МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету
_____ Інна КОНДЮС
«29» серпня 2026 р.

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

СИЛАБУС

з освітнього компонента «Основи кібербезпеки»
ступінь вищої освіти – бакалавр
галузь знань – F Інформаційні технології
спеціальність – F5 Кібербезпека та захист інформації
освітня програма – Кібербезпека

Кафедра кібербезпеки

Силабус склав(ла) старший викладач кафедри кібербезпеки Оксана МІСКЕВИЧ

Силабус затверджений на засіданні кафедри кібербезпеки, протокол № 2 від «28» серпня 2026 р.

Завідувач кафедри к.т.н., доцент Сергій КОСТЮЧКО

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/2533

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Основи кібербезпеки»

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
Обсяг	5 кредитів ECTS / 150 годин, семестр 2
Форма контролю	екзамен
Викладач(і)	старший викладач Оксана МІСКЕВИЧ

1. Мета і завдання дисципліни

Мета: формування у здобувачів освіти базових знань і практичних навичок у сфері кібербезпеки, розуміння основних кіберзагроз і вразливостей інформаційних систем, принципів забезпечення конфіденційності, цілісності та доступності інформації, а також опанування базових методів і засобів захисту інформаційних ресурсів, виявлення кіберзагроз та протидії кібератакам.

Завдання: набуття практичних навичок застосування базових засобів захисту інформації, забезпечення безпеки облікових записів, мережевих з’єднань і персональних даних; ознайомлення з методами виявлення, оцінювання та попередження кіберзагроз, а також формування вмінь застосовувати організаційні й технічні заходи для захисту інформаційних ресурсів.

Пререквізити: -

2. Компетентності

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

ЗК08 — Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

СК01 — Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.

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

№	Назва теми	**Лекції** денна/ заочна	**Лаб.** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**ЗК та СК**
Змістовий модуль 1. Основи кібербезпеки та концепції кібератак								
1	Тема 1. Вступ до кібербезпеки: основні поняття, цілі та принципи	4/1	4/1	10/10	18/12	МН1, МН2, МН4, МН6	МО1, МО2, МО4	ЗК08, СК01

№	Назва теми	Лекції денна/ заочна	Лаб. денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
2	Тема 2. Нормативно-правова база та стандарти кібербезпеки	2/0,5	2/0,5	5/10	9/11	МН1, МН2, МН4, МН6	МО1, МО2, МО4	ЗК08, СК01
3	Тема 3. Інформаційні ресурси та модель куба кібербезпеки Маккамбера	2/0,25	2/0,25	5/10	9/10,5	МН1, МН2, МН4, МН6	МО1, МО2, МО4	ЗК08, СК01
4	Тема 4. Кібернападники та кібервійна: типи, мотиви й цілі	2/0,25	2/0,25	5/10	9/10,5	МН1, МН2, МН4, МН6	МО1, МО2, МО4	ЗК08, СК01
5	Тема 5. Кібератаки: класифікація, концепції та етапи реалізації	4/0,5	4/0,5	10/10	18/11	МН1, МН2, МН4, МН6	МО1, МО2, МО4	ЗК08, СК01
6	Тема 6. Методи проникнення в інформаційні системи та експлуатація вразливостей	2/0,5	2/0,5	5/20	9/21	МН1, МН2, МН4, МН6	МО1, МО2, МО4	ЗК08, СК01
Змістовий модуль 2. Методи та засоби захисту пристроїв та даних								
7	Тема 7. Захист кінцевих пристроїв і мережевої інфраструктури	2/0,5	2/0,5	10/20	14/21	МН1, МН2, МН4, МН6	МО1, МО2, МО4	ЗК08, СК01
8	Тема 8. Збереження даних, право власності на інформацію та захист онлайн-приватності	4/1	4/1	10/10	18/12	МН1, МН2, МН4, МН6	МО1, МО2, МО4	ЗК08, СК01
9	Тема 9. Технічні засоби та технології кібербезпеки	4/0,5	4/0,5	10/5	18/6	МН1, МН2, МН4, МН6	МО1, МО2, МО4	ЗК08, СК01
10	Тема 10. Поведінкові аспекти кібербезпеки та безпечна поведінка користувачів	2/0,5	2/0,5	5/5	9/6	МН1, МН2, МН4, МН6	МО1, МО2, МО4	ЗК08, СК01

