ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФАКУЛЬТЕТ ІНОЗЕМНОЇ ФІЛОЛОГІЇ
КАФЕДРА ІНОЗЕМНИХ МОВ

Декан фізичного факультету
_____
Докт.фіз.мат. наук, проф.**Лазур В.Ю.**
«30» серпня 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ІНОЗЕМНА МОВА ДЛЯ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ»

Рівень вищої освіти	**другий(магістерський)**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека та захист інформації**
Освітня програма	**125 Безпека інформаційних і комунікаційних систем**
Статус дисципліни	**обов'язкова**
Мова навчання	**англійська**

Ужгород 2023

Робоча програма навчальної дисципліни **«Іноземна мова для професійної діяльності»** для здобувачів вищої освіти **галузі знань:** 12 Інформаційні технології; **спеціальності**: 125 Кібербезпека; **освітньої програми:** 125 Безпека інформаційних і комунікаційних систем

Розробники:

Канд.пед.наук, доц.	Канюк Олександра Любомирівна
Канд.пед.наук, доц.	Чейпеш Іванна Василівна
Ст.викладач	Бура Ірина Олегівна

Робочу програму розглянуто та затверджено на засіданні кафедри ***іноземних мов***
протокол № _13_ від «_23_» __червня__ 2023_ р.

Завідувач кафедри: _____ **Олександра КАНЮК**

Схвалено науково-методичною комісією ***фізичного факультету***
протокол № _4__від «_30_» __червня__ 2023_ р.

Голова науково-методичної комісії: _____ **Вікторія СИНЬО**

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td>Розподіл годин за навчальним планом</td></tr>
<tr><td>Денна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС – 3</td><td>Рік підготовки:</td></tr>
<tr><td>Загальна кількість годин – 90</td><td>1-й</td></tr>
<tr><td>Кількість модулів – 1</td><td>Семестр:</td></tr>
<tr><td rowspan="5">Тижневих годин для денної форми навчання: 2

аудиторних – 36

самостійної роботи студента – 54</td><td>1-й</td></tr>
<tr><td>Лекції:</td></tr>
<tr><td>0</td></tr>
<tr><td>Практичні (семінарські):</td></tr>
<tr><td>0</td></tr>
<tr><td rowspan="2">Вид підсумкового контролю:

залік</td><td>Лабораторні:</td></tr>
<tr><td>36</td></tr>
<tr><td rowspan="2">Форма підсумкового контролю:

усна</td><td>Самостійна робота:</td></tr>
<tr><td>54</td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни **«Іноземна мова для професійної комунікації»** є формування у студентів іншомовної комунікативної компетенції у сфері професійного спілкування в усній і письмовій формах у процесі навчання, виховання, освіти і розвитку особистості студента. Вона полягає у практичному оволодінні студентами різними видами мовленнєвої діяльності відповідно до профілю майбутньої професії: інформаційних засобів, опрацювання фахової літератури, адекватне сприйняття іноземних джерел на міжнародному рівні; користування усним монологічним та діалогічним мовленням у межах професійної тематики, переклад з іноземної мови на рідну спеціалізованих матеріалів, вміння підготуватися до участі у міжнародних зустрічах, конференціях, семінарах

Відповідно до освітньої програми **«Безпека інформаційних і комунікаційних систем»,** вивчення дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей:

ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ (ЗК)

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК5. Здатність діяти соціально відповідально та громадсько свідомо.

ЗК6. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності.

Загальні компетентності (ЗК) згідно професійного стандарту «Фахівець сфери захисту інформації»

ЗК.02. Здатність застосовувати знання у практичних ситуаціях, розв’язувати завдання/задачі та практичні проблеми у професійній діяльності.

ЗК.04. Здатність до абстрактного мислення, аналізу та синтезу, вчитися і бути сучасно навченим.

ЗК.05. Здатність до адаптації та дії в новій ситуації.

ЗК.06. Здатність до вибору стратегії спілкування, працювати в команді.

ЗК.07. Здатність спілкуватися рідною мовою як усно, так і письмово, спілкуватися іноземною (переважно англійською) на рівні, що забезпечує ефективну професійну діяльність.

ФАХОВІ КОМПЕТЕНТНОСТІ (ФК)

ФК10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

Професійні компетентності (за трудовою дією або групою трудових дій) згідно професійного стандарту «Фахівець сфери захисту інформації»

Е3. Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень.

ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Передумовами вивчення навчальної дисципліни **«Іноземна мова для професійної комунікації»** є опанування таких навчальних дисциплін (НД) освітньої програми (ОП):

ОК 2. Методика викладання фахових дисциплін у вищій школі

ОК 3. Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації

ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми **«Безпека інформаційних і комунікаційних систем»** вивчення навчальної дисципліни **«Іноземна мова для професійної комунікації»** повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН):

Програмні результати навчання	Шифр ПРН
Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	ПРН 1
Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об’єктивно оцінювати результати навчання.	ПРН17
Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	ПРН 18

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни **«Іноземна мова для професійної комунікації»**:

Очікувані результати навчання з дисципліни	Шифр ПРН
Знання з предметної галузі включають: • програмний матеріал з усього комплексу фонетичних та лексико-граматичних правил; методику самостійної поза аудиторної роботи над удосконаленням мови; • граматичні вимоги щодо правильного оформлення ділового мовлення в усній та письмовій формах. **Когнітивні компетентності включають:** • здатність вільно і фонетично правильно читати тексти, підібрані на базі вивченого лексичного і граматичного матеріалу; • розуміти та вміти характеризувати зміст прочитаного чи прослуханого тексту; • здатність вести бесіду іноземною мовою в межах вивченої тематики, дотримуючись граматичних і фонетичних норм; • переказувати зміст прочитаного тексту чи прослуханого поза аудиторного читання; • здатність переказувати іноземною мовою зміст прочитаного чи прослуханого професійно спрямованого тексту; • письмово викладати прослуханий спеціалізований текст; • перекладати професійні та ділові тексти з рідної мови іноземною і навпаки; • здатність працювати з оригінальною літературою, реферувати й анотувати наукову літературу; • здатність виступати ініціаторами діалогу в ситуації професійного спілкування; • одержувати професійну інформацію з іноземних джерел, а також проводити бесіду-діалог; • здійснювати пошук інформації в мережі інтернет. **До практичних умінь та навичок входять:** • вільно і правильно розмовляти однією з іноземних мов у різних ситуаціях, переважно в ситуаціях професійного спілкування; • читати та анотувати художні тексти; • виступати з доповідями та повідомленнями з тематики своїх професійних інтересів; • оперувати лексикою ділових паперів.	ПРН 17 ПРН 18 ПРН 1

5. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засоби оцінювання та методи демонстрування результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання з навчальної дисципліни є: виступи на практичних заняттях; модульні контрольні роботи; екзамен; виконання індивідуальних та групових завдань під час аудиторних занять та самостійної роботи, що створюються на основі програмних результатів навчання; виконання тестових завдань, доповідь на студентській науковій конференції, підготовка наукової роботи; написання анотації до наукової статті; презентації та виступи на різних заходах; написання особистого листа чи резюме, поза-аудиторне читання та його захист.

Самостійна робота також включає: опрацювання теоретичних та практичних основ прослуханого матеріалу; вивчення окремих тем питань, що передбачені для самостійного опрацювання; поглиблене вивчення літератури на задану тему та пошук додаткової інформації; підготовка до практичних занять; систематизацію вивченого матеріалу перед екзаменом; опрацювання та підготовку огляду опублікованих у фахових та інших виданнях статей; побудову мультимедійних презентацій тощо.

Аудиторна та самостійна робота здобувачів забезпечується всіма навчально методичними засобами, необхідними для вивчення навчальної дисципліни чи окремої теми: підручниками, навчальними та навчально-методичними посібниками, методичними рекомендаціями, конспектами лекцій, науковою літературою та періодичними виданнями, дистанційною організацією навчання в системі Moodle, індивідуальними семестровими завданнями та методичними рекомендаціями для самостійної роботи; тестовими завданнями для контролю та самоконтролю знань, умінь і навичок.

Форми контролю та критерії оцінювання результатів навчання

Форми поточного контролю:	усне опитування, оцінка виконаних практичних завдань
Форма модульного контролю:	тест
Форма підсумкового семестрового контролю:	залік

Форми поточного контролю включають усне опитування студентів на практичних заняттях, презентації та рольові ігри за темами змістових модулів, переклад уривку зі статті з англійської на українську мову і навпаки, поза-аудиторне читання та його захист тощо. Крім цього, поточний контроль охоплює такі вибіркові форми самостійної роботи, як: доповідь на студентській науковій конференції, підготовка наукової роботи тощо.

Форма модульного контролю: проводиться з метою визначення стану успішності здобувачів вищої освіти за період теоретичного навчання. Підсумковий модульний контроль знань студентів здійснюється через проведення аудиторних письмових контрольних робіт та/або комп'ютерного тестування.

Форма підсумкового семестрового контролю: Підсумковий семестровий контроль – це підсумкове оцінювання результатів навчання здобувача вищої освіти за семестр, що здійснюється у формі екзамену. На підсумковий семестровий контроль виносяться питання, ситуаційні завдання тощо, що передбачають перевірку розуміння здобувачами вищої освіти програмного матеріалу дисципліни в цілому та рівня сформованості відповідних компетентностей після опанування курсу. Підсумковий семестровий контроль оцінюється від 0 до 100 балів і переводиться у національну шкалу та шкалу ЄКТС.

Поточний контроль разом з індивідуальним контролем оцінюється:

Критерії оцінки	Параметри оцінювання
90-100 − A − 5	1) на всі запитання завдання було дано вичерпні та точні відповіді. Вичерпною вважається відповідь, яка охоплює всі аспекти, які розглядаються впродовж вивчення всіх складових курсу даної дисципліни (практичні, індивідуальна і самостійна робота); У студента розгорнута, максимально повна відповідь, вільно володіє запропонованою темою; відсутні граматичні та лексичні помилки; комунікативне завдання виконано повністю. 2) за умови акуратного оформлення результатів роботи згідно відповідних вимог.
82-89 − B − 4	1) на всі запитання завдання було дано вичерпні та точні відповіді з окремими недоліками. Вичерпною вважається відповідь, яка охоплює всі аспекти, які розглядаються впродовж вивчення всіх складових курсу даної дисципліни (практичні, індивідуальна і самостійна робота); У студента розгорнута повна відповідь, в якій бракує деякої інформації, яка, проте, не має ключового значення; відсутні граматичні та лексичні помилки; комунікативне завдання виконано повністю. 2) за умови акуратного оформлення результатів роботи згідно відповідних вимог.
74-81 − C − 4	1) на всі запитання завдання було дані повні відповіді. Повною вважається відповідь, яка охоплює основні аспекти питання в рамках конспекту. У студента розгорнута повна відповідь, в якій бракує деякої інформації, яка, проте, не має ключового значення; відсутні граматичні та лексичні помилки; комунікативне завдання виконано

	повністю. 2) за умови акуратного оформлення результатів роботи згідно відповідних вимог.
64-73 − D − 3	1) дані повні відповіді на переважну більшу частину запитань, або неповні відповіді на всі запитання. Неповною вважається відповідь, яка містить не всі аспекти питання, що розглядається; У студента відповідь в достатньому обсязі, допускається опущення певної частини інформації; наявні деякі граматичні та лексичні помилки, які не порушують виконання комунікативного завдання. 2) за умови акуратного оформлення результатів роботи згідно відповідних вимог.
60-63 − E − 3	1) дані повні відповіді на більшу частину запитань, або неповні відповіді на всі запитання. Неповною вважається відповідь, яка містить не всі аспекти питання, що розглядається; У студента відповідь в достатньому обсязі, допускається опущення певної частини інформації; наявні деякі граматичні та лексичні помилки, які не порушують виконання комунікативного завдання. 2) за умови акуратного оформлення результатів роботи згідно відповідних вимог.
35-59 − FX − 2	1) не дані відповіді на більшу частину запитань; У студента відповідь в мінімальному припустимому або в недостатньому обсязі, значна частина інформації пропущена або спотворена; наявні серйозні помилки, що заважають розумінню; комунікативне завдання не виконано або відсутність відповіді взагалі. 2) оформлення результатів роботи є незадовільним.
0-34 − F − 1	1) не дані відповіді на жодну частину запитань; 2)оформлення результатів роботи є незадовільним.

