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 «Технології OSINT»
ступінь вищої освіти – бакалавр
галузь знань – 12 Інформаційні технології
спеціальність – 125 Кібербезпека та захист інформації
освітня програма – Кібербезпека

Кафедра кібербезпеки

Силабус склав(ла) завідувач кафедри кібербезпеки, к.т.н., доцент Сергій КОСТЮЧКО

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/2335

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Технології OSINT»

Освітня програма	Кібербезпека
Галузь знань / Спеціальність	12 Інформаційні технології / 125 Кібербезпека та захист інформації
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 Сергій КОСТЮЧКО

1. Мета і завдання дисципліни

Мета: Формування у здобувачів вищої освіти теоретичних знань і практичних навичок пошуку, збирання, аналізу та перевірки інформації з відкритих джерел, використання сучасних технологій та інструментів OSINT, роботи з відкритими базами даних, а також узагальнення й візуалізації отриманих результатів для розв’язання практичних завдань у сфері інформаційної та кібербезпеки.

Завдання: Ознайомлення з основними видами відкритих інформаційних ресурсів, принципами їх використання та нормативно-правовими засадами роботи з відкритою інформацією.
Опанування методів і технологій пошуку, збирання, систематизації та перевірки достовірності інформації з відкритих джерел.
Набуття практичних навичок використання сучасних інструментів OSINT для пошуку та аналізу інформації.
Вивчення можливостей міжнародних відкритих баз даних та формування навичок їх використання для аналітичних досліджень.
Формування вмінь обробляти, узагальнювати та візуалізувати отримані дані, готувати аналітичні звіти й обґрунтовані висновки.

2. Компетентності

КФ01 — Здатність застосовувати законодавчу та нормативно правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

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. Теоретичні та методологічні основи пошуку й аналізу відкритих інформаційних ресурсів								
1	Тема 1. Відкриті інформаційні ресурси та їх класифікація	2/0,5	2/0,5	6/16	10/17	МН1, МН2, МН3, МН4, МН5	МО2, МО4, МО9	КФ01

№	Назва теми	**Лекції** денна/ заочна	**Практ./ Семін./ лаб** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**СК**
2	Тема 2. Інформаційно-пошукові стратегії та технології в цифрових комунікаційних середовищах	4/0,5	4/0,5	12/16	20/17	МН1, МН2, МН3, МН4, МН5	МО2, МО4, МО9	КФ01
3	Тема 3. Нормативно-правові та етичні засади використання відкритих джерел інформації	4/0,5	4/0,5	12/16	20/17	МН1, МН2, МН3, МН4, МН5	МО2, МО4, МО9	КФ01
4	Тема 4. Методологія аналізу інформаційних масивів та верифікація даних	4/0,5	4/0,5	12/18	20/19	МН1, МН2, МН3, МН4, МН5	МО2, МО4, МО9	КФ01
Змістовий модуль 2. Технології OSINT, міжнародні інформаційні ресурси та аналітична візуалізація								
5	Тема 5. Методи та інструменти розвідки з відкритих джерел інформації (OSINT)	4/1	4/1	12/18	20/20	МН1, МН2, МН3, МН4, МН5	МО2, МО4, МО9	КФ01
6	Тема 6. Глобальні підходи та міжнародний досвід аналізу відкритих інформаційних ресурсів	4/1	4/1	12/18	20/20	МН1, МН2, МН3, МН4, МН5	МО2, МО4, МО9	КФ01
7	Тема 7. Відкриті міжнародні бази даних та їх аналітичний потенціал	4/1	4/1	12/18	20/20	МН1, МН2, МН3, МН4, МН5	МО2, МО4, МО9	КФ01
8	Тема 8. Методологія узагальнення даних та візуалізація аналітичних результатів	4/1	4/1	12/18	20/20	МН1, МН2, МН3, МН4, МН5	МО2, МО4, МО9	КФ01
	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); 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).

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

4. Результати навчання

Знати:

– Основні принципи, методи та технології розвідки на основі відкритих джерел інформації (OSINT).

– Інструменти та засоби пошуку, збору, аналізу й верифікації інформації з відкритих джерел.

Вміти:

– Застосовувати OSINT-інструменти для пошуку, збору та систематизації інформації з відкритих джерел.

– Аналізувати, перевіряти достовірність отриманих даних та використовувати результати OSINT для виявлення потенційних кіберзагроз.

5. Цілі сталого розвитку

ЦСР 4 – Якісна освіта

ЦСР 8 – Гідна праця та економічне зростання

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. Відкриті інформаційні ресурси та їх класифікація

Поняття та сутність відкритих інформаційних ресурсів. Основні характеристики відкритої інформації. Класифікація відкритих джерел інформації. Державні, наукові, освітні, комерційні та громадські інформаційні ресурси. Структуровані, напівструктуровані та неструктуровані дані. Поняття відкритих даних (Open Data). Інформаційні портали, електронні реєстри та цифрові бібліотеки. Інформаційні ресурси соціальних мереж. Переваги та обмеження використання відкритих джерел. Критерії оцінювання достовірності, актуальності та повноти інформаційних ресурсів.

