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 «Системи технічного захисту інформації»
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., доцент Микола ПОЛІЩУК

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/2904

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Системи технічного захисту інформації»

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	6 кредитів ECTS / 180 годин, семестр 6
Форма контролю	екзамен, курсова робота
Викладач(і)	к.т.н., доцент Микола ПОЛІЩУК

1. Мета і завдання дисципліни

Мета: Формування у майбутніх фахівців комплексу теоретичних знань та практичних навичок щодо побудови, розгортання та експлуатації систем технічного захисту інформації (ТЗІ) від її витоку технічними каналами, а також від несанкціонованого доступу та спеціальних засобів технічної розвідки.

Завдання: Вивчення фізичної природи виникнення технічних каналів витоку інформації. Ознайомлення з нормативно-правовою базою України та міжнародними стандартами у сфері ТЗІ. Освоєння методів та засобів виявлення каналів витоку та захисту мовної, видової та цифрової інформації. Набуття навичок роботи з пошуковою апаратурою, вимірювальними комплексами та засобами активного/пасивного захисту.

Пререквізити: Нормативно-правове забезпечення кібербезпеки, Комп'ютерна електроніка та схемотехніка, Сигнали та процеси в системах захисту інформації

2. Компетентності

ІК — інтегральна компетентність: Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

ЗК01 — Здатність застосовувати знання у практичних ситуаціях.

СК03 — Здатність до використання програмних та програмно апаратних комплексів засобів захисту інформації в інформаційнотелекомунікаційних (автоматизованих) системах.

СК06 — Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

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. Основи безпеки даних в комп’ютерних системах								
1	Тема 1. Основні поняття щодо захисту інформації в автоматизованих системах	4/0,5	4/1	9/17	17/18,5	МН1, МН2, МН3	МО1, МО2, МО4, МО7, захист лабораторної роботи	ЗК01, СК06

№	Назва теми	Лекції денна/ заочна	Лаб. денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
2	Тема 2. Загрози безпеки даних та їх особливості	4/1	4/1	9/17	17/19	МН1, МН2, МН3	МО1, МО2, МО4, МО7, захист лабораторної роботи	ЗК01, СК06
3	Тема 3. Канали проникнення та принципи побудови систем захисту	4/0	8/1,5	9/17	21/18,5	МН1, МН2, МН3	МО1, МО2, МО4, МО7, захист лабораторної роботи	ЗК01, СК03, СК06
4	Тема 4. Стандарти із захисту інформації	4/0,5	8/1,5	10/17	22/19	МН1, МН2, МН3	МО1, МО2, МО4, МО7, захист лабораторної роботи	ЗК01, СК03
Змістовий модуль 2. Ідентифікація і аутентифікація користувачів та захист даних від несанкціонованого доступу								
5	Тема 5. Поняття про ідентифікацію користувача та її особливості	4/0,5	6/1	9/17	19/18,5	МН1, МН2, МН3	МО1, МО2, МО4, МО7, захист лабораторної роботи	ЗК01, СК03
6	Тема 6. Протоколи аутентифікації	4/0,5	5/1,5	9/17	18/19	МН1, МН2, МН3	МО1, МО2, МО4, МО7, захист лабораторної роботи	ЗК01, СК06
7	Тема 7. Основні принципи захисту даних від несанкціонованого доступу	3/0,5	5/1,5	10/17	18/19	МН1, МН2, МН3	МО1, МО2, МО4, МО7	ЗК01, СК03, СК06
8	Тема 8. Моделі управління доступом	3/0,5	5/1	10/17	18/18,5	МН1, МН2, МН3	МО1, МО2, МО4, МО7	ЗК01, СК03, СК06
	Курсова робота			30/30	30/30			
	Разом	**30/4**	**45/10**	**105/166**	**180/180**			

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); МН3 — наочний метод (метод ілюстрацій і метод демонстрацій).

Методи оцінювання: МО1 — екзамен; МО2 — усне або письмове опитування; МО4 — тестування; МО7 — презентації результатів виконаних завдань та досліджень.

4. Результати навчання

ПРН04. аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

ПРН31. застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;

ПРН34. приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;

ПРН35. вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;

5. Цілі сталого розвитку

ЦСР 9 – Промисловість, інновації та інфраструктура

ЦСР 11 – Сталий розвиток міст і громад

ЦСР 16 – Мир, справедливість та сильні інститути

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 (25 %) + модульний контроль (20 %) + курсова робота (15 %) + 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. Основні поняття щодо захисту інформації в автоматизованих системах

Основні поняття захисту інформації, зберігання, обробка та передача інформації незалежно від того, якою мовою (українською, російською чи якоюсь іншою) вона закодована, хто або що є її джерелом і який психологічний вплив вона справляє на людей.

Тема 2. Загрози безпеки даних та їх особливості

Найбільш поширені загрози, до яких схильні сучасні інформаційні системи. Уявлення про можливі загрози, а також про вразливі місця, які ці загрози зазвичай використовують, необхідно для того, щоб вибирати найбільш економічні засоби забезпечення безпеки.

