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 «Прикладна криптологія і стеганографія»
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/479

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Прикладна криптологія і стеганографія»

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 7
Форма контролю	екзамен
Викладач(і)	к.т.н., доцент Микола ПОЛІЩУК

1. Мета і завдання дисципліни

Мета: Вивчення навчальної дисципліни сприяє формуванню компетентності майбутніх спеціалістів в галузі сучасних технологій криптографічного захисту інформації в комп’ютерних системах, яка досягається через практичне володіння студентами навичками роботи з новітніми інформаційними технологіями у сфері безпеки і дослідницької роботи.

Завдання: Навчання студентів теоретичним та практичним основам в галузі сучасних технологій криптографії та криптографічного захисту інформації в комп’ютерних системах, яка досягається через практичне володіння студентами навичками роботи з новітніми інформаційними технологіями у сфері безпеки. Програма визначає обсяги знань, якими повинен опанувати здобувач першого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Пререквізити: Алгоритми захисту інформації та системне програмування, Теорія інформації та кодування

2. Компетентності

ЗК01 — Здатність застосовувати знання у практичних ситуаціях.

СК05 — Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

СК09 — Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

СК10 — Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

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 криптології, криптографії та криптографічного аналізу								
1	Тема 1. Основні поняття криптології	2/0,25	2/1	9/14	13/15,25	МН1, МН2, МН5	МО1, МО2, МО4, МО7, захист лабораторної роботи	ЗК01, СК05

№	Назва теми	Лекції денна/ заочна	Лаб. денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
2	Тема 2. Загальні відомості про захист інформації в інформаційно-телекомунікаційних системах	4/0	2/1	9/14	15/15	МН1, МН2	МО1, МО2, МО4, МО7, захист лабораторної роботи	ЗК01, СК05
3	Тема 3. Основи теорії засекреченого зв'язку К. Шеннона	4/0,25	4/1,75	9/13	17/15	МН1, МН2	МО1, МО2, МО4, МО7, захист лабораторної роботи	ЗК01, СК09, СК10
4	Тема 4. Шифрування та інфраструктура відкритих ключів	2/0,25	4/0,75	9/14	15/15	МН1, МН2	МО1, МО2, МО4, МО7, захист лабораторної роботи	ЗК01, СК05, СК10
5	Тема 5. Криптографічні хеш-функції	2/0,25	2/0,75	9/14	13/15	МН1, МН2	МО1, МО2, МО4, МО7	ЗК01, СК05, СК09, СК10
Змістовий модуль 2. Цілісність і достовірність даних								
6	Тема 6. Шифрування	4/0,25	4/0,75	9/14	17/15	МН1, МН2	МО1, МО2, МО4, МО7, захист лабораторної роботи	ЗК01, СК05
7	Тема 7. Використання цифрових підписів	2/0,25	4/1,75	9/13	15/15	МН1, МН2	МО1, МО2, МО4, МО7, захист лабораторної роботи	ЗК01, СК10, СК09, СК05
8	Тема 8. Центри сертифікації і система довіри на основі PKI	4/0,25	2/0,75	9/14	15/15	МН1, МН2	МО1, МО2, МО4, МО7, захист лабораторної роботи	ЗК01, СК05, СК10
9	Тема 9. Положення теорії комп’ютерної стеганографії	4/–	2/0,75	9/14	15/14,75	МН1, МН2	МО1, МО2, МО4, МО7, захист лабораторної роботи	ЗК01, СК05, СК10, СК09
10	Тема 10. Стеганографічні методи приховування інформації	2/0,25	4/0,75	9/14	15/15	МН1, МН2	МО1, МО2, МО4, МО7, захист лабораторної роботи	ЗК01, СК05, СК09
	Разом	**30/2**	**30/10**	**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); МН5 — відеометод у сполученні з новітніми інформаційними технологіями та комп’ютерними засобами навчання (дистанційні, мультимедійні, веб-орієнтовані тощо).

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

4. Результати навчання

ПРН19. застосовувати теорії та методи захисту для забезпечення безпеки інформації в

інформаційно-телекомунікаційних системах;

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

ПРН47. вирішувати задачі захисту інформації, що обробляється в інформаційнотелекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;

ПРН48. виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційнотелекомунікаційних системах;

5. Цілі сталого розвитку

ЦСР 4 – Якісна освіта

ЦСР 9 – Промисловість, інновації та інфраструктура

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 (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. Основні поняття криптології

Основні терміни: криптологія, криптографія, криптоаналіз, текст, шифрування, розшифрування, ключ, простір ключів, криптографічна система, криптологічною стійкістю, вимоги до криптографічних систем. Принципи побудови й схеми криптологічних систем. Класифікація алгоритмів шифрування

Тема 2. Загальні відомості про захист інформації в інформаційно-телекомунікаційних системах

Загальні відомості про захист інформації в інформаційно-телекомунікаційних системах. Основні завдання захисту інформації та їх призначення для користувача. Роль криптографічних протоколів у загальній задачі забезпечення інформаційної безпеки. Загальні відомості про класичну криптологію, криптографію та криптографічний аналіз.

Тема 3. Основи теорії засекреченого зв'язку К. Шеннона

Модель системи передачі шифрованих повідомлень. Досконала криптографічна система. Класифікація методів шифрування повідомлень. Класифікація методів шифрування повідомлень Криптографічний аналіз. Класифікація атак криптографічного аналізу.

