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 «Основи інформаційної безпеки держави»
ступінь вищої освіти – бакалавр
галузь знань – 12 Інформаційні технології
спеціальність – 125 Кібербезпека
освітня програма – Кібербезпека

Кафедра комп'ютерних наук

Силабус склав(ла) професор кафедри комп'ютерних наук, д.п.н., старший науковий співробітник Ігор КОЗУБЦОВ

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 «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/2894

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Основи інформаційної безпеки держави»

Освітня програма	Кібербезпека
Галузь знань / Спеціальність	12 Інформаційні технології / 125 Кібербезпека
Рівень вищої освіти	перший (бакалаврський)
Статус дисципліни	вибіркова
Мова викладання	українська
Обсяг	5 кредитів ECTS / 150 годин, семестр 7
Форма контролю	залік
Викладач(і)	д.п.н., старший науковий співробітник Ігор КОЗУБЦОВ електронна пошта: i.kozubtsov@lntu.edu.ua

1. Мета і завдання дисципліни

Мета: Метою дисципліни «Основи інформаційної безпеки держави» є розкриття змісту роботи майбутнього фахівця з комп’ютерної безпеки; формування цілісного представлення про суть надання послуг у сфері захисту інформатизації в цілому; актуальність проектування комп’ютерних мереж із сучасними засобами безпеки; моніторинг та аудит інформаційно-комунікаційних систем.

Завдання: Завданням дисципліни є набуття студентами знань про теоретичні основи інформаційної безпеки, особливості забезпечення інформаційної безпеки держави, правила відношення інформації до державної таємниці, конфіденційної інформації, що є власністю держави, недержавної конфіденційної і відкритої інформації що потребує захисту, шляхи побудови систем забезпечення інформаційної безпеки.

2. Компетентності

СК14 — Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об’єктів критичної інформаційної інфраструктури.

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. Методологічні основи інформаційної безпеки держави								
1	Тема 1. Інформаційна безпека як складова національної безпеки держави	0,75	0,75	18,5	20	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО2, МО3, МО6, МО7, МО9	СК14
2	Тема 2. Основні загрози інформаційної безпеки	0,75	0,75	18,5	20	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО2, МО3, МО7, МО9	СК14

№	Назва теми	Лекції	Практ./ Семін./ лаб	Самост. робота	Разом	Методи навчання	Методи оцінювання	СК
Змістовий модуль 2. Основи інформаційного протиборства								
3	Тема 3. Основи інформаційного протиборства	0,75	0,75	17	18,5	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО2, МО3, МО7, МО9	СК14
Змістовий модуль 3. Основи безпеки інформаційних технологій та інформаційних ресурсів								
4	Тема 4. Інформаційні системи та технології як об’єкти інформаційної безпеки	0,75	0,75	17	18,5	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО2, МО3, МО7, МО9	СК14
5	Тема 5. Основи безпеки інформаційних ресурсів	0,75	0,75	16,75	18,25	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО2, МО3, МО7, МО9	СК14
Змістовий модуль 4. Система забезпечення інформаційної безпеки								
6	Тема 6. Основи управління інформаційною безпекою	0,75	0,75	16,75	18,25	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО2, МО3, МО7, МО9	СК14
7	Тема 7. Методи та заходи забезпечення інформаційної безпеки України	0,75	0,75	16,75	18,25	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО2, МО3, МО7, МО9	СК14
8	Тема 8. Система та політика забезпечення інформаційної безпеки України	0,75	0,75	16,75	18,25	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО2, МО3, МО7, МО9	СК14
	Разом	**6**	**6**	**138**	**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); МН7 — індивідуальна науково-дослідна робота здобувачів вищої освіти.

Методи оцінювання: МО2 — усне або письмове опитування; МО3 — колоквіум; МО6 — есе; МО7 — презентації результатів виконаних завдань та досліджень; МО9 — залік.

