**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 «Аналіз шкідливого програмного забезпечення»**
**ступінь вищої освіти – бакалавр**
**галузь знань – 12 Інформаційні технології**
**спеціальність – 123 Комп'ютерна інженерія**
**освітня програма – Комп'ютерна інженерія**

**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 «Комп'ютерна інженерія», протокол № 2 від «27» серпня 2026 р.

Гарант ОП «Комп'ютерна інженерія» к.т.н., доцент Світлана ЛАВРЕНЧУК

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

Затверджений силабус онлайн:
https://e.lntu.edu.ua/syllabus/2061

**Луцьк – 2026**

**СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Аналіз шкідливого програмного забезпечення»**

| | |
|---|---|
| **Освітня програма** | Комп'ютерна інженерія |
| **Галузь знань / Спеціальність** | 12 Інформаційні технології / 123 Комп'ютерна інженерія |
| **Рівень вищої освіти** | перший (бакалаврський) |
| **Статус дисципліни** | вибіркова |
| **Мова викладання** | українська |
| **Обсяг** | 5 кредитів ECTS / 150 годин, семестр 8 |
| **Форма контролю** | залік |
| **Викладач(і)** | старший викладач Оксана МІСКЕВИЧ<br>електронна пошта: miskevych.o@lutsk-ntu.com.ua |

## 1. Мета і завдання дисципліни

**Мета:** формування знань і практичних навичок щодо виявлення, дослідження та аналізу шкідливого програмного забезпечення, застосування методів статичного і динамічного аналізу, визначення його функціональних характеристик та оцінювання пов’язаних із ним кіберзагроз.

**Завдання:** вміти виявляти шкідливе програмне забезпечення, проводити аналіз шкідливих програм, розуміти технічні аспекти функціонування шкідливих програм; зменшувати негативні наслідки від впливу шкідливого програмного забезпечення; впроваджувати програмні засоби.

**Пререквізити:** -

## 2. Компетентності

**СК18** — Здатність аналізувати безпеку мереж та вживати заходів для захисту даних

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

| № | Назва теми | Лекції | Практ./ Семін./ лаб | Самост. робота | Разом | Методи навчання | Методи оцінювання | СК |
|---|---|---|---|---|---|---|---|---|
| **Змістовий модуль 1. Основні види шкідливого програмного забезпечення** | | | | | | | | |
| 1 | Тема 1. Основні види шкідливого програмного забезпечення. Термінологічний базис | 4 | 4 | 10 | 18 | МН1, МН2, МН4, МН6 | МО2, МО4, МО9 | СК18 |
| 2 | Тема 2. Аналіз проявів та ознак шкідливого ПЗ | 4 | 4 | 10 | 18 | МН1, МН2, МН4, МН6 | МО2, МО4, МО9 | СК18 |
| 3 | Тема 3. Руткіти, бекдори та прихований запуск шкідливого ПЗ | 4 | 4 | 10 | 18 | МН1, МН2, МН4, МН6 | МО2, МО4, МО9 | СК18 |

| № | Назва теми | Лекції | Практ./ Семін./ лаб | Самост. робота | Разом | Методи навчання | Методи оцінювання | СК |
|---|---|---|---|---|---|---|---|---|
| 4 | Тема 4. Викрадення облікових даних | 2 | 2 | 10 | 14 | МН1, МН2, МН4, МН6 | МО2, МО4, МО9 | СК18 |
| 5 | Тема 5. Впровадження перехоплювачів | 2 | 2 | 10 | 14 | МН1, МН2, МН4, МН6 | МО2, МО4, МО9 | СК18 |
| **Змістовий модуль 2. Способи боротьби зі шкідливим програмним забезпеченням** | | | | | | | | |
| 6 | Тема 6. Інтернет-загрози та їх розповсюдження | 4 | 4 | 10 | 18 | МН1, МН2, МН4, МН6 | МО2, МО4, МО9 | СК18 |
| 7 | Тема 7. Рекламне ПЗ, клавіатурні логери та дозвонювачі | 2 | 2 | 10 | 14 | МН1, МН4, МН6 | МО2, МО4, МО9 | СК18 |
| 8 | Тема 8. Загрози для мобільних телефонів та ОС | 2 | 2 | 10 | 14 | МН1, МН2, МН4, МН6 | МО2, МО4, МО9 | СК18 |
| 9 | Тема 9. Статичний та динамічний аналіз шкідливих програм | 4 | 4 | 5 | 13 | МН1, МН2, МН4, МН6 | МО2, МО4, МО9 | СК18 |
| 10 | Тема 10. Способи боротьби з шкідливим ПЗ | 2 | 2 | 5 | 9 | МН1, МН2, МН4, МН6 | МО2, МО4, МО9 | СК18 |
| | **Разом** | **30** | **30** | **90** | **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); МН4 — робота з навчально-методичною літературою (конспектування, тезування, анотування, рецензування, складання реферату); МН6 — самостійна робота (розв'язання завдань).*