№	Назва теми	**Лекції** денна/ заочна	**Лаб.** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**ЗК та СК**
11	Тема 11. Інструменти виявлення кіберінцидентів та запобігання кіберзагрозам	2/0,5	2/0,5	5/8	9/9	МН1, МН2, МН4, МН6	МО1, МО2, МО4	ЗК08, СК01
	ІЗ/КПІЗ			10/20	10/20			
	Разом	**30/6**	**30/6**	**90/138**	**150/150**			

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); МН4 — робота з навчально-методичною літературою (конспектування, тезування, анотування, рецензування, складання реферату); МН6 — самостійна робота (розв'язання завдань).

Методи оцінювання: МО1 — екзамен; МО2 — усне або письмове опитування; МО4 — тестування.

4. Результати навчання

ПРН03. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

ПРН09. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

5. Цілі сталого розвитку

ЦСР 4 – Якісна освіта

ЦСР 9 – Промисловість, інновації та інфраструктура

ЦСР 16 – Мир, справедливість та сильні інститути

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). Підсумковий бал = поточний контроль (30 %) + ІЗ/КПІЗ (10 %) + модульний контроль (20 %) + екзамен (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. Вступ до кібербезпеки: основні поняття, цілі та принципи

Поняття кібербезпеки та інформаційної безпеки, їх взаємозв'язок.
Мета, завдання та основні напрями кібербезпеки.
Об'єкти кіберзахисту: інформація, інформаційні системи, комп'ютерні мережі та цифрові пристрої.
Основні поняття кібербезпеки: активи, кіберзагрози, вразливості, ризики та кіберінциденти.

Основні тенденції розвитку кіберзагроз і сучасні виклики у сфері кібербезпеки.

Тема 2. Нормативно-правова база та стандарти кібербезпеки

Поняття та структура нормативно-правового регулювання кібербезпеки.
Законодавство України у сфері кібербезпеки.
Державна система кібербезпеки України.
Міжнародні стандарти інформаційної безпеки та кібербезпеки.
Європейські нормативні вимоги у сфері кібербезпеки.
Відповідальність за порушення вимог інформаційної безпеки.

Тема 3. Інформаційні ресурси та модель куба кібербезпеки Маккамбера

Інформаційні ресурси організації: поняття, види, класифікація та цінність даних.
Типи організаційних даних: публічні, внутрішні, конфіденційні та персональні дані.
Куб кібербезпеки Маккамбера (McCumber Cube): призначення, структура та принципи використання.
Тріада CIA: конфіденційність, цілісність і доступність інформації.
Стани існування даних: дані під час зберігання, передавання та оброблення.
Застосування куба Маккамбера для аналізу загроз і вибору заходів захисту інформаційних ресурсів.

Тема 4. Кібернападники та кібервійна: типи, мотиви й цілі

Поняття та класифікація кібернападників.
Мотиви та цілі кібернападників.
Поняття та особливості кібервійни.
Протидія кібернападам і кібероперація̈м.

Тема 5. Кібератаки: класифікація, концепції та етапи реалізації

Поняття та основні характеристики кібератак.
Класифікація кібератак.
Основні цілі та наслідки кібератак.
Етапи реалізації цілеспрямованої кібератаки.
Типові техніки кібератак.
Виявлення та аналіз ознак кібератак.
Методи протидії кібератакам.

Тема 6. Методи проникнення в інформаційні системи та експлуатація вразливостей

Поняття вразливостей та експлойтів.
Класифікація вразливостей інформаційних систем.
Типові вразливості вебзастосунків і мережевих служб.
Ідентифікація та оцінювання вразливостей.
Інструменти виявлення та дослідження вразливостей.

Тема 7. Захист кінцевих пристроїв і мережевої інфраструктури

Поняття та принципи захисту кінцевих пристроїв.
Засоби захисту кінцевих пристроїв.
Безпечне налаштування операційних систем.
Засоби захисту мережевої інфраструктури.
Захист бездротових мереж.
Моніторинг і виявлення загроз.

