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 «Аналітика великих даних у кіберпросторі»
ступінь вищої освіти – бакалавр
галузь знань – 12 Інформаційні технології
спеціальність – 121 Інженерія програмного забезпечення
освітня програма – Інженерія програмного забезпечення

Кафедра комп'ютерних наук

Силабус склав(ла) завідувач кафедри комп'ютерних наук, к.т.н., доцент Валерій ЛІЩИНА

Силабус затверджений на засіданні кафедри комп'ютерних наук, протокол № 1/1 від «29» серпня 2026 р.

Завідувач кафедри к.т.н., доцент Валерій ЛІЩИНА

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

Гарант ОП «Інженерія програмного забезпечення» к.т.н., доцент Наталія ЛІЩИНА

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

Затверджений силабус онлайн:
https://e.lntu.edu.ua/syllabus/2085

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Аналітика великих даних у кіберпросторі»

Освітня програма	Інженерія програмного забезпечення
Галузь знань / Спеціальність	12 Інформаційні технології / 121 Інженерія програмного забезпечення
Рівень вищої освіти	перший (бакалаврський)
Статус дисципліни	вибіркова
Мова викладання	українська
Обсяг	5 кредитів ECTS / 150 годин, семестр 6
Форма контролю	залік
Викладач(і)	к.т.н., доцент Валерій ЛІЩИНА електронна пошта: v.lishchyna@lntu.edu.ua

1. Мета і завдання дисципліни

Мета: Формування знань і практичних навичок збирання, опрацювання, аналізу та візуалізації великих даних цифрового середовища для виявлення закономірностей, аномалій і підтримки прийняття рішень.

Завдання: Ознайомлення з характеристиками великих даних та принципами їх зберігання; опанування методів підготовки й аналізу мережевих, текстових і подієвих даних; застосування розподіленого опрацювання та машинного навчання; формування навичок оцінювання результатів, захисту персональних даних і відповідального використання інформації.

Пререквізити: Знання основ програмування, баз даних, комп’ютерних мереж, теорії ймовірностей і математичної статистики. Базові навички роботи з Python та SQL.

2. Компетентності

СК07 — Володіння знаннями про інформаційні моделі даних, здатність створювати програмне забезпечення для зберігання, видобування та опрацювання даних.

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

№	Назва теми	Лекції	Лаб.	Самост. робота	Разом	Методи навчання	Методи оцінювання	СК
1	Тема 1. Великі дані в кіберпросторі	4	4	12	20	МН1, МН2, МН3, МН4, МН5, МН6	МО2, МО4, МО9, захист лабораторної роботи	СК07
2	Тема 2. Збирання та підготовка даних	4	4	12	20	МН1, МН2, МН3, МН4, МН5, МН6	МО2, МО4, МО9, захист лабораторної роботи	СК07
3	Тема 3. Зберігання й розподілене опрацювання	4	4	11	19	МН1, МН2, МН3, МН4, МН5, МН6	МО2, МО4, МО9, захист лабораторної роботи	СК07

№	Назва теми	Лекції	Лаб.	Самост. робота	Разом	Методи навчання	Методи оцінювання	СК
4	Тема 4. Дослідницький аналіз і візуалізація	4	4	11	19	МН1, МН2, МН3, МН4, МН5, МН6	МО2, МО4, МО9, захист лабораторної роботи	СК07
5	Тема 5. Машинне навчання для цифрових даних	4	4	11	19	МН1, МН2, МН3, МН4, МН5, МН6	МО2, МО4, МО9, захист лабораторної роботи	СК07
6	Тема 6. Аналіз журналів і виявлення аномалій	4	4	11	19	МН1, МН2, МН3, МН4, МН5, МН6	МО2, МО4, МО9, захист лабораторної роботи	СК07
7	Тема 7. Текстова та графова аналітика	3	3	11	17	МН1, МН2, МН3, МН4, МН5, МН6	МО2, МО4, МО9, захист лабораторної роботи	СК07
8	Тема 8. Приватність і відтворюваність аналітики	3	3	11	17	МН1, МН2, МН3, МН4, МН5, МН6	МО2, МО4, МО9, захист лабораторної роботи	СК07
	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); 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; МО4 — тестування; МО9 — залік.

4. Результати навчання

Знати:

– Принципи збирання, зберігання, опрацювання й аналізу великих даних у кіберпросторі, методи виявлення аномалій та захисту приватності.

Вміти:

– Готувати й аналізувати дані засобами Python, SQL та Apache Spark, застосовувати машинне навчання, візуалізувати й обґрунтовувати результати.

5. Цілі сталого розвитку

ЦСР 4 – Якісна освіта

ЦСР 9 – Промисловість, інновації та інфраструктура

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. Великі дані в кіберпросторі

Характеристики Big Data; цифрові сліди, журнали подій, мережеві й текстові дані; задачі аналітики.

Тема 2. Збирання та підготовка даних

даних Відкриті набори, API, формати CSV, JSON і Parquet; пропуски, дублікати, нормалізація.