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

## 4. Результати навчання

**Знати:**

– Класифікацію та термінологію шкідливого програмного забезпечення.

– Прояви та ознаки зараження системи.

– Способи викрадення облікових даних і персональної інформації.

– Засоби та стратегії протидії ШПЗ.

**Вміти:**

– Виконувати статичний аналіз підозрілих файлів.

– Відстежувати процеси, реєстр і файлову систему.

– Аналізувати мережевий трафік.

– Видаляти ШПЗ і відновлювати працездатність системи.

**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 (60 %) + 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. Основні види шкідливого програмного забезпечення. Термінологічний базис**

1. Поняття шкідливого програмного забезпечення та його мета.
2. Базові терміни: пейлоад, вектор зараження, механізм закріплення, індикатори компрометації, сигнатура.
3. Класифікація ШПЗ за способом поширення: віруси, черв'яки, троянські програми.
4. Класифікація ШПЗ за функціями: бекдори, руткіти, вимагачі, шпигунське та рекламне ПЗ, боти, завантажувачі, криптомайнери.
5. Класифікація за середовищем існування: файлові, завантажувальні, макровіруси, скриптові, безфайлові.
6. Життєвий цикл шкідливої програми: від проникнення до поширення.
7. Комбіноване ШПЗ у сучасних атаках.

**Тема 2. Аналіз проявів та ознак шкідливого ПЗ**

1. Ознаки зараження на рівні продуктивності системи.
2. Мережеві ознаки: невідомі з'єднання, нетиповий трафік, періодичні запити до C2.
3. Зміни у файловій системі, реєстрі, службах та автозапуску.
4. Прояви в інтерфейсі користувача та облікових записах.

**Тема 3. Руткіти, бекдори та прихований запуск шкідливого ПЗ**

1. Поняття руткіта та принципи приховування присутності ШПЗ.
2. Рівні руткітів: користувацький, ядра, завантажувальний, мікропрограмний, гіпервізорний.
3. Бекдори: призначення, різновиди (RAT, веб-оболонки, апаратні, через ланцюг постачання).
4. Зв'язок бекдорів із сервером керування та маскування трафіку.
5. Механізми прихованого запуску та закріплення у Windows і Linux.
6. Методи виявлення руткітів: крос-перевірка, аналіз дампу пам'яті, перевірка цілісності завантаження.

**Тема 4. Викрадення облікових даних**

1. Облікові дані як головна ціль атак: паролі, хеші, токени, cookie, ключі.
2. Фішинг та перехоплення сесій (AitM) як способи викрадення.
3. Інфостілери: схема роботи та канали збуту викрадених даних.
4. Атаки на облікові дані в Windows: дамп LSASS, Pass-the-Hash, Pass-the-Ticket.
5. Атаки на сховища паролів та credential stuffing.

6. Ознаки компрометації облікових записів.
7. Захист облікових даних: MFA, стійке хешування, менеджери паролів.

**Тема 5. Впровадження перехоплювачів**

1. Поняття перехоплювача (hook): легітимне та шкідливе використання.
2. Перехоплення повідомлень ОС і функцій API.
3. Впровадження коду в процеси: DLL injection, process hollowing, APC injection.
4. Перехоплення в браузері: шкідливі розширення та атака man-in-the-browser.
5. Перехоплення на рівні ядра та мережі (MitM, ARP- і DNS-спуфінг).
6. Методи виявлення перехоплювачів.
7. Засоби захисту від впровадження перехоплювачів.

