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

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

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

СИЛАБУС

з освітнього компонента «Етичний хакер»
ступінь вищої освіти – бакалавр
галузь знань – 12 Інформаційні технології
спеціальність – 126 Інформаційні системи та технології
освітня програма – Інформаційні системи та технології охорони і безпеки

Кафедра комп'ютерної інженерії та охоронних систем

Силабус склав(ла) доцент кафедри комп'ютерної інженерії та охоронних систем, к.т.н., доцент Наталія БАГНЮК

Силабус затверджений на засіданні кафедри комп'ютерної інженерії та охоронних систем, протокол № 1/1 від «29» серпня 2026 р.

Завідувач кафедри к.т.н., доцент Тарас ТЕРЛЕЦЬКИЙ

Розглянуто та схвалено групою забезпечення освітньої програми «Інформаційні системи та технології охорони і безпеки», протокол № 2 від «29» серпня 2026 р.

Гарант ОП «Інформаційні системи та технології охорони і безпеки» к.т.н., доцент Тарас ТЕРЛЕЦЬКИЙ

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

Затверджений силабус онлайн:
https://e.lntu.edu.ua/syllabus/3609

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Етичний хакер»

Освітня програма	Інформаційні системи та технології охорони і безпеки
Галузь знань / Спеціальність	12 Інформаційні технології / 126 Інформаційні системи та технології
Рівень вищої освіти	перший (бакалаврський)
Статус дисципліни	вибіркова
Мова викладання	українська
Обсяг	5 кредитів ECTS / 150 годин
Форма контролю	залік
Викладач(і)	к.т.н., доцент Наталія БАГНЮК

1. Мета і завдання дисципліни

Мета: стійкість кібербезпеки в сучасному світі не може бути лише додатком – це необхідність. Фахівці з агресивної безпеки, як от етичні хакери та тестери на проникнення, можуть допомогти завчасно виявити невідомі загрози та усунути їх раніше, ніж це зроблять кіберзлочинці.
Мета викладання дисципліни: підготовка до навичок етичного хакера, чітке розуміння наступальної безпеки, забезпечення навиків визначення обсягу, виконання та звітування про оцінку вразливості, а також рекомендацій стратегії пом’якшення.

Завдання: завдання курсу «Етичний хакер» полягають у формуванні у студентів ґрунтовного розуміння концепцій наступальної безпеки, навичок етичного хакерства та відмінностей між легальним тестуванням на проникнення і протиправною діяльністю кіберзлочинців. Вивчення даної дисципліни дає можливість навчитися визначати обсяг тестування, формулювати його цілі та межі з урахуванням етичних і правових аспектів, а також опанувати практичні навички збору інформації, сканування, виявлення та експлуатації вразливостей із дотриманням принципів відповідального розкриття. Особлива увага приділяється аналізу результатів, правильному документуванню знайдених слабких місць і підготовці звітів для різних аудиторій з рекомендаціями щодо усунення ризиків. Важливою складовою завдань є розвиток критичного мислення і здатності мислити як потенційний зловмисник, що дозволяє передбачати шляхи атак і підвищувати ефективність захисних заходів. Також набуваються уміння працювати із сучасними інструментами тестування на проникнення, дотримуючись вимог безпеки під час їх застосування. Значна увага приділяється формуванню навичок професійної комунікації зі стейкхолдерами, відповідального розкриття вразливостей і презентації результатів перевірок. Завдяки відпрацюванню практичних кейсів та сценаріїв майбутні фахівці здатні контролювати, аналізувати й ефективно реагувати на актуальні загрози кіберпростору.

2. Компетентності

КС.6 — Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов’язків

КС.10 — Здатність вибору, проектування, розгортання, інтегрування, управління, адміністрування та супроводжування інформаційних систем, технологій та інфокомунікацій, сервісів та інфраструктури організації.

КС.12 — Здатність управляти та користуватися сучасними інформаційнокомунікаційними системами та технологіями (у тому числі такими, що базуються на використанні Інтернет).