Тема 2. Інформаційно-пошукові стратегії та технології в цифрових комунікаційних середовищах

Поняття та принципи інформаційного пошуку. Основні види інформаційно-пошукових систем. Методи формування пошукових запитів. Використання логічних операторів та операторів розширеного пошуку. Пошукові стратегії в глобальній мережі Інтернет. Методи пошуку інформації в соціальних мережах, електронних бібліотеках і базах даних. Пошук за ключовими словами, метаданими та контекстом. Використання спеціалізованих пошукових систем. Автоматизація процесів інформаційного пошуку. Оцінювання релевантності та повноти результатів пошуку.

Тема 3. Нормативно-правові та етичні засади використання відкритих джерел інформації

Правові основи доступу до публічної інформації. Законодавство України у сфері інформації та відкритих даних. Основні положення законів України «Про інформацію», «Про доступ до публічної інформації» та «Про захист персональних даних». Правові аспекти збирання, зберігання та оброблення інформації з відкритих джерел. Захист персональних даних і приватності. Авторське право та ліцензування відкритих даних. Ліцензії Creative Commons.

Етичні принципи використання відкритої інформації. Обмеження щодо автоматизованого збирання даних. Принципи відповідального використання результатів інформаційного аналізу.

Тема 4. Методологія аналізу інформаційних масивів та верифікація даних

Основні етапи аналізу інформації з відкритих джерел. Методи збирання, систематизації та оброблення інформаційних масивів. Попереднє очищення та нормалізація даних. Структурування інформаційних наборів. Методи статистичного та порівняльного аналізу. Виявлення закономірностей і взаємозв'язків у даних. Поняття верифікації та фактчекінгу. Методи перевірки достовірності інформації. Перехресна перевірка даних за незалежними джерелами. Аналіз метаданих документів і зображень. Виявлення інформаційних маніпуляцій та дезінформації. Оцінювання надійності джерел і формування аналітичних висновків.

Тема 5. Методи та інструменти розвідки з відкритих джерел інформації (OSINT)

Поняття та основні принципи Open Source Intelligence (OSINT). Основні етапи OSINT-дослідження. Планування інформаційного пошуку. Методи збирання інформації з вебресурсів і соціальних мереж. Пошук інформації про домени, IP-адреси та мережеву інфраструктуру. Використання сервісів WHOIS, DNS Lookup та Shodan. Аналіз відкритих профілів і цифрових слідів. Використання OSINT Framework, Maltego та SpiderFoot. Основи геолокаційного аналізу інформації (GEOINT). Перевірка зображень і відеоматеріалів. Автоматизація збирання відкритих даних. Документування результатів OSINT-досліджень. Правові та етичні обмеження OSINT.

Тема 6. Глобальні підходи та міжнародний досвід аналізу відкритих інформаційних ресурсів

Міжнародні практики використання відкритої інформації. Роль OSINT у забезпеченні кібербезпеки та інформаційно-аналітичній діяльності. Використання відкритих джерел у державному управлінні, наукових дослідженнях та бізнес-аналітиці. Діяльність міжнародних організацій у сфері відкритих даних. Основні принципи Open Government Data. Міжнародні ініціативи Open Government Partnership та Open Data Charter. Європейські підходи до відкритих даних. Використання відкритої інформації для виявлення кіберзагроз. Міжнародні практики фактчекінгу та протидії дезінформації. Особливості використання OSINT у міжнародних аналітичних дослідженнях.

Тема 7. Відкриті міжнародні бази даних та їх аналітичний потенціал

Поняття та класифікація міжнародних баз даних. Основні джерела відкритих статистичних і соціально-економічних даних. Використання World Bank Open Data, UNdata, Eurostat та OECD Data. Європейський портал відкритих даних data.europa.eu. Міжнародні наукові інформаційні ресурси OpenAlex, Crossref та Google Scholar. Бази даних кібербезпеки CVE, NVD та MITRE ATT&CK. Пошук і завантаження відкритих наборів даних. Використання API для отримання інформації. Формати CSV, JSON та XML. Порівняння показників із різних джерел. Оцінювання повноти, актуальності та якості міжнародних даних. Практичне застосування відкритих баз даних для аналітичних досліджень.

Тема 8. Методологія узагальнення даних та візуалізація аналітичних результатів

Основні принципи узагальнення результатів інформаційного аналізу. Методи групування, агрегування та систематизації даних. Формування аналітичних показників. Статистичне опрацювання результатів досліджень. Принципи візуального подання інформації. Основні види діаграм і графіків. Побудова таблиць, часових рядів і порівняльних графіків. Геопросторова візуалізація даних. Використання Microsoft Excel, Power BI, Tableau та Python для візуалізації інформації. Створення інтерактивних інформаційних панелей (Dashboard). Основи побудови графів взаємозв'язків. Виявлення тенденцій та аномалій у даних. Підготовка аналітичних звітів. Формулювання висновків і рекомендацій на основі отриманих результатів.

