МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ЦИФРОВИХ, ОСВІТНІХ ТА СОЦІАЛЬНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету
_____ Галина ГЕРАСИМЧУК
«28» серпня 2026 р.

ЗАТВЕРДЖУЮ
Перший проректор
_____ Надія КОВАЛЬЧУК
«29» серпня 2026 р.

СИЛАБУС

з освітнього компонента «Іноземна мова за професійним спрямуванням (англійська)»
ступінь вищої освіти – бакалавр
галузь знань – F Інформаційні технології
спеціальність – F5 Кібербезпека та захист інформації
освітня програма – Кібербезпека

Кафедра іноземної філології та прикладної лінгвістики

Силабус склали: доцент кафедри іноземної філології та прикладної лінгвістики, д.ф., доцент Ольга МЕЛЬНИЧУК; викладач (ПП) кафедри іноземної філології та прикладної лінгвістики Денис МАЛЕНИЦЬКИЙ; доцент кафедри іноземної філології та прикладної лінгвістики, к. ф. н., доцент Лариса ПИЛИПЮК

Силабус затверджений на засіданні кафедри іноземної філології та прикладної лінгвістики, протокол № 1б від «28» серпня 2026 р.

Завідувач кафедри к.пед.н., доцент Алла МАРТИНЮК

Розглянуто та схвалено групою забезпечення освітньої програми «Кібербезпека», протокол № 2 від «28» серпня 2026 р.

Гарант ОП «Кібербезпека» к.т.н., доцент Сергій КОСТЮЧКО

Схвалено науково-методичною радою університету, протокол № 1/а від «29» серпня 2026 р.

Затверджений силабус онлайн:
https://e.lntu.edu.ua/syllabus/1754

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Іноземна мова за професійним спрямуванням (англійська)»

Освітня програма	Кібербезпека
Галузь знань / Спеціальність	F Інформаційні технології / F5 Кібербезпека та захист інформації
Рівень вищої освіти	перший (бакалаврський)
Статус дисципліни	нормативна
Мова викладання	українська
Мова, що вивчається	англійська
Обсяг	6 кредитів ECTS / 180 годин, семестр 3, 4
Форма контролю	залік
Викладач(і)	д.ф., доцент Ольга МЕЛЬНИЧУК електронна пошта: o.melnychuk@lntu.edu.ua викладач (пп) Денис МАЛЕНИЦЬКИЙ к. ф. н., доцент Лариса ПИЛИПЮК

1. Мета і завдання дисципліни

Мета: Метою вивчення дисципліни «Іноземна мова за професійним спрямуванням» є формування у здобувачів вищої освіти іншомовної комунікативної компетентності, необхідної для ефективного усного та письмового спілкування у професійній, освітній і науковій сферах кібербезпеки, опрацювання фахової англомовної інформації та участі в міжнародній професійній взаємодії.

Завдання: Основними завданнями дисципліни є:
- формування та розширення англомовного термінологічного апарату у сфері інформаційних технологій і кібербезпеки;
- розвиток навичок читання, розуміння, аналізу та узагальнення англомовних фахових текстів;
- удосконалення вмінь професійного усного спілкування, зокрема участі в дискусіях, переговорах і командній роботі;
- розвиток навичок підготовки професійних повідомлень, електронних листів, звітів, інструкцій та презентацій англійською мовою;
- формування вмінь описувати кіберзагрози, вразливості, заходи захисту й процедури реагування на інциденти;
- розвиток здатності використовувати англомовні цифрові ресурси та професійну документацію;
- формування навичок представлення результатів індивідуальної та командної роботи англійською мовою;
- розвиток міжкультурної комунікативної компетентності та готовності до професійної взаємодії в міжнародному середовищі;
- формування здатності до самостійного вдосконалення професійної іншомовної компетентності.

Пререквізити: Іноземна мова

2. Компетентності

ІК — інтегральна компетентність: Здатність розв’язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.

ЗК03 — Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК04 — Здатність спілкуватися іноземною мовою.

3. Структура дисципліни, розподіл годин, зв'язок тем з компетентностями

№	Назва теми	Лекції денна/ заочна	Практ./ Семін./ лаб денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
Семестр 3. Змістовий модуль 1. English for Cybersecurity Fundamentals								
1	Тема 1. Careers and Professional Communication in Cybersecurity		8/2	15/21	23/23	МН1, МН2, МН3, МН4, МН5, МН6	МО2, МО3, МО4, МО7	ЗК03, ЗК04
2	Тема 2. Computer Systems and Networks		8/2	15/21	23/23	МН1, МН2, МН3, МН4, МН5, МН6	МО2, МО3, МО4, МО7	ЗК03, ЗК04
3	Тема 3. Cybersecurity Fundamentals		8/2	15/21	23/23	МН1, МН2, МН3, МН4, МН5, МН6	МО2, МО3, МО4, МО7	ЗК03, ЗК04
4	Тема 4. Malware and Social Engineering		6/–	15/21	21/21	МН1, МН2, МН3, МН4, МН5, МН6	МО2, МО3, МО4, МО7	ЗК03, ЗК04
Семестр 4. Змістовий модуль 2. Cybersecurity Operations and Professional Communication								
5	Тема 5. Data Protection and Privacy		8/2	15/21	23/23	МН1, МН2, МН3, МН4, МН5, МН6	МО2, МО3, МО4, МО7	ЗК03, ЗК04
6	Тема 6. Network and Cloud Security		8/–	15/21	23/21	МН1, МН2, МН3, МН4, МН5, МН6	МО2, МО3, МО4, МО7	ЗК03, ЗК04
7	Тема 7. Incident Response and Risk Management		8/2	15/21	23/23	МН1, МН2, МН3, МН4, МН5, МН6	МО2, МО3, МО4, МО7	ЗК03, ЗК04

