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 великих даних»
ступінь вищої освіти – бакалавр
галузь знань – 12 Інформаційні технології
спеціальність – 125 Кібербезпека та захист інформації
освітня програма – Кібербезпека

Кафедра кібербезпеки

Силабус склав(ла) доцент кафедри кібербезпеки, к.т.н. Наталія СУРОВА

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/1806

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Аналіз великих даних»

Освітня програма	Кібербезпека
Галузь знань / Спеціальність	12 Інформаційні технології / 125 Кібербезпека та захист інформації
Рівень вищої освіти	перший (бакалаврський)
Статус дисципліни	нормативна
Мова викладання	українська
Обсяг	5 кредитів ECTS / 150 годин, семестр 5
Форма контролю	екзамен
Викладач(і)	к.т.н. Наталія СУРОВА

1. Мета і завдання дисципліни

Мета: забезпечити формування у фахівців комплексу професійних знань щодо пошуку раціональних рішень в багатовимірному просторі альтернатив, зведення різнорідних джерел даних до придатного для аналізу вигляду, побудови й обґрунтовування ознак виявлення загроз, оцінювання якості отриманих результатів кількісно та чіткого окреслення меж доказовості аналітичних висновків.

Завдання: освоєння принципів обробки великих обсягів різнорідних даних у задачах кібербезпеки; засвоєння основних понять теорії аналізу даних і моделей виявлення відхилень; визначення статичних та динамічних характеристик об'єктів спостереження за журналами подій і графами зв'язків; побудова ознак виявлення загроз та злиття незалежних джерел даних; кількісне оцінювання точності й повноти виявлення та вибір порога з урахуванням критерію вартості помилок; запобігання хибним висновкам через перевірку альтернативних пояснень; ознайомлення з методологічними основами відтворюваного дослідження та визначення меж отриманих висновків.

Пререквізити: Прикладна математика

2. Компетентності

ЗК05 — Здатність до пошуку, оброблення та аналізу інформації.

СК02 — Здатність до використання інформаційно комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

СК11 — Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

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. Застосування аналізу великих даних у різних аспектах кібербезпеки								
1	Тема 1. Аналіз великих даних у кібербезпеці	2/0,5	2/0,5	6/9	10/10	МН1, МН2, МН6	МО1, МО2, МО4	ЗК05, СК02, СК11

№	Назва теми	Лекції денна/ заочна	Лаб. денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
2	Тема 2. Мережева криміналістика та застосування аналізу великих даних	2/0,5	2/0,5	6/9	10/10	МН1, МН2, МН6	МО1, МО2, МО4	ЗК05, СК02, СК11
3	Тема 3. Динамічне оцінювання вразливостей та їх експлуатації на основі аналізу даних	2/0,5	2/0,5	6/9	10/10	МН1, МН2, МН6	МО1, МО2, МО4	ЗК05, СК02, СК11
4	Тема 4. Аналіз кореневих причин у кібербезпеці	2/0,5	2/0,5	6/10	10/11	МН1, МН2, МН6	МО1, МО2, МО4	ЗК05, СК11, СК02
5	Тема 5. Візуалізація даних для кібербезпеки	2/0,5	2/0,5	6/10	10/11	МН1, МН2, МН6	МО1, МО2, МО4	ЗК05, СК02, СК11
6	Тема 6. Навчання з кібербезпеки: проєктування та оцінювання	2/0,25	2/0,25	6/10	10/10,5	МН1, МН2, МН6	МО1, МО2, МО4	ЗК05, СК11, СК02
7	Тема 7. Машинне рознавчання: відновлення моделей у змагальному середовищі	2/0,25	2/0,25	6/10	10/10,5	МН1, МН2, МН6	МО1, МО2, МО4	ЗК05, СК02, СК11
Змістовий модуль 2. Застосування аналізу великих даних у нових галузях кібербезпеки. Інструменти та джерела даних у сфері кібербезпеки.								
8	Тема 8. Аналіз великих даних для безпеки мобільних застосунків	2/0,5	2/0,5	6/9	10/10	МН1, МН2, МН6	МО1, МО2, МО4	ЗК05, СК02, СК11
9	Тема 9. Безпека, приватність і довіра в хмарних обчисленнях	4/0,5	4/0,5	12/14	20/15	МН1, МН2, МН6	МО1, МО2, МО4	ЗК05, СК02, СК11
10	Тема 10. Кібербезпека інтернету речей	2/0,5	2/0,5	6/9	10/10	МН1, МН2, МН6	МО1, МО2, МО4	ЗК05, СК02, СК11
11	Тема 11. Аналіз великих даних для безпеки туманних обчислень	2/0,5	2/0,5	6/9	10/10	МН1, МН2, МН6	МО1, МО2, МО4	ЗК05, СК02, СК11