4. Результати навчання

Знати:

– сутність, принципи та основні складові інформаційної безпеки як компонента національної безпеки держави;

– основні види загроз інформаційній безпеці, джерела їх виникнення, способи реалізації та можливі наслідки;

– сутність, форми, методи й засоби інформаційного протиборства, зокрема інформаційно-психологічного впливу;

– особливості функціонування інформаційних систем і технологій як об'єктів інформаційної безпеки;

– принципи класифікації, використання та захисту інформаційних ресурсів з урахуванням їхньої цінності й установленого правового режиму доступу;

– основні принципи, функції та методи управління інформаційною безпекою;

– нормативно-правові, організаційні й технічні методи та заходи забезпечення інформаційної безпеки України;

– структуру, основні завдання та повноваження суб'єктів системи забезпечення інформаційної безпеки України;

– основні положення державної політики у сфері інформаційної безпеки, принципи її формування та реалізації.

Вміти:

– аналізувати роль інформаційної безпеки в системі національної безпеки держави та визначати її значення для захисту національних інтересів;

– ідентифікувати основні загрози інформаційній безпеці, визначати джерела їх виникнення, можливі наслідки та пріоритетні напрями протидії;

– аналізувати ситуації інформаційного протиборства, розпізнавати ознаки інформаційно-психологічного впливу та обґрунтовувати заходи протидії;

– визначати основні вразливості інформаційних систем і технологій та обґрунтовувати вимоги до їх захисту;

– визначати категорію інформаційних ресурсів за правовим режимом доступу й обґрунтовувати відповідні заходи їх захисту;

– застосовувати базові підходи до управління інформаційною безпекою, зокрема ідентифікувати ризики, визначати пріоритети захисту та обґрунтовувати вибір заходів безпеки;

– добирати нормативно-правові, організаційні й технічні заходи для протидії загрозам інформаційній безпеці;

– аналізувати структуру та функції системи забезпечення інформаційної безпеки України, визначати роль відповідних державних органів та інших суб'єктів;

– аналізувати основні положення державної політики у сфері інформаційної безпеки й обґрунтовувати пропозиції щодо її реалізації та вдосконалення.

5. 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.

6. Критерії та форми контролю

Оцінювання — за 100-бальною шкалою (національна шкала / ЄКТС). Підсумковий бал = поточний контроль (80 %) + модульний контроль (20 %).

Академічна доброчесність: самостійне виконання завдань; коректне посилання на джерела; позначення частин тексту, згенерованих засобами ШІ. Порушення академічної доброчесності не толеруються.

7. Зміст тем

Тема 1. Інформаційна безпека як складова національної безпеки держави

Основні поняття та визначення інформаційної безпеки. Інтереси суб’єктів у інформаційній сфері. Співвідношення понять інформаційної та кібербезпеки. Основні нормативно-правові документи України у сфері інформаційної безпеки. Концепція інформаційної безпеки держави.

Тема 2. Основні загрози інформаційної безпеки

Дестабілізуючі фактори інформаційної безпеки. Класифікація загроз інформаційній безпеці. Ієрархічна класифікація загроз інформаційній безпеці. Джерела загроз інформаційній безпеці. Взаємозв’язки і мотивація здійснення кібер/інформаційних впливів.

Тема 3. Основи інформаційного протиборства

Основні поняття інформаційне протиборство. Основні поняття інформаційної війни в контексті інформаційної безпеки держави. Концепція інформаційної війни. Інформаційна зброя в інформаційній війні. Основні способи та заходи інформаційної боротьби. Методологія оцінки ефективності інформаційної боротьби

Тема 4. Інформаційні системи та технології як об’єкти інформаційної безпеки

Види та властивості інформації як предмета захисту інформаційної безпеки. Основні властивості інформації як предмета захисту інформаційної безпеки. Інформаційні системи як об’єкти захисту інформаційної безпеки. Основні характеристики інформаційної системи як об’єкта захисту інформаційної безпеки. Інформаційні технології та проблеми їхньої безпеки. Класифікація та види інформаційних технологій. Основні проблеми безпеки інформаційних технологій.

Тема 5. Основи безпеки інформаційних ресурсів

Загрози безпеці інформації та інформаційних ресурсів. Основні напрями забезпечення безпеки інформації та інформаційних ресурсів. Архітектура захисту інформації в мережах телекомунікацій. Моделі порушень інформаційних ресурсів.