№	Назва теми	Лекції денна/ заочна	Практ./ Семін./ лаб денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
8	Тема 8. Cybersecurity Policies and Professional Projects		6/2	15/21	21/23	МН1, МН2, МН3, МН4, МН5, МН6	МО2, МО3, МО4, МО7	ЗК03, ЗК04
	Разом	**0/0**	**60/12**	**120/168**	**180/180**			

Легенда: ЗК — загальна компетентність (номер за п. 2); СК — спеціальна (фахова) компетентність (номер за п. 2). Повне формулювання кожного коду наводиться в ОП / стандарті спеціальності.

Методи навчання: МН1 — словесний метод (лекція, дискусія, співбесіда тощо); МН2 — практичний метод (лабораторні та практичні заняття); МН3 — наочний метод (метод ілюстрацій і метод демонстрацій); МН4 — робота з навчально-методичною літературою (конспектування, тезування, анотування, рецензування, складання реферату); МН5 — відеометод у сполученні з новітніми інформаційними технологіями та комп'ютерними засобами навчання (дистанційні, мультимедійні, веб-орієнтовані тощо); МН6 — самостійна робота (розв'язання завдань).

Методи оцінювання: МО2 — усне або письмове опитування; МО3 — колоквіум; МО4 — тестування; МО7 — презентації результатів виконаних завдань та досліджень.

4. Результати навчання

ПРН02. Спілкування іноземною мовою з метою забезпечення ефективності професійної комунікації.

5. Цілі сталого розвитку

ЦСР 4 – Якісна освіта

ЦСР 8 – Гідна праця та економічне зростання

ЦСР 17 – Партнерство заради сталого розвитку

6. Неформальна освіта

Рекомендовані курси, тренінги, стажування та інші: результати навчання, здобуті у формальній, неформальній чи інформальній освіті, можуть бути визнані відповідно до процедур ЛНТУ. Підтвердженнями можуть бути сертифікати тематичних тренінгів, вебінарів чи онлайн-курсів разом з описом досягнутих результатів навчання та, за потреби, коротке верифікаційне завдання або портфоліо.

7. Критерії та форми контролю

Оцінювання — за 100-бальною шкалою (національна шкала / ЄКТС).

Семестр 3. Підсумковий бал = поточний контроль (40 %) + ІЗ/КПІЗ (20 %) + модульний контроль (40 %).

Семестр 4. Підсумковий бал = поточний контроль (40 %) + ІЗ/КПІЗ (20 %) + модульний контроль (40 %).

Академічна доброчесність: самостійне виконання завдань; коректне посилання на джерела; позначення частин тексту, згенерованих засобами ШІ. Порушення академічної доброчесності не толеруються.

8. Зміст тем

Тема 1. Careers and Professional Communication in Cybersecurity

IT and cybersecurity professions. Professional responsibilities. Workplace communication. Describing

skills and experience.

Тема 2. Computer Systems and Networks

Computer hardware and software. Operating systems. Networks and network devices. Technical specifications.

Тема 3. Cybersecurity Fundamentals

Basic cybersecurity concepts. Types of threats and vulnerabilities. The CIA triad. Cybersecurity terminology.

Тема 4. Malware and Social Engineering

Types of malware. Phishing and social engineering attacks. Warning users about online threats. Giving security advice.

Тема 5. Data Protection and Privacy

Personal and sensitive data. Data protection principles. Password security. Encryption and access control.

Тема 6. Network and Cloud Security

Network attacks. Firewalls and authentication. Cloud security risks. Describing security measures and procedures.

Тема 7. Incident Response and Risk Management

Reporting security incidents. Describing causes and consequences. Risk assessment. Incident response procedures.

Тема 8. Cybersecurity Policies and Professional Projects

Security policies and guidelines. Ethical issues in cybersecurity. Presenting a cybersecurity solution. Professional presentations.

9. Опис ІЗ/КПІЗ

Cybersecurity Awareness Campaign (створення англомовної інформаційної кампанії з кібербезпеки)

Мета КПІЗ:
розвиток здатності використовувати англійську мову для розв’язання професійних завдань у сфері кібербезпеки, опрацювання фахової інформації, створення цифрового контенту та представлення результатів роботи.

Зміст завдання:
здобувачі індивідуально або в малих групах розробляють англомовну інформаційну кампанію, спрямовану на підвищення обізнаності визначеної цільової аудиторії щодо однієї з актуальних проблем кібербезпеки.