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**	**СК**
Змістовий модуль 1. Тестування на проникнення та збір інформації.								
1	Тема 1. Вступ до етичного хакерства та тестування на проникнення.	2/0,5	2/0,5	4/10	8/11	МН1, МН2	МО2, МО4, МО9, захист практичної роботи	
2	Тема 2. Планування та визначення обсягу тестування на проникнення.	2/0,5	2/0,5	4/10	8/11	МН1, МН2	МО2, МО4, МО9, захист практичної роботи	
3	Тема 3. Збір інформації та сканування вразливостей.	4/1	6/0,5	8/18	18/19,5	МН1, МН2	МО2, МО4, МО9, захист практичної роботи	
4	Тема 4. Атаки соціальної інженерії.	2/0,5	2/0,5	12/14	16/15	МН1, МН2	МО2, МО4, МО9, захист практичної роботи	
5	Тема 5. Використання дротових і бездротових мереж.	4/0,5	4/1	12/16	20/17,5	МН1, МН2	МО2, МО4, МО9, захист практичної роботи	
Змістовий модуль 2. Вразливості та аналіз коду.								
6	Тема 6. Використання вразливостей програми.	4/0,5	10/2	12/10	26/12,5	МН1, МН2	МО2, МО4, МО9, захист практичної роботи	
7	Тема 7. Хмарна, мобільна та безпека Інтернету речей.	4/1		10/10	14/11	МН1, МН2	МО2, МО4, МО9	
8	Тема 8. Виконання методів після експлуатації.	4/0,5		8/16	12/16,5	МН1, МН2	МО2, МО4, МО9	

№	Назва теми	**Лекції** денна/ заочна	**Практ./ Семін./ лаб** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**СК**
9	Тема 9. Звітність та комунікація.	2/0,5	4/1	8/14	14/15,5	МН1, МН2	МО2, МО4, МО9, захист практичної роботи	
10	Тема 10. Інструменти та аналіз коду.	2/0,5		12/20	14/20,5	МН1, МН2	МО2, МО4, МО9	
	Разом	**30/6**	**30/6**	**90/138**	**150/150**			

Легенда: 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).

Методи оцінювання: МО2 — усне або письмове опитування; МО4 — тестування; МО9 — залік.

4. Результати навчання

Результати навчання з дисципліни «Етичний хакер» передбачають формування у студентів глибоких знань про принципи наступальної безпеки, особливості діяльності етичних хакерів та методологію тестування на проникнення. Після опанування курсу студенти володітимуть розумінням основних етапів проведення пентесту, від збору інформації до аналізу та представлення результатів, а також знатимуть сучасні інструменти, методи і технології, що застосовуються у цій сфері. Студенти зможуть застосовувати здобуті знання на практиці, здійснювати аналіз вразливостей та моделювати реальні сценарії атак, мислячи з позиції потенційного зловмисника. Важливим результатом стане розвиток умінь формувати звіти для різних аудиторій, включаючи технічний і управлінський рівні, надавати рекомендації щодо усунення виявлених ризиків і впровадження ефективних стратегій пом’якшення наслідків. Також здобувачі набудуть компетентностей у сфері етичних і правових аспектів роботи етичного хакера, що дозволить їм професійно взаємодіяти зі стейкхолдерами та відповідально розкривати виявлені вразливості. Після завершення навчання випускники зможуть ефективно інтегрувати здобуті знання у свою професійну діяльність у сфері кібербезпеки, забезпечуючи проактивне виявлення і нейтралізацію загроз у сучасному цифровому середовищі.

5. Цілі сталого розвитку

ЦСР 4 – Якісна освіта

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 (50 %) + модульний контроль (50 %).

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 етичного хакерства та тестування на проникнення.

Розуміння етичного хакінгу та тестування на проникнення, вивчення методів тестування на проникнення та створення власної лабораторії.

Тема 2. Планування та визначення обсягу тестування на проникнення.

Порівняння та зіставлення концепцій управління, ризиків та комплаєнсу, пояснення важливості визначення обсягу робіт та вимог організації або клієнта, а також демонстрація етичного хакерського мислення шляхом підтримки професіоналізму та чесності.

Тема 3. Збір інформації та сканування вразливостей.

Виконання пасивної розвідки, проведення активної розвідки, розуміння мистецтва виконання сканування вразливостей та розуміння того, як аналізувати результати сканування на вразливості.

Тема 4. Атаки соціальної інженерії.

Використання приводу для підходу та видавання себе за іншу особу, атаки соціальної інженерії, фізичні напади, інструменти соціальної інженерії та методи впливу.

Тема 5. Використання дротових і бездротових мереж.

Використання мережевих вразливостей та вразливостей бездротового зв'язку.

Тема 6. Використання вразливостей програми.

Огляд атак на веб-застосунки для фахівців із безпеки та топ-10 OWASP, як створити власну лабораторію веб-застосунків, розуміння недоліків бізнес-логіки, розуміння вразливостей, пов’язаних з ін’єкціями, використання вразливостей на основі автентифікації, використання вразливостей, пов’язаних з авторизацією, розуміння вразливостей міжсайтового скриптингу (XSS), розуміння підробки міжсайтових запитів (CSRF/XSRF) та атак підробки запитів на стороні сервера, розуміння клікіджекингу, використання неправильних конфігурацій безпеки, використання вразливостей включення файлів та використання небезпечних практик коду.