Тема 3. Канали проникнення та принципи побудови систем захисту

Сучасні засоби перехоплення інформації. Класифікація каналів проникнення в систему. Заходи протидії загрозам. Принципи побудови систем захисту.

Тема 4. Стандарти із захисту інформації

Стандарти із захисту інформації. Світові стандарти із захисту даних в комп'ютерних системах. Державний стандарт України із захисту інформації.

Тема 5. Поняття про ідентифікацію користувача та її особливості

Поняття про ідентифікацію, найпоширеніші види ідентифікації: парольна ідентифікація, апаратна ідентифікація, біометрична ідентифікація. Переваги та недоліки ідентифікації.

Тема 6. Протоколи аутентифікації

Основні принципи та методи аутентифікації. Процедура аутентифікації та протоколи аутентифікації. Однофакторні та двофакторні методи аутентифікації.

Тема 7. Основні принципи захисту даних від несанкціонованого доступу

Технічний захист інформації. Два великих класи завдань технічного захисту інформації: захист інформації від несанкціонованого доступу і захисту інформації від витоку технічними каналами. Захист інформації на рівні прикладного й системного програмного забезпечення, апаратного мережевого забезпечення.

Тема 8. Моделі управління доступом

Правила управління доступом. Властивості моделей управління доступом. Матричні та багаторівневі моделі управління доступом. Використання паролів і механізмів контролю за доступом.

9. Курсова робота

Тематика курсових робіт з дисципліни «Системи технічного захисту інформації» максимально прикладні та відображають реальні інженерно-технічні завдання. Студенти мають виконати проектування, розрахунки або практичне дослідження, які стосуються множення та перетворення частоти електричного сигналу.

Захист проводиться кафедральною комісією в складі двох – трьох осіб, включаючи керівника роботи. Дні захисту курсових робіт оголошуються наперед, про що свідчить відповідне оголошення на дошці оголошень кафедри. На захисті можуть бути присутні студенти, викладачі та інші зацікавлені особи, які також мають право задавати питання доповідачеві

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. Методи та засоби технічного захисту інформації. Опорний конспект лекцій : навч. посіб. для здобувачів ступеня бакалавра за освітньою програмою «Системи технічного захисту інформації» спеціальності 125 «Кібербезпека», уклад.: В. М. Луценко, Д. О. Прогонов. Київ : КПІ ім. Ігоря Сікорського, 2021. 289 с.

2. Захист інформації в комп’ютерних системах: підручник з курсу «Захист інформації в комп’ютерних системах» призначено для студентів інженерно-технічного факультету ДВНЗ «УжНУ» спеціальності 123-«комп’ютерна інженерія», уклад.: О.М. Гапак, Балога С.І., Ужгород: ДВНЗ «УжНУ», 2021. 184с.

3. Пархоменко, О. М. Захист інформації від технічних каналів витоку: монографія. Дніпро: ДНУ, 2022. 184 с.

4. Коваль, Р. В., Гончар, О. В. Технічні методи забезпечення конфіденційності та цілісності

інформації. Тернопіль: ТНТУ ім. І. Пулюя, 2023. 208 с.

5. Мельник, А. П., Гнатюк, С. О. Комплексні системи технічного захисту інформації: проєктування та аналіз ефективності. Київ: КПІ ім. І. Сікорського, 2023. 236.

6. Романенко, І. В. Комплексний підхід до побудови систем технічного захисту інформації в організаціях. – Львів: ЛНУ ім. І. Франка, 2022. 200 с.

II. Наукові праці

Праці автора силабуса:

7. Burban, O., Polishchuk, M., Tkachuk, A., Kostiuchko, S., Polishchuk, L., & Tkachuk, V. Applying Box-Behnken design to research voice control automatic lighting systems. Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, 2026. Vol. 16(2)/ Pp. 44–49.

8. 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. № 15 (1). P. 55–61.

9. Гринюк С. В., Поліщук М. М., Костючко С. М., Конкевич Л. М., Крив’янчук Н. С. Система автоматичного захисту Smart Home з мобільним управлінням. Комп’ютерно-інтегровані технології: освіта, наука, виробництво, 2025. № 61. С. 242-248.

10. 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.

11. Kostiuchko, S., Polishchuk, M., Zabolotnyi, O., Tkachuk, A., & Twarog, B. (2021). The Auxiliary Parametric Sensitivity Method as a Means of Improving Project Management Analysis and Synthesis of Executive Elements. In M. H. Miraz, G. Southall, M. Ali, A. Ware, & S. Soomro (Eds.), Emerging Technologies in Computing (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol. 395, P. 92–103. Springer, Cham.

12. 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.

III. Інформаційні ресурси

13. Державний стандарт України Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96 URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38883&cat_id =38836 (дата звернення 09.05.2026).

14. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом URL: https://data.gov.ua/dataset/eab73672- 181f-4b20-8819-56d47723ff11 (дата звернення 10.06.2025).

15. Закон України Про криптографічний та технічний захист інформації URL: https://ips.ligazakon.net/document/NT1819 (дата звернення 09.06.2026).

16. Закон України «Про інформацію» URL: https://zakon.rada.gov.ua/laws /show/2657-12. (дата звернення 09.05.2026).