Орієнтовні теми:

1. Phishing and social engineering;
2. Password security;
3. Personal data protection;
4. Safe use of public Wi-Fi;
5. Malware and ransomware;
6. Secure social media use;
7. Cyberbullying and online safety;
8. Mobile device security;
9. AI-related cybersecurity risks;
10. Secure remote work.

Етапи виконання:

Вибір проблеми й цільової аудиторії

Визначити тему, мету кампанії та цільову аудиторію.

Опрацювання англомовних джерел
Проаналізувати щонайменше три надійні англомовні джерела та скласти список ключових термінів.

Створення комплекту матеріалів
Підготувати:

інформаційний текст англійською мовою обсягом 300–400 слів;

цифрову інфографіку, постер або пам’ятку;

5–7 практичних рекомендацій для користувачів;

короткий слоган або повідомлення для соціальних мереж.

Представити кампанію англійською мовою у форматі 5–7-хвилинної презентації та відповісти на запитання.

Результат:
Англомовний цифровий комплект Cybersecurity Awareness Kit, що містить інформаційний матеріал, візуальний продукт, практичні рекомендації, список використаних джерел і презентацію.

10. Загальні вимоги

Освітній процес регулюється академічними правилами ЛНТУ. Здобувачі освіти зобов’язані ознайомитися з вимогами, визначеними Кодексом академічної доброчесності ЛНТУ та Політикою етичного використання штучного інтелекту в ЛНТУ, і дотримуватися принципів академічної доброчесності та етичного використання штучного інтелекту в освітній діяльності.

Академічна доброчесність. Учасники освітнього процесу зобов’язані дотримуватися Закону України «Про академічну доброчесність» від 18.12.2025 № 4742-IX та внутрішніх нормативних документів ЛНТУ. Не допускаються академічний плагіат, фабрикація, фальсифікація, привласнення авторства, несамостійне виконання завдань, а також недоброчесне використання результатів, згенерованих штучним інтелектом.

Використання штучного інтелекту. Інструменти штучного інтелекту можуть використовуватися для пошуку ідей, пояснення методів, попереднього структурування, мовного редагування та допоміжного аналізу неконфіденційних даних, якщо конкретне завдання не передбачає повністю самостійного виконання. Здобувач освіти має зазначати використаний інструмент, мету та етап його застосування, перевіряти факти й розрахунки та самостійно обґрунтовувати висновки.

11. Література

І. Навчально-методичні матеріали та розробки

Праці інших авторів:

1. Павліна Т. В. English for Cybersecurity Students: навчальний посібник з англійської мови. Харків: Харківський національний університет внутрішніх справ, 2026.

2. Акмалдінова О. М., Гурська О. О., Теремінко Л. Г., Сорокун Г. В. Professional English. Cybersecurity and Data Protection: навчальний посібник. Київ: КАІ, 2025. 91 с. ISBN 978-966-932-223-4.

3. Evans V., Dooley J., Wright S. Career Paths: Information Technology. 2nd ed. Student’s Book. Express Publishing. ISBN 978-1-3992-0578-8.

4. Esteras S. R., Fabre E. M. Professional English in Use: ICT. Cambridge: Cambridge University Press, 2007. ISBN 978-0-521-68543-6.

5. Hill D., Bonamy D. English for Information Technology 2. Harlow: Pearson Education, 2012. 80 p. ISBN 978-1-4082-6990-9.

6. Evans V., Dooley J., Kennedy W. Career Paths: Computing. 2nd ed. Student’s Book. Express Publishing. ISBN 978-1-3992-0576-4. Express Publishing

7. Esteras S. R. Infotech: English for Computer Users. 4th ed. Cambridge: Cambridge University Press, 2008. 168 p. ISBN 978-0-521-70299-7.

8. Glendinning E. H., McEwan J. Oxford English for Information Technology. 2nd ed. Oxford: Oxford University Press, 2014. 222 p. ISBN 978-0-19-457492-1.

9. Olejniczak M. English for Information Technology 1. Pearson Longman, 2011. 79 p. ISBN 978-1-4082-6996-1.

10. Andrzejczyk A. English for Security in Cyberspace. Szczytno: Police Academy Publishing House, 2025. 48 p. ISBN 978-83-7462-902-7.

11. Butterfield A., Ngondi G. A Dictionary of Computer Science. 7th ed. Oxford: Oxford University Press, 2016. ISBN 978-0-19-968897-5.

III. Інформаційні ресурси

12. National Institute of Standards and Technology. Cybersecurity Framework 2.0. URL: https://www.nist.gov/cyberframework NIST

13. Cybersecurity and Infrastructure Security Agency. CISA Learning. URL: https://www.cisa.gov/resources-tools/resources/cisa-learning cisa.gov

14. European Union Agency for Cybersecurity. ENISA. URL: https://www.enisa.europa.eu enisa.europa.eu

15. ENISA Threat Landscape. URL: https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape European Union

16. OWASP Foundation. Web Application and Generative AI Security Resources. URL: https://owasp.org

17. NIST Cybersecurity and Privacy Training Resources. URL: https://www.nist.gov/itl/smallbusinesscyber/training