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. IoT-технології для кіберфізичних систем : конспект лекцій для здобувачів другого (магістерського) рівня вищої освіти освітньої програми «Комп'ютерна інженерія» галузь знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія денної та заоч. форм навч. / уклад. С. В. Гринюк. Луцьк : ЛНТУ, 2026. 48 с. URL: https://repository.lntu.edu.ua/handle/123456789/4406.

2. Програмування на Python : метод. вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 12 (F) Інформаційні технології денної та заоч. форм навч. / уклад.: С. М. Костючко, Л. М. Конкевич. Луцьк : ЛНТУ, 2026. 60 с. URL: https://repository.lntu.edu.ua/handle/123456789/3352.

ІІ. Наукові праці

Праці автора силабуса:

3. Tkachuk A., Polishchuk M., Polishchuk L., Kostiuchko S., Hryniuk S., Konkevych L. Investigation of DC-AC converter with microcontroller control of inverter frequency. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. 2025. Vol. 15, No. 1. P. 55–61. URL: https://repository.lntu.edu.ua/handle/123456789/2012.

4. Bahniuk N., Terletskyi T., Kaidyk O., Kostiuchko S., Kondius I. Solving operational tasks in the design of video surveillance systems. CEUR Workshop Proceedings : Applied Information Technologies and Artificial Intelligence Systems. 2025. P. 332–342. URL: https://ceur-ws.org/Vol-4160/paper20.pdf.

5. 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.

6. Римчук І., Костючко С., Поліщук М., Гринюк С., Конкевич Л. Безпека комунікаційних процесів з використанням візуальної криптографії. Кібербезпека: освіта, наука, техніка. 2024. № 2(26). С. 258–267. URL: https://repository.lntu.edu.ua/handle/123456789/4595.

7. Каган І., Костючко С. CRM-системи як інструмент підвищення ефективності бізнесу. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2023. № 52. С. 5–9. DOI: https://doi.org/10.36910/6775-2524-0560-2023-52-01.

8. Polishchuk M., Grinyuk S., Kostiuchko S., Tkachuk A., Savaryn P. Tesla Switch of 4 Batteries Based on the Arduino Uno Board. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. 2023. Vol. 13, No. 3. P. 111–116. DOI: https://doi.org/10.35784/iapgos.4051.

9. Kostiuchko S., Polishchuk M., Zabolotnyi O., Tkachuk A., Twarog B. The Auxiliary Parametric Sensitivity Method as a Means of Improving Project Management Analysis and Synthesis of Executive Elements. Emerging Technologies in Computing / eds. M. H. Miraz, G. Southall, M. Ali, A. Ware, S. Soomro. Cham : Springer, 2021. (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering ; vol. 395). P. 92–103. DOI: https://doi.org/10.1007/978-3-030-90019-9_8.

10. Kostiuchko S., Kyryliuk L., Chernyashchuk N., Bortnyk K., Hrunjuk S. Wireless access point with multilayer data protection algorithm. Computer-integrated technologies: education, science, production. 2021. No. 42. P. 147–151. DOI: https://doi.org/10.36910/6775-2524-0560-2021-42-21.

11. Костючко С. М., Багнюк Н. В., Кузьмич О. І., Поліщук М. М., Кирилюк Л. М. Біометрична ідентифікація засобами Python та Raspberry Pi. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2021. Вип. 42. С. 142–146. DOI: https://doi.org/10.36910/6775-2524-0560-2021-42-20.

Праці інших авторів:

12. Meredith D. The OSINT Handbook : A Practical Guide to Gathering and Analyzing Online Information. Birmingham : Packt Publishing, 2024. 204 p. URL: https://www.packtpub.com/en-nl/product/the-osint-handbook-9781837638277.

13. Ghioni R., Taddeo M., Floridi L. Open source intelligence and AI: A systematic review of the GELSI literature. AI & Society. 2024. Vol. 39. P. 1827–1842. DOI: https://doi.org/10.1007/s00146-023-01628-x.

14. Watters P. A. Counterintelligence in a Cyber World. Cham : Springer, 2023. 145 p. DOI: https://doi.org/10.1007/978-3-031-35287-4.

15. Kühn P. Proactive Cyber Threat Intelligence : Automating the Intelligence Cycle Based on Open Sources. Wiesbaden : Springer Vieweg, 2025. 255 p. DOI: https://doi.org/10.1007/978-3-658-49241-0.

16. Kolokolov A., Zelensky M. Data Visualization with Microsoft Power BI. Sebastopol : O’Reilly Media, 2024. 416 p. URL: https://www.oreilly.com/library/view/data-visualization-with/9781098152772/.