Тема 7. Хмарна, мобільна та безпека Інтернету речей.

Дослідження векторів атак та здійснення атак на хмарні технології, пояснення поширених атак та вразливостей проти спеціалізованих систем.

Тема 8. Виконання методів після експлуатації.

Створення опори та підтримка стійкості після компрометації системи, а також розуміння того, як виконувати бічний рух, уникати виявлення та переховування.

Тема 9. Звітність та комунікація.

Порівняння та зіставлення важливих компонентів письмових звітів, аналіз результатів та рекомендації щодо відповідних коригуючих заходів у звіті, пояснення важливості комунікації під час процесу тестування на проникнення та пояснення дій після подання звіту.

Тема 10. Інструменти та аналіз коду.

Розуміння основних концепцій сценаріїв та розробки програмного забезпечення, а також розуміння різних варіантів використання інструментів тестування на проникнення та аналізу коду експлойту.

9. Опис ІЗ/КПІЗ

Не передбачено навчальним планом.

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 автора силабуса:

1. Комп’ютерні мережі : конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Комп’ютерна інженерія» галузі знань 12 (F) Інформаційні технології спец. 123 (F7) Комп’ютерна інженерія денної та заоч. форм навч. / уклад.: Н. В. Багнюк, Д. В. Гордєєва. Луцьк : ЛНТУ, 2026 116 с. URL: https://repository.lntu.edu.ua/handle/123456789/1695

2. Адміністрування комп’ютерних мереж та систем : конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Комп’ютерна інженерія» галузі знань 12 (F) Інформаційні технології спец. 123 (F7) Комп’ютерна інженерія денної та заоч. форм навч. / уклад.: Н. В. Багнюк, К. Я. Бортник. Луцьк : ЛНТУ, 2026. 328 с. URL: https://repository.lntu.edu.ua/handle/123456789/1630

3. Інформаційні мережі та адміністрування : конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12/F Інформаційні технології спец. 126/F6 Інформаційні системи та технології денної та заоч. форм навч. / уклад.: Н. В. Багнюк, О. Л. Кайдик. Луцьк : ЛНТУ, 2026. 236 с. URL: https://repository.lntu.edu.ua/handle/123456789/2756

Праці інших авторів:

4. Cisco Networking Academy: Ethical Hacker. URL: https://www.netacad.com/courses/ethical-hacker?courseLang=en-US (date of access: 26.06.2026).

5. Підручник з етичного хакерства. Guru99. URL: https://www.guru99.com/uk/ethical-hacking-tutorials.html (дата звернення: 26.06.2026).

6. Посібник з хакінгу за допомогою Kali Linux. URL: https://hackyourmom.com/osvita/posibnyk-z-hakingu-za-dopomogoyu-kali-linux/?utm_source=chatgpt.com (дата звернення: 26.06.2026).

7. GigaCloud About. Що таке Етичний хакер та чому за ними майбутнє, 2023. YouTube. URL: https://www.youtube.com/watch?v=6_pLtA9OTNs (дата звернення: 26.06.2026).

8. Етичний хакер, що це таке та як розпочати кар’єру у сфері кібербезпеки. https://hackyourmom.com/osvita/etychnyj-haker-shho-cze-take-ta-yak-rozpochaty-karyeru-u-sferi-kiber bezpeky/ (дата звернення: 26.06.2026).

9. Девопс На Дроті. Devops - різниця між віртуальними машинами та контейнерами, 2022. YouTube. URL: https://www.youtube.com/watch?v=I_XRrnNt_d0 (дата звернення: 26.06.2026).

10. OWASP Top 10:2021. OWASP Foundation, the Open Source Foundation for Application Security. OWASP Foundation. URL: https://owasp.org/Top10/?utm_source=chatgpt.com (date of access: 26.06.2026).

11. Free Ebook: OSCP & PEN-200 Prep. OffSec. OffSec. URL: https://www.offsec.com/resources/guides/ebook-oscp-prep-pen200/?utm_source=chatgpt.com (date of access: 26.06.2026).

12. NIST SP 800-61. NIST. URL: https://www.nist.gov/privacy-framework/nist-sp-800-61 (date of access: 26.06.2026).

13. Security Onion Solutions. 30Security Onion Solutions. URL: https://securityonionsolutions.com/software (date of access: 26.06.2026).

14. Prometheus - Monitoring system & time series database. Prometheus - Monitoring system & time series database. URL: https://prometheus.io/ (date of access: 26.06.2026).