**Тема 6. Інтернет-загрози та їх розповсюдження**

1. Інтернет як основний канал доставки ШПЗ.
2. Поширення через електронну пошту та шкідливі вкладення.
3. Drive-by download, шкідлива реклама та піратське ПЗ.
4. Атаки на ланцюг постачання та репозиторії пакетів.
5. Інфраструктура атакувальників: C2, ботнети, моделі MaaS та RaaS.
6. Методи соціальної інженерії при поширенні ШПЗ.
7. Захист на рівні мережі, пошти та браузера.

**Тема 7. Рекламне ПЗ, клавіатурні логери та дозвонювачі**

1. Потенційно небажані програми (PUP/PUA) та їх монетизація.
2. Рекламне ПЗ і викрадачі браузера: функції та способи поширення.
3. Клавіатурні логери: програмні, драйверні, браузерні, апаратні.
4. Побічні канали відновлення введення та легітимні засоби моніторингу.
5. Дозвонювачі: історичні модемні та сучасні мобільні різновиди.
6. Методи протидії рекламному ПЗ, кейлогерам і дозвонювачам.

**Тема 8. Загрози для мобільних телефонів та ОС**

1. Смартфон як ціль атак: які дані під загрозою.
2. Банківські трояни та зловживання службами спеціальних можливостей.
3. Шпигунське ПЗ, у тому числі zero-click атаки.
4. Шкідливі застосунки, smishing, vishing та SIM-swap.
5. Порівняння моделей безпеки Android, iOS та настільних ОС.
6. Ризики root-доступу та jailbreak.
7. Заходи захисту мобільних пристроїв і корпоративне управління (MDM).

**Тема 9. Статичний та динамічний аналіз шкідливих програм**

1. Мета аналізу ШПЗ та отримання індикаторів компрометації.
2. Базовий статичний аналіз: хеші, рядки, формат файлу, імпорт, ентропія.
3. Поглиблений статичний аналіз: дизасемблювання та декомпіляція.
4. Динамічний аналіз у пісочниці: моніторинг процесів, файлів, реєстру, мережі.
5. Методи ухиляння ШПЗ від аналізу.
6. Порядок проведення аналізу та формування звіту.

**Тема 10. Способи боротьби з шкідливим ПЗ**

1. Методи виявлення в антивірусних засобах: сигнатурний, евристичний, поведінковий, хмарний.
2. Запобігання зараженню: оновлення, мінімальні привілеї, контроль запуску застосунків.
3. Засоби виявлення: EDR/XDR, SIEM, IDS/IPS, пошук загроз.
4. Реагування на інциденти за NIST SP 800-61.
5. Відновлення: резервне копіювання за правилом 3-2-1 та видалення ШПЗ.
6. Нормативна база кібербезпеки в Україні.

**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. Соціальна інженерія : конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 12 (F) Інформаційні технології денної та заоч. форм навч. / уклад. О. І. Міскевич. Луцьк : ЛНТУ, 2025. 76 с. URL: https://repository.lntu.edu.ua/handle/123456789/627

2. Теорія інформації та кодування : методичні вказівки до лабораторних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань F (12) Інформаційні технології спеціальності F6 (126) Інформаційні системи та технології денної та заоч. форм навч. / уклад. С. В. Гринюк, О. І. Міскевич. Луцьк : ЛНТУ, 2026. 74 с. URL: https://repository.lntu.edu.ua/handle/123456789/4409

3. Аналіз шкідливого програмного забезпечення : методичні вказівки до виконання самостійної роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Кібербезпека» галузі знань 12 Інформаційні технології спеціальності 125 «Кібербезпека» денної та заочної форм навчання / уклад. О. І. Міскевич. Луцьк : ЛНТУ, 2022. 24 с. URL: https://lib.lntu.edu.ua/uk/147258369/19546

### ІІ. Наукові праці

*Праці автора силабуса:*

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

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

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

### ІІІ. Інформаційні ресурси

7. Cisco Networking Academy : офіційний сайт. URL: https://www.netacad.com (дата звернення: 20.05.2026).

8. Prometheus : онлайн-платформа освітніх курсів. URL: https://courses.prometheus.org.ua/ (дата звернення: 20.05.2026).

9. Дія. Освіта : національна онлайн-платформа з цифрової освіти. URL: https://osvita.diia.gov.ua

(дата звернення: 20.05.2026).