№	Назва теми	**Лекції** денна/ заочна	**Лаб.** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**ЗК та СК**
12	Тема 12. Аналіз девіантної соціотехнічної поведінки	2/0,5	2/0,5	6/10	10/11	МН1, МН2, МН6	МО1, МО2, МО4	ЗК05, СК02, СК11
13	Тема 13. Засоби кібербезпеки та їх добір	2/0,25	2/0,25	6/10	10/10,5	МН1, МН2, МН6	МО1, МО2, МО4	ЗК05, СК02, СК11
14	Тема 14. Дані та дослідницькі ініціативи для аналізу кібербезпеки	2/0,25	2/0,25	6/10	10/10,5	МН1, МН2, МН6	МО1, МО2, МО4	ЗК05, СК02, СК11
	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); МН6 — самостійна робота (розв'язання завдань).

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

4. Результати навчання

ПРН02. організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

ПРН03. використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

ПРН06. критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

ПРН10. виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;

ПРН23. реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах;

ПРН27. вирішувати задачі захисту потоків даних в інформаційних, інформаційнотелекомунікаційних (автоматизованих) системах;

5. Цілі сталого розвитку

ЦСР 4 – Якісна освіта

ЦСР 8 – Гідна праця та економічне зростання

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 (40 %) + 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. Аналіз великих даних у кібербезпеці

Вступ до аналізу великих даних: означення, характеристики, відмінності від традиційної аналітики, екосистема технологій. Потреба в аналізі великих даних у кібербезпеці: обмеження традиційних механізмів, еволюція загроз, нові можливості. Застосування: категорії рішень, архітектура, сценарії використання (зберігання даних, збагачення контекстом, виявлення аномалій). Виклики та обмеження підходу.

Тема 2. Мережева криміналістика та застосування аналізу великих даних

Вступ до мережевої криміналістики: предмет, задачі, відмінності від криміналістики носіїв інформації. Терміни та процес: базовий понятійний апарат і чотири фази розслідування. Сучасна практика: джерела даних, найпоширеніші інструменти та обмеження традиційних технологій. Застосування аналізу великих даних: програмні засоби, проєктні рішення, наявні платформи. Практична реалізація: архітектура платформи, компоненти сервісів, ключові можливості.

Тема 3. Динамічне оцінювання вразливостей та їх експлуатації на основі аналізу даних

Вступ: потреба, виклики та підхід до розв'язання задачі. Оцінювання вразливостей, атрибуція та експлуатація: атрибути вразливості, система CVSS та її обмеження, приклад практичного розслідування. Сучасні інструменти, джерела даних та методи їх опрацювання. Безпечне керування кіберподіями: порівняння систем SIEM, часовий і причинний аналіз. Напрями подальшого розвитку.

Тема 4. Аналіз кореневих причин у кібербезпеці

Проблема передчасної атрибуції кіберінцидентів та чинники тиску на аналітиків безпеки. Аналіз кореневих причин та атрибуція атак. Причинний аналіз загроз безпеки: виклики виявлення, відбір ознак, кластеризація на графах, багатокритеріальне рішення. Практичні дослідження: атрибуція через багатокритеріальне рішення та аналіз журналів великого масштабу.

Тема 5. Візуалізація даних для кібербезпеки

Візуалізація: як працює зорове сприйняття, канали кодування. Виявлення, аналіз і пом'якшення загроз: подання для роботи з алертами. Керування вразливостями: подання для інвентаризації та пріоритезації. Криміналістика: часові шкали, графи зв'язків, послідовності подій. Мережевий трафік: подання для великих обсягів однорідних записів. Нові напрями: поєднання сприйняття з аналітикою, боротьба з невдалими конструкціями.

Тема 6. Навчання з кібербезпеки: проєктування та оцінювання

Особливості навчання з кібербезпеки: специфіка та виклики професійної підготовки в сучасних умовах. Загальні принципи навчання: основні положення, що визначають результат. Практичне проєктування: від внутрішнього подання для автоматизованого оцінювання до пілотної перевірки.

Тема 7. Машинне рознавчання: відновлення моделей у змагальному середовищі

Потреба систем забувати, родовід даних, поняття рознавчання. Передумови та модель зловмисника: атаки виведення та атаки отруєння. Цілі та робочий процес рознавчання: повнота і своєчасність. Підхід: проміжний рівень сумувань, неадаптивне та адаптивне SQ-навчання. Суміжні напрями: змагальне навчання, захист приватності, інкрементне навчання.

