматики, переклад фахового тексту (350–450 слів), усна відповідь на запитання за курсом. Підсумкова оцінка враховує результати поточного, проміжного та підсумкового контролю: 100-бальна система з переведенням у національну шкалу та ЄКТС (A, B, C, D, E, FX, F).

Усі методи контролю спрямовані на формування іншомовних компетентностей, передбачених освітньо-професійною програмою «Організація захисту інформації в ІКС» спеціальності 123 «Комп'ютерна інженерія».

Рекомендована література та ресурси

Навчальна та наукова література (2022–2024)

1. Бабій М. С., Кравченко Т. О. Фахова німецька мова для студентів технічних спеціальностей: навч. посіб. — Київ : КПІ ім. Ігоря Сікорського, 2022. — 228 с.
2. Гаращенко Л. В., Сінченко Є. І. Deutsch für Informatiker: навчальний посібник з фахової мови для студентів спеціальності «Комп'ютерна інженерія». — Харків : ХНУРЕ, 2023. — 210 с.
3. Грищенко Т. А., Шевченко О. М. Технічний переклад з німецької мови: навч. посіб. для студентів технічних спеціальностей. — Київ : НАУ, 2022. — 256 с.
4. Коваленко Н. В., Остапченко В. І. Fachsprache Informatik und IT-Sicherheit: навч. посіб. — Львів : Видавництво Львівської політехніки, 2023. — 240 с.
5. Кузьменко О. Ю., Панченко І. В. Deutsch im IT-Bereich: комплекс завдань для розвитку фахових комунікативних компетентностей. — Київ : Університет «Україна», 2023. — 196 с.
6. Лисенко М. А., Романченко С. В. Фахова іноземна мова (німецька) у сфері захисту інформації: навч. посіб. — Київ : ДУІКТ, 2022. — 284 с.
7. Назаренко А. В., Петрук В. О. Deutsch für Cybersicherheit: читання, переклад та анотування фахових текстів: навч. посіб. — Київ : Видавничий дім «Академперіодика», 2024. — 198 с.
8. Олійник Р. С., Ткаченко Д. М. Термінологічний словник з інформаційних технологій та кібербезпеки (українсько-англійсько-німецький): навч. посіб. — Харків : ХНУРЕ, 2023. — 178 с.
9. Семенченко К. І., Бондаренко О. П. Ділова комунікація в ІТ-сфері: навч. посіб. з фахової мови (нім.) для студентів технічних ЗВО. — Київ : Алерта, 2024. — 212 с.
10. Шевчук О. В., Голубченко І. Л. Граматика і стиль технічного тексту (німецька мова): навч. посіб. для студентів технічних спеціальностей. — Київ : НАДУ, 2023. — 220 с.

Офіційні інтернет-ресурси та фахові видання

1. Федеральне відомство з інформаційної безпеки Німеччини (BSI). — URL: **https://www.bsi.bund.de/**
2. BSI IT-Grundschutz — каталоги та методологія. — URL: **https://www.bsi.bund.de/grundschutz**
3. Офіційний текст DSGVO (Datenschutz-Grundverordnung). — URL: **https://dsgvo-gesetz.de/**
4. Fraunhofer-Institut für Sichere Informationstechnologie (SIT). — URL: **https://www.sit.fraunhofer.de/**
5. Журнал Datenschutz und Datensicherheit (DuD). — URL: **https://www.springer.com/journal/11623**
6. Heise Security — новини та аналітика з IT-безпеки (нім.). — URL: **https://www.heise.de/security/**
7. Державна служба спеціального зв'язку та захисту інформації України. — URL: **https://cip.gov.ua/**
8. Науково-технічний журнал «Кібербезпека: освіта, наука, техніка». — URL: **https://csecurity.kubg.edu.ua/**

Рекомендована література охоплює видання **2022–2024 років** українських авторів та актуальні ресурси відповідно до вимог ОП «Організація захисту інформації в ІКС» спеціальності 123 «Комп'ютерна інженерія».