Розподіл балів, які отримують здобувачі вищої освіти (модуль 1)

Поточне оцінювання та самостійна робота																**Модульна контрольна робота**	**Сума**
Т1+Т1.1	Т2+Т2.1	Т3+Т3.1	Т4+Т4.1	Т5+Т5.1	Т6+Т6.1	Т7+Т7.1	Т8+Т8.1	Т9+Т9.1	Т10+Т10.1	Т11+Т11.1	Т12+Т12.1	Т13+Т13.1	Т14+Т14.1	Т15+Т15.1	Т16+Т16.1	50	**100**
3	3	4	3	3	3	3	3	3	3	3	3	3	3	3	4		

Т1, Т2 ... – теми

Оцінювання окремих видів навчальної роботи з дисципліни

Вид діяльності здобувача вищої освіти	**Модуль 1**	
	Кількість	Максимальна кількість балів (сумарна)
Лабораторні заняття (допуск, виконання та захист)	16	32
Письмове тестування при тематичному оцінюванні	3	9
Презентація / Реферат	1	3
Самостійна робота	3	6
Модульна контрольна робота	1	50
Разом	**24**	**100**

Оцінка знань, умінь та практичних навичок студента з навчальної дисципліни здійснюється за 100-бальною системою.

Оцінювання знань студентів здійснюється на основі результатів:

- поточного контролю знань;
- підсумкового контролю знань (екзамен).

Поточний контроль знань студентів здійснюється за двома складовими:

- контроль систематичності та активності роботи студента протягом семестру;
- контроль за виконанням модульних завдань.

При контролі систематичності та активності роботи студента оцінці підлягають:

- відвідування лабораторних занять;
- активність на лабораторних заняттях;
- рівень засвоєння знань програмного матеріалу;
- підготовка і презентація рефератів, наукових доповідей, участь в олімпіадах тощо.

Критерії оцінювання підсумкового семестрового контролю: поточний контроль наприкінці семестру перераховується у 50-бальну оцінку; модульний контроль наприкінці семестру перераховується у 50-бальну оцінку.

Підсумковий контроль. За наявності рівня результатів поточних контролів з усіх видів навчальних занять не менше 60 балів, оцінювання виконується без участі студента шляхом визначення середньозваженого значення. У випадку, коли студент за результатами поточних контролів з усіх видів навчальних занять отримав менше 60 балів, або не погоджується з оцінкою, яку отримав під час підсумкового контролю, він має право складати екзамен. Студент, який не з'явився на екзамен без поважних причин, вважається таким, що одержав незадовільну оцінку, чи погоджується зі своїм підсумковим контролем.

Якщо студент був не допущений до екзамену, він повинен до встановленого терміну перескладання екзамену набрати необхідну кількість балів з поточного та /або проміжного контролю, виконуючи додаткові види робіт або перескладаючи модульну контрольну роботу.

Повторне складання підсумкового контролю з дисципліни, коли студент отримав оцінку «не задовільно» (нижче 60-ти балів), допускається не більше двох разів. Спроби студента виправити оцінку й не допустити академічної заборгованості обмежуються терміном в один місяць після закінчення екзаменаційної сесії.

Критерії оцінювання та схема нарахування балів є наступною:

Загальна сума балів	Оцінка ECTS	Оцінка за національною шкалою для екзамену
90 – 100	A	відмінно
82-89	B	добре
74-81	C	
64-73	D	задовільно
60-63	E	
35-59	FX	незадовільно з можливістю повторного складання
0-34	F	незадовільно з обов'язковим повторним вивченням дисципліни

6. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

6.1. Зміст навчальної дисципліни

Модуль 1.

Topic 1. Introduction to Computer Security

Topic 1.1. Networks and the internet

Topic 2. Terms in Computer Security

Topic 2.1. Doing exercises on the topic 2.

Topic 3. Data Protection and Data Security

Topic 3.1. What Can Happen to Data?

Topic 4. Types of Computer Security

Topic 4.1. The Layers of Cyber Security

Topic 5. Types of Cyber Attacks: System-based Attacks

Topic 5.1. Web-based Attacks

Topic 6. Malware and its types

Topic 6.1. Adware and Spyware

Topic 7. Browser hijacking software

Topic 7.1. Virus. Worms

Topic 8. Trojan Horse.

Topic 8.1. Scareware

Topic 9. Preventing Malware Attacks

Topic 9.1. How Cyber Security specialists deals with Malware Attacks

Topic 10, Classification of Cyber Crimes

Topic 10.1. Reasons for Commission of Cyber Crimes

Topic 11. Kinds of Cyber Crimes

Topic 11.1. The most Famous Cyber Crimes

Topic 12. Cybercrimes: Mobile and Wireless

Topic 12.1. Credit Card Frauds in Mobile and Wireless Computing Era.