Тема 3. Зберігання й розподілене опрацювання

Реляційні та NoSQL-сховища; принципи розподілених обчислень; базові операції Apache Spark.

Тема 4. Дослідницький аналіз і візуалізація

Статистичні характеристики, часові тенденції, кореляції, інформаційні панелі.

Тема 5. Машинне навчання для цифрових даних

Класифікація, кластеризація, підготовка ознак, поділ вибірки та оцінювання моделей.

Тема 6. Аналіз журналів і виявлення аномалій

Агрегація подій, часові вікна, нетипова активність, хибні спрацювання.

Тема 7. Текстова та графова аналітика

Опрацювання текстів, TF-IDF, тематична кластеризація; графи взаємодій і базові метрики.

Тема 8. Приватність і відтворюваність аналітики

Знеособлення, упередження даних, обмеження висновків, документування та представлення проєкту.

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

I. Навчально-методичні матеріали та розробки

Праці інших авторів:

1. Олещенко Л. М. Машинне навчання: комп'ютерний практикум: навчальний посібник. Київ: КПІ ім. Ігоря Сікорського, 2022. 92 с. URL: https://ela.kpi.ua/handle/123456789/48731.

2. Шелестов А. Ю., Куссуль Н. М., Яйлимова Г. О. Методи аналізу великих гетерогенних даних. Лабораторний практикум: навчальний посібник. Київ: КПІ ім. Ігоря Сікорського, 2022. 57 с. URL: https://ela.kpi.ua/bitstreams/2f3269fe-807c-41f1-a65c-ac92b133bae0/download.

3. Рогоза В. С., Письменний І. О., Іщенко Г. В., Яременко В. С. Обробка надвеликих масивів даних. Навчальний посібник до виконання курсових робіт. Київ: КПІ ім. Ігоря Сікорського, 2024. 207 с. URL: https://ela.kpi.ua/handle/123456789/80255.

4. Олещенко Л. М. Великі дані та аналітика: підручник. Київ: ПТФ Просвіта, 2026. 350 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/808c9159-8349-4a48-9422-0d4b355270d8/content.

II. Наукові праці

Праці автора силабуса:

5. Shnain S. K., Najm M. A. M., Taher N. A., Abdalrazzaq A. S., Rashit B., Lishchyna V. Classification of Landsat 8 Images Using Convolutional Neural Network Based on Minimum Noise Fraction Transform. Proceedings of the 35th Conference of FRUCT Association. 2024. P. 692–698. URL: https://www.fruct.org/files/publications/volume-35/fruct35/Shn2.pdf.

6. Kozubtsova L., Ali R. H. M., Kozubtsov I., Lishchyna V., Yashchuk A., Hassan N. B., Lukashenka V. Approach To Risk Management Based On The Assessment Of The Cost Of Quality Of Implementation Of Cybersecurity Measures Of The Organization. Proceedings of the 35th Conference of FRUCT Association. 2024. P. 399–406. URL: https://fruct.org/publications/volume-35/fruct35/files/Koz2.pdf.

7. Barabash O., Laptiev O., Sobchuk V., Salanda I., Melnychuk Y., Lishchyna V. Comprehensive Methods of Evaluation of Distance Learning System Functioning. International Journal of Computer Network and Information Security. 2021. Vol. 13, No. 3. P. 62–71. DOI: https://doi.org/10.5815/ijcnis.2021.03.06.

Праці інших авторів:

8. Sanjalawe Y., Fraihat S., Al-E'mari S., Makhadmeh S. N. A review of artificial intelligence-based intrusion detection in industrial internet of things. Discover Internet of Things. 2026. Vol. 6. Article 44. DOI: https://doi.org/10.1007/s43926-026-00285-y.

9. Kikissagbe B. R., Adda M. Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review. Electronics. 2024. Vol. 13, No. 18. Article 3601. DOI: https://doi.org/10.3390/electronics13183601.

10. Neto E. C. P., Dadkhah S., Ferreira R., Zohourian A., Lu R., Ghorbani A. A. CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment. Sensors. 2023. Vol. 23, No. 13. Article 5941. DOI: https://doi.org/10.3390/s23135941.

11. Tian S., Zhang T., Liu J. et al. Exploring the Role of Large Language Models in Cybersecurity: A Systematic Survey. Препринт. arXiv:2504.15622. 2025. DOI: https://doi.org/10.48550/arXiv.2504.15622.

III. Інформаційні ресурси

12. MITRE. ATT&CK: база знань про тактики й техніки кіберзагроз та підходи до їх виявлення.

URL: https://attack.mitre.org/.

13. Canadian Institute for Cybersecurity, University of New Brunswick. CICIoT2023: набір мережевих даних для дослідження, класифікації та виявлення атак в IoT-середовищах. URL: https://www.unb.ca/cic/datasets/iotdataset-2023.html.

14. Zeek Project. Zeek Documentation: документація засобу аналізу мережевого трафіку та формування журналів подій. URL: https://docs.zeek.org/en/current/.

15. Open Information Security Foundation. Suricata User Guide: документація системи виявлення мережевих загроз та аналізу подій безпеки. URL: https://docs.suricata.io/.