Тема 6. Основи управління інформаційною безпекою

Стандарти менеджменту інформаційної безпеки. Політика інформаційної безпеки організації. Основні правила інформаційної безпеки організації. Система менеджменту інформаційної безпеки та її оцінка.

Тема 7. Методи та заходи забезпечення інформаційної безпеки України

Загальні методи забезпечення інформаційної безпеки України. Особливості забезпечення інформаційної безпеки України в різних сферах громадського життя.

Тема 8. Система та політика забезпечення інформаційної безпеки України

Національні інтереси України в інформаційній сфері та шляхи їх забезпечення. Завдання із забезпечення інформаційної безпеки України. Основні функції системи забезпечення інформаційної безпеки України. Основні елементи організаційної основи системи забезпечення інформаційної безпеки України.Основні положення політики забезпечення інформаційної безпеки України. Першочергові заходи щодо реалізації політики забезпечення інформаційної безпеки України.

8. Опис ІЗ/КПІЗ

Не передбачено навчальним планом.

9. Самостійна робота

№ п/п	Назва теми	Кількість годин	Форми контролю самостійної роботи
1	Інформаційна безпека як складова національної безпеки держави. Аналіз інформаційних потоків на підприємстві чи організації та визначення загроз.	18,5	МО2, МО3, МО9,
2	Основи інформаційного протиборства	18,5	МО2, МО3, МО9,
3	Основні загрози інформаційної безпеки. Інформаційні системи та технології як об’єкти інформаційної безпеки	17	МО2, МО3, МО9,
4	Основи безпеки інформаційних ресурсів	17	МО2, МО3, МО9,
5	Основи управління інформаційною безпекою	16,75	МО2, МО3, МО9,
6	Обґрунтовування застосування методів та засобів забезпечення інформаційної безпеки.	16,75	МО2, МО3, МО9,
7	Методи та заходи забезпечення інформаційної безпеки України.	16,75	МО2, МО3, МО9,
8	Аналіз інформаційних ризиків та розроблення політики безпеки. Система та політика забезпечення інформаційної безпеки України	16,75	МО2, МО3, МО9,
	Всього	138	

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. Основи інформаційної безпеки держави: Конспект лекцій / укладачі Ю.І. Хлапонін, І.М. Козубцов. К. КНУБА, 2024. 180 с.

Праці інших авторів:

2. Богуш В.М., Богуш В.В., Бровко В.Д., Гордієнко С.Б., Кудін А.М. Управління інформаційною безпекою та кібербезпекою організації. Навчальний посібник. К.:Ліра-К, 2026. 552 с.

3. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с.

ІІ. Наукові праці

Праці автора силабуса:

4. Ліщина В. О., Козубцова Л. М., Козубцов І. М., Глобін А. В. Модель формалізованого аудиту інформаційної безпеки організації на предмет виконанням вимог стандартів. Наука і техніка сьогодні. Серія: Техніка. 2025. № 9 (50). С. 1281–1296. URL: https://repository.lntu.edu.ua/handle/123456789/3794

5. Ліщина В. О., Козубцов І. М., Глобін А. В. Про потребу розумного поєднання віртуальної та фізичної лабораторних робіт в закладах вищої освіти. Наука і техніка сьогодні. Серія: Техніка. 2025. № 6 (47). С. 671–684. URL: https://repository.lntu.edu.ua/handle/123456789/3803

6. Козубцова Л. М., Ліщина В. О., Козубцов І. М. Від обізнаності до управління: концепція людських ризиків в системі кіберзахисту. Кібербезпека: освіта, наука, техніка. 2025. Вип. 2 (30). С. 360–373. URL: https://repository.lntu.edu.ua/handle/123456789/3802

7. Козубцов І. М., Ліщина В. О., Сулім В. О. Методика випереджаючого викладання навчальної дисципліни «Методологія наукових досліджень» здобувачам другого (магістерського) рівня вищої освіти освітньої програми «Комп’ютерні науки». Комп’ютерно-інтегровані технології: освіта, наука, виробництво. 2024. Вип. 54. С. 113-124. URL: https://repository.lntu.edu.ua/handle/123456789/3801