Topic 13. Security Challenges proposed by Mobile devices

Topic 13.1. Guideline for setting secure Password

Topic 14. Investigating Cyber Crimes

Topic 14.1. Computer Forensics

Topic 15. Cyber Security Techniques

Topic 15. 1. Antivirus and firewalls

Topic 16. My future profession

Topic 16.1. Famous Companies Deals with Cyber Security

6.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин:90					
	Форма навчання: **денна**					
	Усього	у тому числі				
		Лекції	Практичні (семінарські)	Лабораторні	Індивідуальна робота	Самостійна робота
1-й семестр						
Модуль 1.						
Topic 1. Introduction to Computer Security	2			2		0
Topic 1.1. Networks and the internet	4			0		4
Topic 2. Terms in Computer Security	2			2		0
Topic 2.1. Doing exercises on the topic 2.	3			0		3
Topic 3. Data Protection and Data Security	2			2		0
Topic 3.1. What Can Happen to Data?	3			0		3
Topic 4. Types of Computer Security	2			2		0
Topic 4.1. The Layers of Cyber Security	3			0		3
Topic 5. Types of Cyber Attacks: System-based Attacks	2			2		0
Topic 5.1. Web-based Attacks	3			0		3
Topic 6. Malware and its types	3			3		0
Topic 6.1. Adware and Spyware	3			0		3
Topic 7. Browser hijacking software	3			3		0
Topic 7.1. Virus. Worms	4			0		4
Topic 8. Trojan Horse.	2			2		0
Topic 8.1. Scareware	4			0		4

Topic 9. Preventing Malware Attacks	2			2		0
Topic 9.1. How Cyber Security specialists deals with Malware Attacks	3			0		3
Topic 10, Classification of Cyber Crimes	2			2		0
Topic 10.1. Reasons for Commission of Cyber Crimes	3			0		3
Topic 11. Kinds of Cyber Crimes	2			2		0
Topic 11.1. The most Famous Cyber Crimes	3			0		3
Topic 12. Cybercrimes: Mobile and Wireless	2			2		0
Topic 12.1. Credit Card Frauds in Mobile and Wireless Computing Era.	3			0		3
Topic 13. Security Challenges proposed by Mobile devices	2			2		0
Topic 13.1. Guideline for setting secure Password	4			0		4
Topic 14. Investigating Cyber Crimes	2			2		0
Topic 14.1. Computer Forensics	3			0		3
Topic 15. Cyber Security Techniques	2			2		0
Topic 15. 1. Antivirus and firewalls	4			0		4
Topic 16. My future profession	2			2		0
Topic 16.1. Famous Companies Deals with Cyber Security	4			0		4
Модульна контрольна робота	2			2		0
Разом за модуль	**90**			**36**		**54**

6.3. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
		денна
	Модуль 1.	
1.	Topic 1. Introduction to Computer Security	2
2.	Topic 2. Terms in Computer Security	2
3.	Topic 3. Data Protection and Data Security	2

4.	Topic 4. Types of Computer Security	2
5.	Topic 5. Types of Cyber Attacks: System-based Attacks	2
6.	Topic 6. Malware and its types	3
7.	Topic 7. Browser hijacking software	3
8.	Topic 8. Trojan Horse.	2
9.	Topic 9. Preventing Malware Attacks	2
10.	Topic 10, Classification of Cyber Crimes	2
11.	Topic 11. Kinds of Cyber Crimes	2
12.	Topic 12. Cybercrimes: Mobile and Wireless	2
13.	Topic 13. Security Challenges proposed by Mobile devices	2
14.	Topic 14. Investigating Cyber Crimes	2
15.	Topic 15. Cyber Security Techniques	2
16.	Topic 16. My future profession	2
	Модульна контрольна робота	2
	Разом за модуль	**36**

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин
		денна
	Модуль 1.	
1.	Topic 1.1. Networks and the internet	4
2.	Topic 2.1. Doing exercises on the topic 2	3
3.	Topic 3.1. What Can Happen to Data?	3
4.	Topic 4.1. The Layers of Cyber Security	3
5.	Topic 5.1. Web-based Attacks	3
6.	Topic 6.1. Adware and Spyware	3
7.	Topic 7.1. Virus. Worms	4

8.	Topic 8.1. Scareware	4
9.	Topic 9.1. How Cyber Security specialists deals with Malware Attacks	3
10.	Topic 10.1. Reasons for Commission of Cyber Crimes	3
11.	Topic 11.1. The most Famous Cyber Crimes	3
12.	Topic 12.1. Credit Card Frauds in Mobile and Wireless Computing Era.	3
13.	Topic 13.1. Guideline for setting secure Password	4
14.	Topic 14.1. Computer Forensics	3
15.	Topic 15. 1. Antivirus and firewalls	4
16.	Topic 16.1. Famous Companies Deals with Cyber Security	4
	Разом за модуль	**54**

7. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

Технічні засоби : комп'ютер, мультимедійні презентації, відеоматеріали, чат, аудіозаписи тощо.
Обладнання: настільні та портативні комп'ютери, смартфони, портативні мультимедійні програвачі.
Програмне забезпечення: офісні програми (Google Meet, Moodle), програми для перегляду файлів (pdf, .djvu), електронні перекладачі текстів, електронні словники, мультимедійне програмне забезпечення тощо.

7. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. Чейпеш І.В., Бура І.О. Методичні рекомендації з дисципліни «Іноземна мова для професійної комунікації (для спеціальності: 125 Кібербезпека та захист інформації» / І.В.Чейпеш, І.О.Бура) – Ужгород: УжНУ, 2023. - 44с.
1. Charles P. Pfleeger і Shari Lawrence Pfleeger / Security in Computing. – Pearson, 2018, 320 p.
2. Nell Ann Pickett, Ann Appleton, і Katherine E. Staples / Technical English: Writing, Reading and Speaking. - Pearson Education, 2018. 848 p.
3. Stallings, William, and Lawrie Brown/ Computer Security: Principles and Practice. – Pearson, 2018. 848 p.

Допоміжна література

1. Stallings, William / Cryptography and Network Security: Principles and Practice. – Pearson, 2020. 784 p.
2. Stuttard, Dafydd, and Marcus Pinto / The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. – Wiley, 2020. 816 p.