15. OpenSearch. OpenSearch. URL: https://opensearch.org/ (date of access: 26.06.2026)

16. Security and Privacy Controls for Information Systems and Organizations. NIST. URL: https://www.nist.gov/publications/security-and-privacy-controls-information-systems-and-organizations-0 (date of access: 26.06.2026).

ІІ. Наукові праці

Праці автора силабуса:

17. 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. Луцьк, 2026. № 63. С. 145-153. URL: https://repository.lntu.edu.ua/handle/123456789/3569

18. Мельник В. М., Багнюк Н. В., Ройко О. Ю., Кізим С. О. Мережеві сокети на основі псевдонімів з віддаленою передачею адрес. Комп’ютерно-інтегровані технології: освіта, наука, виробництво. Луцьк, 2025. № 59. С. 194-204. URL: https://repository.lntu.edu.ua/handle/123456789/6371

19. Мельник В. М., Багнюк, Н. В., Корчук О. І. Пошук прихованих помилок програмного використання пам’яті програмним кодом C++ за допомогою статичного аналізу Deep Learning. Комп’ютерно-інтегровані технології: освіта, наука, виробництво. Луцьк, 2025. № 61. С. 156-163. URL: https://repository.lntu.edu.ua/handle/123456789/6372

20. Melnyk, V., Bahniuk, N., Bortnyk, K., Kondius, I., Zubovetska, N., & Kondius, K. Development of Network Traffic Monitoring System Elements Using Deep Learning. Dependable Systems, Services and Technologies: 14th International Conference. (Athens, Greece, October 11–13, 2024.). Piscataway, NJ: IEEE, 2024. P. 1–7. URL: https://repository.lntu.edu.ua/handle/123456789/3557

21. Melnyk V., Bahniuk N., Roiko O., Bortnyk K., Kizym S. Socket performance influence on data processing intensity in a virtual machine cluster with heterogeneous conditions. Комп’ютерно-інтегровані технології: освіта, наука, виробництво. 2024. № 55. С. 143-154. URL: https://repository.lntu.edu.ua/handle/123456789/3648

22. Bahniuk N., Linchuk O., Bortnyk K., Kondius I., Melnyk K., Kondius K. Threats Detection and Analysis Based on SYSMON Tool // 2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT). Athens, Greece, 2023. P. 1–7. DOI: 10.1109/DESSERT61349.2023.10416443. URL: https://repository.lntu.edu.ua/handle/123456789/3643

23. Мельник В. М., Багнюк Н. В., Бортник К. Я., Лінчук О. М. Система моніторингу веб-ресурсів за допомогою Elasticsearch. Комп’ютерно-інтегровані технології: освіта, наука, виробництво. 2023. № 51. С. 59-72. URL: https://repository.lntu.edu.ua/handle/123456789/3646

24. Кардашук В., Бортник К., Багнюк Н. Проблеми захисту інформації у віртуальних приватних мережах та захисту від атак на Web-додатки. Комп’ютерно-інтегровані технології: освіта, наука, виробництво. 2023. № 53, С. 117-124. URL: https://repository.lntu.edu.ua/handle/123456789/3738

25. Бортник, К., Ярощук, Б., Багнюк Н., Пех, П. Подолання проблем у навчанні штучного інтелекту : обмеження даних, обчислювальні витрати та стійкість моделі. Комп’ютерно-інтегровані технології: освіта, наука, виробництво. 2023. № 53, С. 37-43. URL: https://repository.lntu.edu.ua/handle/123456789/3737

26. Багнюк Н. В., Бортник К. Я., Варченко Л. Л. Моніторингова система для операційної системи Windows. Комп’ютерно-інтегровані технології: освіта, наука, виробництво. 2022. № 49. С. 18-23. URL: https://repository.lntu.edu.ua/handle/123456789/3629

Праці інших авторів:

27. Hemalatha S., Jency A., Gnanasekar A. та ін. A Comprehensive Survey on Ethical Hacking, Footprinting, and AI-Driven Penetration Testing in Modern Cybersecurity. International Journal of Safety and Security Engineering. 2026. Vol. 16, no. 4. P. 837–848. DOI: 10.18280/ijsse.160411

III. Інформаційні ресурси

28. Електронний освітній портал ЛНТУ https://mdl.lntu.edu.ua/.

29. Репозиторій ЛНТУ https://repository.lntu.edu.ua/home

30. Мережева академія Cisco https://www.netacad.com/ (дата звернення: 26.06.2026).

31. Курс мережевої академії Cisco Packet Tracer (Курс-інструкція до симулятору мереж та IoT). Доступний з URL https://www.netacad.com/courses/getting-started-cisco-packet-tracer?courseLang=en-US (дата звернення: 26.06.2026).