Тема 8. Аналіз великих даних для безпеки мобільних застосунків

Безпека мобільних застосунків: постановка задачі та масштаб. Машинне навчання як засіб сортування черги. Типові ознаки та алгоритми. Проблеми оцінювання. Рекомендації і проблеми,

які вони усувають.

Тема 9. Безпека, приватність і довіра в хмарних обчисленнях

Хмарні обчислення: моделі розгортання та обслуговування, відмітні властивості, ключові технології. Загрози безпеці, приватності та довірі: атаки на багатокористувацькі середовища та системи віртуалізації, захист даних за умов взаємної недовіри учасників. Засоби захисту: журналювання, керування доступом, криптографічні рішення, ізоляція, протидія співрозміщенню, побудова довіри. Напрями розвитку.

Тема 10. Кібербезпека інтернету речей

Інтернет речей як предмет кібербезпеки: масштаб, склад, відмінності від звичайної мережі. Взаємодія інтернету речей та великих даних: домінування фактора різнорідності над обсягом. Вимоги до безпеки та наявні проблеми. Аналіз великих даних для безпеки інтернету речей: від одного набору до злиття джерел.

Тема 11. Аналіз великих даних для безпеки туманних обчислень

Основи туманних обчислень: означення, властивості, архітектури, наявні реалізації. Коли великі дані зустрічаються з туманними обчисленнями: межа передавання даних. Аналітика для безпеки туманного рівня: п'ять напрямів.

Тема 12. Аналіз девіантної соціотехнічної поведінки

Девіантна соціотехнічна поведінка. Основні поняття. Огляд підходів: аналіз соціальних мереж і кіберкриміналістика окремо та разом. Методика дослідження: від збору даних до перевірки ознак координації. Межі висновку, помилкова атрибуція та етичні обмеження.

Тема 13. Засоби кібербезпеки та їх добір

Добір засобів як окрема інженерна задача. Засоби межі мережі: екрани, антивірусні засоби, фільтрування вмісту. Засоби моніторингу мережі. Засоби захисту та криміналістики пам'яті. Керування паролями та автентифікацією. Методика добору: матриця покриття, надлишковість, бюджет.

Тема 14. Дані та дослідницькі ініціативи для аналізу кібербезпеки

Джерела даних для аналізу кібербезпеки. Еталонні набори даних: склад, придатність, обмеження. Сховища даних і майданчики збору. Чому вік набору визначає придатність результату. Напрями розвитку обміну даними. Паспорт набору даних.

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 інших авторів:

1. Géron A. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow : Concepts, Tools, and Techniques to Build Intelligent Systems. 3rd ed. Sebastopol : O'Reilly Media, 2022. 850p.

2. Maleh Y., Alazab M., Tawalbeh L. (Eds.). Big Data Analytics and Intelligent Systems for Cyber Threat Intelligence. Gistrup : River Publishers, 2023. 312p.

3. McKinney W. Python for Data Analysis : Data Wrangling with pandas, NumPy, and Jupyter. 3rd ed. Sebastopol : O'Reilly Media, 2022. URL: https://wesmckinney.com/book/ (Last accessed: 20.05.2026).

4. Molnar C. Interpretable Machine Learning : A Guide for Making Black Box Models Explainable. 2nd ed. 2022. URL: https://christophm.github.io/interpretable-ml-book/ (Last accessed: 20.05.2026).

5. Reis J., Housley M. Fundamentals of Data Engineering : Plan and Build Robust Data Systems. Sebastopol : O'Reilly Media, 2022. 445p.

ІІ. Наукові праці

Праці автора силабуса:

6. Сурова Н. М. Методичні аспекти викладання вищої математики студентам технічних спеціальностей у закладах вищої освіти. Наукові записки. Серія: Педагогічні науки. 2026. Вип. 222. С.528-531. URL: https://repository.lntu.edu.ua/handle/123456789/5361

7. Сурова Н. М. Основні аспекти прогнозування захворювання та їх реалізація в медичних системах. Наука і техніка сьогодні. Серія: Техніка. 2025. № 4(45) 2025. С.1634-1641. URL: https://repository.lntu.edu.ua/handle/123456789/5362

8. Сурова Н. М. Методологічні аспекти прогнозування креативності та інноваційності технічного мислення в контексті наукового пізнання. Наука і техніка сьогодні. Серія: Техніка. 2024. № 12(40) 2024. С.1489-1496. URL: https://repository.lntu.edu.ua/handle/123456789/5364