Інформаційні ресурси в мережі Інтернет

1. Cybercrime https://www.britannica.com/topic/cybercrime
2. Glossary of cyber security terms https://www.ukcybersecuritycouncil.org.uk/glossary/
3. Malware and its types https://www.geeksforgeeks.org/malware-and-its-types/
4. Types of Cyber Attacks You Should Be Aware of in 2023 https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks

ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФАКУЛЬТЕТ ІНОЗЕМНОЇ ФІЛОЛОГІЇ
Кафедра ІНОЗЕМНИХ МОВ

Декан фізичного факультету
_____
докт. фіз.-мат. наук, проф. **Лазур В.Ю.**
«20» червня 2023 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ІНОЗЕМНА МОВА ДЛЯ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ»

Рівень вищої освіти	**другий (магістерський)**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека та захист інформації**
Освітня програма	**125 Безпека інформаційних і комунікаційних систем**
Статус дисципліни	**обов'язкова**
Мова навчання	**німецька**

Ужгород 2023

Робоча програма навчальної дисципліни **«Іноземна мова для професійної діяльності»** для здобувачів вищої освіти **галузі знань:** 12 Інформаційні технології; **спеціальності**: 125 Кібербезпека; **освітньої програми:** 125 Безпека інформаційних і комунікаційних систем

Розробники:
Канд. пед. наук, доц. Канюк Олександра Любомирівна
Канд. пед. наук, доц. Кіш Надія Василівна

Робочу програму розглянуто та затверджено на засіданні кафедри ***іноземних мов***
протокол № _13_ від «_23_» __червня__ 2023_ р.

Завідувач кафедри: _____ **Олександра КАНЮК**

Схвалено науково-методичною комісією ***фізичного факультету***
протокол № _4__від «_30_» __червня__ 2023_ р.

Голова науково-методичної комісії: _____ **Вікторія СИНЬО**

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td>Розподіл годин за навчальним планом</td></tr>
<tr><td>Денна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС – 3</td><td>Рік підготовки:</td></tr>
<tr><td>Загальна кількість годин – 90</td><td>1-й</td></tr>
<tr><td>Кількість модулів – 1</td><td>Семестр:</td></tr>
<tr><td rowspan="5">Тижневих годин для денної форми навчання: 2

аудиторних – 36

самостійної роботи студента – 54</td><td>1-й</td></tr>
<tr><td>Лекції:</td></tr>
<tr><td>0</td></tr>
<tr><td>Практичні (семінарські):</td></tr>
<tr><td>0</td></tr>
<tr><td rowspan="2">Вид підсумкового контролю:

залік</td><td>Лабораторні:</td></tr>
<tr><td>36</td></tr>
<tr><td rowspan="2">Форма підсумкового контролю:

усна</td><td>Самостійна робота:</td></tr>
<tr><td>54</td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни **«Іноземна мова для професійної комунікації»** є формування у студентів іншомовної комунікативної компетенції у сфері професійного спілкування в усній і письмовій формах у процесі навчання, виховання, освіти і розвитку особистості студента. Вона полягає у практичному оволодінні студентами різними видами мовленнєвої діяльності відповідно до профілю майбутньої професії: інформаційних засобів, опрацювання фахової літератури, адекватне сприйняття іноземних джерел на міжнародному рівні; користування усним монологічним та діалогічним мовленням у межах професійної тематики, переклад з іноземної мови на рідну спеціалізованих матеріалів, вміння підготуватися до участі у міжнародних зустрічах, конференціях, семінарах

Відповідно до освітньої програми **«Безпека інформаційних і комунікаційних систем»,** вивчення дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей:

ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ (ЗК)

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК5. Здатність діяти соціально відповідально та громадсько свідомо.

ЗК6. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності.

Загальні компетентності (ЗК) згідно професійного стандарту «Фахівець сфери захисту інформації»

ЗК.02. Здатність застосовувати знання у практичних ситуаціях, розв’язувати завдання/задачі та практичні проблеми у професійній діяльності.

ЗК.04. Здатність до абстрактного мислення, аналізу та синтезу, вчитися і бути сучасно навченим.

ЗК.05. Здатність до адаптації та дії в новій ситуації.

ЗК.06. Здатність до вибору стратегії спілкування, працювати в команді.

ЗК.07. Здатність спілкуватися рідною мовою як усно, так і письмово, спілкуватися іноземною (переважно англійською) на рівні, що забезпечує ефективну професійну діяльність.

ФАХОВІ КОМПЕТЕНТНОСТІ (ФК)

ФК10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

Професійні компетентності (за трудовою дією або групою трудових дій) згідно професійного стандарту «Фахівець сфери захисту інформації»

Е3. Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень.

ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Передумовами вивчення навчальної дисципліни **«Іноземна мова для професійної комунікації»** є опанування таких навчальних дисциплін (НД) освітньої програми (ОП):

ОК 2. Методика викладання фахових дисциплін у вищій школі

ОК 3. Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації

ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми **«Безпека інформаційних і комунікаційних систем»** вивчення навчальної дисципліни **«Іноземна мова для професійної комунікації»** повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН):

Програмні результати навчання	Шифр ПРН
Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	ПРН 1
Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об’єктивно оцінювати результати навчання.	ПРН17
Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	ПРН 18

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни **«Іноземна мова для професійної комунікації»**:

Очікувані результати навчання з дисципліни	Шифр ПРН
Знання з предметної галузі включають: • програмний матеріал з усього комплексу фонетичних та лексико-граматичних правил; методику самостійної поза аудиторної роботи над удосконаленням мови; • граматичні вимоги щодо правильного оформлення ділового мовлення в усній та письмовій формах. **Когнітивні компетентності включають:** • здатність вільно і фонетично правильно читати тексти, підібрані на базі вивченого лексичного і граматичного матеріалу; • розуміти та вміти характеризувати зміст прочитаного чи прослуханого тексту; • здатність вести бесіду іноземною мовою в межах вивченої тематики, дотримуючись граматичних і фонетичних норм; • переказувати зміст прочитаного тексту чи прослуханого поза аудиторного читання; • здатність переказувати іноземною мовою зміст прочитаного чи прослуханого професійно спрямованого тексту; • письмово викладати прослуханий спеціалізований текст; • перекладати професійні та ділові тексти з рідної мови іноземною і навпаки; • здатність працювати з оригінальною літературою, реферувати й анотувати наукову літературу; • здатність виступати ініціаторами діалогу в ситуації професійного спілкування; • одержувати професійну інформацію з іноземних джерел, а також проводити бесіду-діалог; • здійснювати пошук інформації в мережі інтернет. **До практичних умінь та навичок входять:** • вільно і правильно розмовляти однією з іноземних мов у різних ситуаціях, переважно в ситуаціях професійного спілкування; • читати та анотувати художні тексти; • виступати з доповідями та повідомленнями з тематики своїх професійних інтересів; • оперувати лексикою ділових паперів.	ПРН 17 ПРН 18 ПРН 1

5. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засоби оцінювання та методи демонстрування результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання з навчальної дисципліни є:

- залік;
- виконання тестових завдань та проведення аудиторних письмових контрольних робіт;
- написання особистого листа чи резюме, поза-аудиторне читання та його захист;
- доповідь на студентській науковій конференції, підготовка наукової роботи;
- написання анотації до наукової статті;
- презентації та виступи на різних заходах.