Тема 4. Шифрування та інфраструктура відкритих ключів

Захист комунікацій. Методи захисту пристроїв і хостів в мережевій інфраструктурі. Історичні приклади методів шифрування і розшифровки тексту, методи криптографії, а також фізичні пристосування і пристрої. Шифрування з використанням підстановочного шифру Цезаря. Багатоалфавітніх шифри. Шифр Віженера. Криптоаналіз – злом коду. Використання ключів у

шифруванні.

Тема 5. Криптографічні хеш-функції

Створення хеш-коду. Як працює криптографічний алгоритм хешування. Формула хешування. MD5 і SHA. Алгоритми хешування MD5. Код аутентифікації повідомлень на основі хешу. Використання функції HMAC в маршрутизаторах Cisco.

Тема 6. Шифрування

Класи шифрування для забезпечення конфіденційності даних. Симетричне шифрування. Симетричні алгоритми шифрування. Класифікація алгоритмів шифрування. Алгоритми асиметричного шифрування. Асиметричне шифрування – конфіденційність. Асиметричне шифрування – аутентифікація. Асиметричне шифрування – цілісність. Алгоритм Діффі - Хеллмана.

Тема 7. Використання цифрових підписів

Цифрові підписи. Сервіси, що надаються цифровими підписами. Властивості цифрового підпису. Цифрові підписи коду. Цифрові підписи для цифрових сертифікатів.

Тема 8. Центри сертифікації і система довіри на основі PKI

Управління загальними ключами. Інфраструктура загальних ключів. Система центрів PKI. Система довіри на основі PKI. Взаємодія різних постачальників PKI. Реєстрація, аутентифікація та відкликання сертифікатів. Застосування PKI. Шифрування мережевих транзакцій. Шифрування і моніторинг безпеки. Шифрування та інфраструктура відкритих ключів.

Тема 9. Положення теорії комп’ютерної стеганографії

Деякі узагальнені термінологічні поняття. Узагальнена модель стегосистеми. Класифікація стегосистем. Безключові стегосистеми. Стегосистеми із секретним ключем. Стегосистеми з відкритим ключем. Змішані стегосистеми. Стенографічний аналіз. Можливі ознаки на стенографічну систему. Основні етапи практичного стеганоаналізу. Аналіз стійкості стегосистеми. Абсолютно надійна стегосистема. Пасивна атака: виявлення прихованих повідомлень. Активні і зловмисні атаки. Стійкість стенографічної системи до активних атак. Відкритий стенографічний канал.

Тема 10. Стеганографічні методи приховування інформації

Класифікація методів приховування інформації. Текстові стеганографи. Методи перекручування формату текстового документа. Синтаксичні методи. Семантичні методи. Методи генерації стеганограм. Приховування даних у зображенні і відео. Методи заміни. Методи приховування в частотній області зображення. Широкосмугові методи. Статистичні методи. Методи перекручування. Структурні методи. Приховування інформації в звуковому середовищі. Стеганографічні методи захисту даних в звуковому середовищі.

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. Бойко, В. І., Кравчук, О. М. Криптографічні методи захисту інформації : навчальний посібник. Київ: НАУ, 2021. 212 с.

2. Білан, С. В., Федоренко, І. О. Сучасні методи шифрування інформації та їх програмна реалізація. Львів : ЛНУ ім. І. Франка, 2022. 184 с.

3. Мельник, А. П., Шевчук, В. П. Основи стеганографії та цифрового водяного маркування : навч. посіб. Харків : ХНУРЕ, 2021. 168 с.

4. Гончар, О. В., Кузьменко, С. І. Прикладна криптологія : теорія та практика. Київ : КПІ ім. І. Сікорського, 2023. 240 с.

II. Наукові праці

Праці автора силабуса:

5. Литвин В., Костючко С., Поліщук М., Гринюк С. Криптографічна обробка облікових даних користувача в мережевому обладнанні. Міжнародна науково-практична конференція «Сучасні інформаційні технології: від теорії до практики (СІнТех-2026)», м. Луцьк, 22-23 травня 2026 р. Луцьк : ЛНТУ. С. 671-673.

6. 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. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, 2021. P. 174–184.

7. Поліщук, М., Семенюк, О., Поліщук, Л., Ломакін, М. Можливості авторизації та захисту даних користувача під час розробки хмарних веб-додатків для IoT. КОМП’ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ: ОСВІТА, НАУКА, ВИРОБНИЦТВО.Луцьк, 2023. Вип.52. С. 94-103.

8. Костючко С., Поліщук М., Конкевич Л., Абрамович В. Аналітика поведінки користувачів і об'єктів. Технічні вісті. Львів, 2022. №1(55), 2(56). С. 34-35.

Праці інших авторів:

9. Пархоменко, О. М. Сучасні методи криптоаналізу симетричних шифрів. Дніпро : ДНУ, 2022. 153 с.

10. Шевченко, О. Г. Алгоритми шифрування та захисту даних у комп’ютерних мережах: монографія. Київ : НАУ, 2023. 230 с.

III. Інформаційні ресурси

11. Cisco. Networking Academy. URL: https://www.netacad.com (дата звернення: 23.05.2026)