8. Козубцова Л. М., Козубцов І. І., Ліщина В. О., Штаненко С. Концепція навчально-тренувального комплексу підготовки військових спеціалістів інформаційної та кібербезпеки на засадах комп’ютерної гри (гейміфікації). Кібербезпека: освіта, наука, техніка. 2022. Вип. 2 (18). С. 49–60. URL: https://repository.lntu.edu.ua/handle/123456789/3811

Праці інших авторів:

9. Khlaponin Y., Izmailova O., Krasovska H., Krasovska K., Bodnar N., Abbas S.Q. Base of models of the information security risks assessment system. Proceedings of FRUCT’35Tampere, Finland, 24-26 April 2024 Oy, Finland, Issue 1, p.352-366. https://fruct.org/publications/volume-35/fruct35/files/Khl.pdf.

10. Ізмайлова О., Красовська Г., Красовська К. Система підтримки прийняття рішень оцінки ризиків інформаційної безпеки компанії. The 2st International Conference on Emerging Technology Trends on the Smart Industry and the Internet of Things, January 24-25th 2023, C.56-61.

11. Козубцов І.М. Модель дослідження впливу факторів та чинників соціального захисту на ефективність діяльності викладачів ВВНЗ із числа військовослужбовців. Освіта України в умовах воєнного стану: управління, цифровізація, євроінтеграційні аспекти: збірник тез доповідей V Міжнародної науково-практичної конференції (наукове електронне видання), (Київ, 26 жовт. 2023 р.). ДНУ «Інститут освітньої аналітики», 2023. С. 124 – 127.

12. Козубцов І.М., Козубцова Л.М. Прогноз можливих наслідків настання “колапсу інформаційних систем спеціального призначення”. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021 р.). Київ: НА СБУ, 2021. С. 50 – 53.

13. Козубцова Л.М., Бескровний О.І., Козубцов І.М., Соловйова Т.В. Пасенченко Ю.А. Управління ризиками на засадах оцінки вартість якості реалізації заходів з кібербезпеки на об’єктах критичної інформаційної інфраструктури. Міжнародна науково-практична конференція «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку» (Харків, 15 березня 2023 р.). Харків: НАНГ України, 2023. С. 18 – 20.

14. Козубцова Л.М., Козубцов І.М., Ліщина В.О., Штаненко С.С. Концепція навчально-тренувального комплексу підготовки військових спеціалістів інформаційної та кібербезпеки на засадах комп’ютерної гри (гейміфікації). Кібербезпека: освіта, наука, техніка. 2022. Том 2. № 18. С. 49 – 60.

15. Козубцова Л.М., Хлапонин Ю.І., Козубцов І.М. Методика оцінювання ефективності виконання заходів забезпечення кібербезпеки об’єктів критичної інформаційної інфраструктури організацій. Сучасні інформаційні технології у сфері безпеки та оборони. 2021. №2 (41). С. 17 – 22.

16. Хлапонін Ю.І., Козубцова Л.М., Козубцов І.М., Штонда Р.М. Функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури. Кібербезпека освіта, наука, техніка. 2022. Том 3. №15. С. 124 – 134.

III. Інформаційні ресурси

17. Безпека інформації. URL: http://jrnl.nau.edu.ua/index.php/Infosecurity

18. Національна бібліотека України імені В.І. Вернадського, наукова періодика розділу «Інформаційні ресурси»: 1. Інформаційна безпека: науковий журнал. URL: http://archive.nbuv.gov.ua/portal/natural/Ibez/index.html

19. Безпека людини, суспільства, держави: науковий журнал. URL: http://archive.nbuv.gov.ua/portal/Soc_Gum/iblsd/index.html

20. Захист інформації: науково-практичний журнал. URL: http://archive.nbuv.gov.ua/portal/natural/Zi/index.html.

21. Державна служба спеціального зв’язку та захисту інформації. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/index

22. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі». Київ : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. URL: http://www.dut.edu.ua/uploads/l_1023_75718671.pdf