Форми контролю та критерії оцінювання результатів навчання

Форми поточного контролю:	усне опитування, оцінка виконаних практичних завдань
Форма модульного контролю:	тест
Форма підсумкового семестрового контролю:	залік

Форми поточного контролю включають усне опитування студентів на практичних заняттях, презентації та рольові ігри за темами змістових модулів, переклад уривку зі статті з німецької на українську мову і навпаки, поза-аудиторне читання та його захист тощо. Крім цього, поточний контроль охоплює такі вибіркові форми самостійної роботи, як: доповідь на студентській науковій конференції, підготовка наукової роботи тощо.

Форма модульного контролю: проводиться з метою визначення стану успішності здобувачів вищої освіти за період теоретичного навчання. Підсумковий модульний контроль знань студентів здійснюється через проведення аудиторних письмових контрольних робіт та/або комп'ютерного тестування.

Форма підсумкового семестрового контролю: Підсумковий семестровий контроль – це підсумкове оцінювання результатів навчання здобувача вищої освіти за семестр, що здійснюється у формі екзамену. На підсумковий семестровий контроль виносяться питання, ситуаційні завдання тощо, що передбачають перевірку розуміння здобувачами вищої освіти програмного матеріалу дисципліни в цілому та рівня сформованості відповідних компетентностей після опанування курсу. Підсумковий семестровий контроль оцінюється від 0 до 100 балів і переводиться у національну шкалу та шкалу ЄКТС.

Поточний контроль разом з індивідуальним контролем оцінюється:

Критерії оцінки	Параметри оцінювання
90-100 − A − 5	1) на всі запитання завдання було дано вичерпні та точні відповіді. Вичерпною вважається відповідь, яка охоплює всі аспекти, які розглядаються впродовж вивчення всіх складових курсу даної дисципліни (практичні, індивідуальна і самостійна робота); У студента розгорнута, максимально повна відповідь, вільно володіє запропонованою темою; відсутні граматичні та лексичні помилки; комунікативне завдання виконано повністю. 2) за умови акуратного оформлення результатів роботи згідно відповідних вимог.
82-89 − B − 4	1) на всі запитання завдання було дано вичерпні та точні відповіді з окремими недоліками. Вичерпною вважається відповідь, яка охоплює всі аспекти, які розглядаються впродовж вивчення всіх складових курсу даної дисципліни (практичні, індивідуальна і самостійна робота); У студента розгорнута повна відповідь, в якій бракує деякої інформації, яка, проте, не має ключового значення; відсутні граматичні та лексичні помилки; комунікативне завдання виконано повністю. 2) за умови акуратного оформлення результатів роботи згідно відповідних вимог.
74-81 − C − 4	1) на всі запитання завдання було дані повні відповіді. Повною вважається відповідь, яка охоплює основні аспекти питання в рамках конспекту. У студента розгорнута повна відповідь, в якій бракує деякої інформації, яка, проте, не має ключового значення; відсутні

	граматичні та лексичні помилки; комунікативне завдання виконано повністю. 2) за умови акуратного оформлення результатів роботи згідно відповідних вимог.
64-73 − D − 3	1) дані повні відповіді на переважну більшу частину запитань, або неповні відповіді на всі запитання. Неповною вважається відповідь, яка містить не всі аспекти питання, що розглядається; У студента відповідь в достатньому обсязі, допускається опущення певної частини інформації; наявні деякі граматичні та лексичні помилки, які не порушують виконання комунікативного завдання. 2) за умови акуратного оформлення результатів роботи згідно відповідних вимог.
60-63 − E − 3	1) дані повні відповіді на більшу частину запитань, або неповні відповіді на всі запитання. Неповною вважається відповідь, яка містить не всі аспекти питання, що розглядається; У студента відповідь в достатньому обсязі, допускається опущення певної частини інформації; наявні деякі граматичні та лексичні помилки, які не порушують виконання комунікативного завдання. 2) за умови акуратного оформлення результатів роботи згідно відповідних вимог.
35-59 − FX − 2	1) не дані відповіді на більшу частину запитань; У студента відповідь в мінімальному припустимому або в недостатньому обсязі, значна частина інформації пропущена або спотворена; наявні серйозні помилки, що заважають розумінню; комунікативне завдання не виконано або відсутність відповіді взагалі. 2) оформлення результатів роботи є незадовільним.
0-34 − F − 1	1) не дані відповіді на жодну частину запитань; 2)оформлення результатів роботи є незадовільним.

Розподіл балів, які отримують здобувачі вищої освіти (модуль 1)

Поточне оцінювання та самостійна робота																**Модульна контрольна робота**	**Сума**
Т1+Т1.1	Т2+Т2.1	Т3+Т3.1	Т4+Т4.1	Т5+Т5.1	Т6+Т6.1	Т7+Т7.1	Т8+Т8.1	Т9+Т9.1	Т10+Т10.1	Т11+Т11.1	Т12+Т12.1	Т13+Т13.1	Т14+Т14.1	Т15+Т15.1	Т16+Т16.1	50	**100**
3	3	4	3	3	3	3	3	3	3	3	3	3	3	3	4		

Т1, Т2 ... – теми

Оцінювання окремих видів навчальної роботи з дисципліни

Вид діяльності здобувача вищої освіти	**Модуль 1**	
	Кількість	Максимальна кількість балів (сумарна)
Лабораторні заняття (допуск, виконання та захист)	16	32
Письмове тестування при тематичному оцінюванні	3	9
Презентація / Реферат	1	3
Самостійна робота	3	6
Модульна контрольна робота	1	50
Разом	**24**	**100**

Критерії оцінювання підсумкового семестрового контролю: поточний контроль наприкінці семестру перераховується у 50-бальну оцінку; модульний контроль наприкінці семестру перераховується у 50-бальну оцінку.