Тема 8. Збереження даних, право власності на інформацію та захист онлайн-приватності

Поняття та способи збереження даних.
Резервне копіювання та відновлення даних.
Персональні дані та права користувачів.
Поняття онлайн-приватності.
Методи захисту онлайн-приватності.
Захист даних у хмарних сервісах.

Тема 9. Технічні засоби та технології кібербезпеки

Поняття та класифікація засобів кібербезпеки.
Антивірусні засоби та технології захисту кінцевих пристроїв.
Системи виявлення та запобігання вторгненням.
Безпека паролів.
Засоби криптографічного захисту інформації.

Тема 10. Поведінкові аспекти кібербезпеки та безпечна поведінка користувачів

Безпека на основі поведінки.
Моніторинг мережевого трафіку NetFlow.
Тестування на проникнення.
Управління ризиками.

Тема 11. Інструменти виявлення кіберінцидентів та запобігання кіберзагрозам

Поняття та класифікація інструментів кібербезпеки.
Засоби моніторингу подій безпеки.
Індикатори компрометації (IOC) та кіберрозвідка.
Методи запобігання кіберзагрозам.
Оцінювання ефективності засобів кіберзахисту.

9. Опис ІЗ/КПІЗ

- Виконання КПІЗ є одним із обов'язкових складових модулів залікового кредиту з дисципліни «Основи кібербезпеки». Індивідуальне завдання з дисципліни «Основи кібербезпеки» виконується самостійно кожним студентом. Підготовка завдання здійснюється на основі методичних вказівок до виконання самостійної роботи з дисципліни «Основи кібербезпеки», опрацьованої літератури, лабораторних робіт, конспекту лекцій та зібраної інформації в мережі Інтернет, її аналізу та формулювання висновків. КПІЗ оформляється відповідно до встановлених вимог.
  Завдання виконання комплексного практичного індивідуального завдання полягає у обґрунтованому виборі оптимальних структур та алгоритмів для вирішення прикладних задач.
  В індивідуальній роботі студенти повинні показати:
  - правильне розуміння поставленого завдання;
  - вміння працювати з літературними джерелами;
  - можливість використовувати теоретичні знання, отримані на лекціях, застосовувати сучасні підходи до вирішення прикладних задач.

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. Євсеєв С. П.. Основи кібербезпеки: навчально-практичний посібник. Львів : ПП «Новий Світ-2000», 2025. 320 с.

ІІ. Наукові праці

Праці автора силабуса:

2. Khrystynets N., Melnyk K., Lavrenchuk S., Miskevych O., Kostiuchko S. Multiprocessing as a Way to Optimize Queries. Advances in Transdisciplinary Engineering. 2024. No. 48. P. 455–464. DOI: https://doi.org/10.3233/ATDE231357.

3. Багнюк Н. В., Мельник К. В., Бортник К. Я., Міскевич О. І., Карасійчук Д. Я. Автоматизація керування конфігураціями комп'ютерних систем за допомогою Ansible та підходу «Infrastructure as Code». Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2026. № 63. С. 145-153. URL: https://repository.lntu.edu.ua/handle/123456789/3569

4. Міскевич О. І., Омельчук Д. Ю. Ручне та автоматизоване тестування блокчейну за допомогою Postman. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2023. № 53. С. 23–30. URL: https://repository.lntu.edu.ua/handle/123456789/4455

5. Міскевич О. І. Аналіз роботи мережевих утиліт в командному вікні Windows. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2023. № 50. С. 84–89. URL: https://repository.lntu.edu.ua/handle/123456789/4449

6. Міскевич О. І., Столенко І. О., Куліков Н. О. Фреймворк testNG як інструмент для написання тестів. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2023. № 53. С. 152–157. URL: https://repository.lntu.edu.ua/handle/123456789/4456

ІІІ. Інформаційні ресурси

7. Introduction to Cybersecurity: онлайн-курс. Cisco Networking Academy. URL: https://www.netacad.com/courses/introduction-to-cybersecurity?courseLang=en-US

8. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19