Підсумковий контроль. За наявності рівня результатів поточних контролів з усіх видів навчальних занять не менше 60 балів, оцінювання виконується без участі студента шляхом визначення середньозваженого значення. У випадку, коли студент за результатами поточних контролів з усіх видів навчальних занять отримав менше 60 балів, або не погоджується з оцінкою, яку отримав під час підсумкового контролю, він має право складати екзамен. Студент, який не з'явився на екзамен без поважних причин, вважається таким, що одержав незадовільну оцінку, чи погоджується зі своїм підсумковим контролем.

Якщо студент був не допущений до екзамену, він повинен до встановленого терміну перескладання екзамену набрати необхідну кількість балів з поточного та /або проміжного контролю, виконуючи додаткові види робіт або перескладаючи модульну контрольну роботу.

Повторне складання підсумкового контролю з дисципліни, коли студент отримав оцінку «не задовільно» (нижче 60-ти балів), допускається не більше двох разів. Спроби студента виправити

оцінку й не допустити академічної заборгованості обмежуються терміном в один місяць після закінчення екзаменаційної сесії.

Критерії оцінювання та схема нарахування балів є наступною:

Загальна сума балів	Оцінка ECTS	Оцінка за національною шкалою для екзамену
90 – 100	A	відмінно
82-89	B	добре
74-81	C	
64-73	D	задовільно
60-63	E	
35-59	FX	незадовільно з можливістю повторного складання
0-34	F	незадовільно з обов’язковим повторним вивченням дисципліни

6. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

6.1. Зміст навчальної дисципліни

Модуль 1.

Thema 1. Was ist Cyberkriminalität? Wie schützen Sie sich?
Thema 1.1 Physik als Wissenschaftszweig.
Thema 2. Cyberraum, Cybersicherheit und Cyberterrorismus.
Thema 2.1 Präsens Passiv. Pronomen „man“
Thema 3. Soziale Netzwerke und Sicherheit.
Thema 3.1 Objektnebensätze.
Thema 4. Was ist Computerkriminalität?
Thema 4.1 Attributnebensätze.
Thema 5. Internetbetrug.
Thema 5.1 Die Pandemie und ihre Auswirkungen.
Thema 6. Blockchain, Kryptos und NFTs.
Thema 6.1 Konditionalis1. Komparativ.
Thema 7. Digitalisierung, IT – Sicherheit, Security, Datenschutz.
Thema 7.1 Andere Arten von Cyberkriminalität.
Thema 8. 18 Arten von Cyberkriminalität, die Unternehmen kennen sollten.
Thema 8.1 Best of Cyberkrimi: die verrücktesten Hackerangriffe.
Thema 9. Cyberkrimi gegen Privatpersonen. Ergebnisse einer…
Thema 9.1 Modalverben im Präsens.
Thema 10. Wie sieht die aktuelle Cybercrime Lage in Deutschland aus?
Thema 10.1 Rektion der Verben.
Thema 11. Suchtgifthandel im Darknet.
Thema 11.1 Zustandspassiv.
Thema 12. Pornographische Darstellungen Minderjährigen.
Thema 12.1 Nominales Prädikat. Imperfekt Aktiv.
Thema 13. Cybercrime - Bekämpfung in den Bundesländern.
Thema 13.1 Cybercrime - Bekämpfung in der Ukraine.
Thema 14. Werbung.
Thema 14.1 Schaffung neuer Bedürfnisse durch Werbung.
Thema 15. Medienporträt. Der Geschäftsbrief.
Thema 15.1 Anlageformen.
Thema 16. Mein zukünftiger Beruf.
Thema 16.1 Ein paar staatliche Giganten.

6.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин:90					
	Форма навчання: **денна**					
	Усього	у тому числі				
		Лекції	Практичні (семінарські	Лабораторні	Індивідуальна робота	Самостійна робота
1-й семестр						
Модуль 1.						
Thema 1. Was ist Cyberkriminalität? Wie schützen Sie sich?	2			2		0
Thema 1.1 Physik als Wissenschaftszweig.	4			0		4
Thema 2. Cyberraum, Cybersicherheit und Cyberterrorismus.	2			2		0
Thema 2.1 Präsens Passiv. Pronomen „man“	3			0		3
Thema 3. Soziale Netzwerke und Sicherheit.	2			2		0
Thema 3.1 Objektnebensätze.	3			0		3
Thema 4. Was ist Computerkriminalität?	2			2		0
Thema 4.1 Attributnebensätze.	3			0		3
Thema 5. Internetbetrug.	2			2		0
Thema 5.1 Die Pandemie und ihre Auswirkungen.	3			0		3
Thema 6. Blockchain, Kryptos und NFTs.	3			3		0
Thema 6.1 Konditionalis1. Komparativ.	3			0		3
Thema 7. Digitalisierung, IT – Sicherheit, Security, Datenschutz.	3			3		0
Thema 7.1 Andere Arten von Cyberkriminalität.	4			0		4
Thema 8. 18 Arten von Cyberkriminalität, die Unternehmen kennen sollten.	2			2		0
Thema 8.1 Best of Cyberkrimi: die verrücktesten Hackerangriffe.	4			0		4
Thema 9. Cyberkrimi gegen Privatpersonen. Ergebnisse einer…	2			2		0

Thema 9.1 Modalverben im Präsens.	3			0		3
Thema 10. Wie sieht die aktuelle Cybercrime Lage in Deutschland aus?	2			2		0
Thema 10.1 Rektion der Verben.	3			0		3
Thema 11. Suchtgifthandel im Darknet.	2			2		0
Thema 11.1 Zustandspassiv.	3			0		3
Thema 12. Pornographische Darstellungen Minderjährigen.	2			2		0
Thema 12.1 Nominales Prädikat. Imperfekt Aktiv.	3			0		3
Thema 13. Cybercrime - Bekämpfung in den Bundesländern.	2			2		0
Thema 13.1 Cybercrime - Bekämpfung in der Ukraine.	4			0		4
Thema 14. Werbung.	2			2		0
Thema 14.1 Schaffung neuer Bedürfnisse durch Werbung.	3			0		3
Thema 15. Medienporträt. Der Geschäftsbrief.	2			2		0
Thema 15.1 Anlageformen.	4			0		4
Thema 16. Mein zukünftiger Beruf.	2			2		0
Thema 16.1 Ein paar staatliche Giganten.	4			0		4
Модульна контрольна робота	2			2		0
Разом за модуль	**90**			**36**		**54**

6.3. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
		денна
	Модуль 1.	
1.	Thema 1. Was ist Cyberkriminalität? Wie schützen Sie sich?	2
2.	Thema 2. Cyberraum, Cybersicherheit und Cyberterrorismus.	2
3.	Thema 3. Soziale Netzwerke und Sicherheit.	2
4.	Thema 4. Was ist Computerkriminalität?	2

5.	Thema 5. Internetbetrug.	2
6.	Thema 6. Blockchain, Kryptos und NFTs.	3
7.	Thema 7. Digitalisierung, IT – Sicherheit, Security, Datenschutz.	3
8.	Thema 8. 18 Arten von Cyberkriminalität, die Unternehmen kennen sollten.	2
9.	Thema 9. Cyberkrimi gegen Privatpersonen. Ergebnisse einer…	2
10.	Thema 10. Wie sieht die aktuelle Cybercrime Lage in Deutschland aus?	2
11.	Thema 11. Suchtgifthandel im Darknet.	2
12.	Thema 12. Pornographische Darstellungen Minderjährigen.	2
13.	Thema 13. Cybercrime - Bekämpfung in den Bundesländern.	2
14.	Thema 14. Werbung.	2
15.	Thema 15. Medienporträt. Der Geschäftsbrief.	2
16.	Thema 16. Mein zukünftiger Beruf.	2
	Модульна контрольна робота	2
	Разом за модуль	**36**

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин
		денна
	Модуль 1.	
1.	Thema 1.1 Physik als Wissenschaftszweig.	4
2.	Thema 2.1 Präsens Passiv. Pronomen „man“	3
3.	Thema 3.1 Objektnebensätze.	3
4.	Thema 4.1 Attributnebensätze.	3
5.	Thema 5.1 Die Pandemie und ihre Auswirkungen.	3
6.	Thema 6.1 Konditionalis1. Komparativ.	3
7.	Thema 7.1 Andere Arten von Cyberkriminalität.	4
8.	Thema 8.1 Best of Cyberkrimi: die verrücktesten Hackerangriffe.	4

9.	Thema 9.1 Modalverben im Präsens.	3
10.	Thema 10.1 Rektion der Verben.	3
11.	Thema 11.1 Zustandspassiv.	3
12.	Thema 12.1 Nominales Prädikat. Imperfekt Aktiv.	3
13.	Thema 13.1 Cybercrime - Bekämpfung in der Ukraine.	4
14.	Thema 14.1 Schaffung neuer Bedürfnisse durch Werbung.	3
15.	Thema 15.1 Anlageformen.	4
16.	Thema 16.1 Ein paar staatliche Giganten.	4
	Разом за модуль	**54**

7. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

Технічні засоби : комп’ютер, мультимедійні презентації, відеоматеріали, чат, аудіозаписи тощо.
Обладнання: настільні та портативні комп’ютери, смартфони, портативні мультимедійні програвачі.
Програмне забезпечення: офісні програми (Google Meet, Moodle), програми для перегляду файлів (pdf, .djvu), електронні перекладачі текстів, електронні словники, мультимедійне програмне забезпечення тощо.

7. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. Канюк О.Л., Кіш Н.В. Методичні рекомендації з дисципліни «Іноземна мова для професійної комунікації (для спеціальності: 125 Кібербезпека та захист інформації» / О.Л.Канюк, Н.В.Кіш) – Ужгород: УжНУ, 2023. - 44 с.
2. Закон України Про Освіту https://urst.com.ua/act/pro_osvitu
3. Загальноєвропейські Рекомендації з мовної освіти: вивчення, викладання, оцінювання / Науковий редактор українського видання доктор пед. наук, проф. С.Ю. Ніколаєва. К.: Ленвіт, 2013. 273 с.

Допоміжна література

1.Cybercrime Report 2022. Lagebericht über die Entwicklung von Cybercrime. – Wien. 2023 // https://bundeskriminalamt.at › files › 2022-222

2. Cybercrime Report 2023. Lagebericht über die Entwicklung von Cybercrime // https://docplayer.org › 2284

3. Psychologische und neurologische Gründe für Cybercrime // https://link.springer.com › ar..

4. Cyberkriminalität: Übersicht zu aktuellen und // https://www.researchgate.net ›.

5. Cybercrime Report 2021 - Bundeskriminalamt // https://bundeskriminalamt.at › files › 2022-222

6. Cybercrime, Cyberkriminalität, Computerkriminalität - Anwalt.de // https://www.anwalt.de › cybe.

7. Cyberkriminalität in Deutschland: das Problem breitet sich … // https://www.marktforschung.de ›

8. Cyberversicherung für Unternehmen – Allianz // https://www.allianz.de › cybe..

9. Cyberversicherung für Privatpersonen // https://www.transparent-beraten.de › ...

Інформаційні ресурси в мережі Інтернет

1. Корпус текстів німецькою мовою https://www.dwds.de /
2. Тлумачний словник німецької мови https://www.duden.de/
3. Deutsches Wörterbuch von Jacob und Wilhelm Grimm. - http://Grimm.ADWGoettingen.gwdg.de/.
4. OWID. URL : https://www1.ids-mannheim.de/lexik/owid.html
5. PONS. Online-Wörterbuch. URL : https://de.pons.com/
6. WORTSCHATZ. Universität Leipzig. URL : https://wortschatz.unileipzig.de/de