МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ЦИФРОВИХ, ОСВІТНІХ ТА СОЦІАЛЬНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету
_____ Галина ГЕРАСИМЧУК
«28» серпня 2026 р.

ЗАТВЕРДЖУЮ
Перший проректор
_____ Надія КОВАЛЬЧУК
«29» серпня 2026 р.

СИЛАБУС

з освітнього компонента «Комп'ютерна безпека та криптографія»
ступінь вищої освіти – бакалавр
галузь знань – 01 Освіта/Педагогіка
спеціальність – 014.09 Середня освіта (Інформатика)
освітня програма – Середня освіта. Інформатика

Кафедра цифрових освітніх технологій

Силабус склав(ла) доцент кафедри цифрових освітніх технологій, к.пед.н., доцент Юлія МЕЛЬНИЧУК

Силабус затверджений на засіданні кафедри цифрових освітніх технологій, протокол № 1а від «28» серпня 2026 р.

Завідувач кафедри к.пед.н., доцент Віталій КАБАК

Розглянуто та схвалено групою забезпечення освітньої програми «Середня освіта. Інформатика», протокол № 1а від «28» серпня 2026 р.

Гарант ОП «Середня освіта. Інформатика» к.пед.н., доцент Юлія МЕЛЬНИЧУК

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

Затверджений силабус онлайн:
https://e.lntu.edu.ua/syllabus/3495

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Комп'ютерна безпека та криптографія»

Освітня програма	Середня освіта. Інформатика
Галузь знань / Спеціальність	01 Освіта/Педагогіка / 014.09 Середня освіта (Інформатика)
Рівень вищої освіти	перший (бакалаврський)
Статус дисципліни	нормативна
Мова викладання	українська
Обсяг	4 кредити ECTS / 120 годин, семестр 8 (денна); 4 (заочна)
Форма контролю	екзамен
Викладач(і)	к.пед.н., доцент Юлія МЕЛЬНИЧУК

1. Мета і завдання дисципліни

Мета: Метою вивчення освітнього компонента «Комп'ютерна безпека та криптографія» є формування у здобувачів вищої освіти системи теоретичних знань і практичних умінь щодо основ комп'ютерної безпеки, принципів криптографічного захисту інформації, математичних засад криптографії, методів шифрування та криптоаналізу, сучасних криптографічних алгоритмів і стандартів, а також розвиток здатності застосовувати криптографічні методи й інструменти для забезпечення конфіденційності, цілісності та автентичності інформації в комп'ютерних системах і цифровому освітньому середовищі.

Завдання: Основними завданнями вивчення освітнього компонента є:
- формування розуміння сутності комп'ютерної безпеки, основних загроз інформаційним ресурсам і принципів забезпечення конфіденційності, цілісності та доступності інформації;
- засвоєння понятійного апарату криптології, принципів побудови та класифікації криптографічних систем;
- ознайомлення з математичними основами криптографічних перетворень, зокрема модульною арифметикою, двійковими операціями та їх застосуванням в алгоритмах шифрування;
- вивчення принципів функціонування класичних шифрів заміни та перестановки, поліалфавітних і поліграмних криптографічних систем;
- набуття практичних навичок шифрування, розшифрування повідомлень і застосування базових методів криптоаналізу;
- формування вмінь оцінювати криптографічну стійкість алгоритмів і визначати потенційні загрози безпеці криптосистем;
- вивчення принципів побудови та функціонування симетричних потокових і блокових алгоритмів шифрування;
- ознайомлення із сучасними криптографічними стандартами, зокрема AES, ChaCha20 та національними стандартами криптографічного захисту інформації;
- формування уявлень про принципи асиметричної криптографії, криптографічного хешування та електронного підпису;
- розвиток практичних умінь застосовувати програмні засоби та цифрові інструменти для реалізації, дослідження й порівняння криптографічних алгоритмів;
- формування здатності використовувати набуті знання для забезпечення безпечної роботи з інформацією та розвитку культури кібербезпеки в освітньому середовищі.

Пререквізити: Для вивчення дисципліни необхідні базові знання з алгоритмізації та програмування, дискретної математики, комп’ютерних систем і мереж: двійкове подання даних, логічні операції, основи теорії чисел та модульної арифметики, побудова й програмна реалізація алгоритмів, принципи роботи операційних систем і передавання даних у мережах. Необхідні практичні вміння працювати з файлами, використовувати середовище програмування та аналізувати результати виконання програм.

2. Компетентності

ІК — інтегральна компетентність: Здатність розв’язувати складні спеціалізовані задачі у галузі середньої освіти, що передбачає застосування теоретичних знань і практичних умінь з наук предметної спеціальності, педагогіки, психології, теорії та методики навчання і характеризується комплексністю та невизначеністю умов організації освітнього процесу в закладах загальної середньої освіти.

ЗК01 — Здатність до абстрактного мислення, аналізу та синтезу, до застосування знань у практичних ситуаціях.

ЗК02 — Знання й розуміння предметної області та професійної діяльності.

ЗК04 — Здатність орієнтуватися в інформаційному просторі, здійснювати пошук, аналіз та обробку інформації з різних джерел, ефективно використовувати цифрові ресурси та технології в освітньому процесі.

ЗК05 — Здатність діяти автономно, приймати обґрунтовані рішення у професійній діяльності і відповідати за їх виконання, діяти відповідально і свідомо на основі чинного законодавства та етичних міркувань (мотивів).

ЗК12 — Здатність вчитися і оволодівати сучасними знаннями.

СК01 — Здатність перенесення системи наукових знань у професійну діяльність та в площину навчального предмету.

СК10 — Здатність використовувати знання наукових фактів, концепцій, теорій, принципів і методів сучасної інформатики у практиці навчання інформатики.

СК11 — Володіння методами інформаційного моделювання; здатність реалізовувати інформаційну модель засобами інформаційно-комунікаційних технологій; проводити комп’ютерний експеримент, інтерпретувати, аналізувати та узагальнювати його результати.

СК12 — Здатність до використання сучасних методів розробки та дослідження алгоритмів розв'язування задач у моделюванні об'єктів і процесів та реалізації цих алгоритмів сучасними мовами програмування.

СК13 — Здатність використовувати програмні засоби загального та спеціального призначення для розв’язання прикладних задач з інформатики.

СК14 — Володіння технологіями налагодження, обслуговування та експлуатації комп’ютерної мережі; здатність реалізовувати комплекс заходів, спрямованих на забезпечення захищеності інформації, здатність формувати вміння безпечної роботи школярів у комп’ютерній мережі.

СК19 — Здатність виконувати математичний опис, аналіз та синтез дискретних об’єктів та систем, використовуючи поняття й методи дискретної математики та теорії алгоритмів.

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. Теоретичні основи комп'ютерної безпеки та криптографії								
1	Тема 1. Основи комп'ютерної та інформаційної безпеки	2/1	2/1	4/6	8/8	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО1, МО2, МО3, МО4, МО5, МО7	ЗК01, ЗК02, ЗК04, ЗК05, ЗК12, СК01, СК10, СК11, СК12, СК13, СК14, СК19

№	Назва теми	Лекції денна/ заочна	Лаб. денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
2	Тема 2. Теоретичні засади криптології та класифікація криптографічних систем	2/1	2/1	4/6	8/8	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО1, МО2, МО3, МО4, МО5, МО7	ЗК01, ЗК02, ЗК04, ЗК05, ЗК12, СК01, СК10, СК11, СК12, СК13, СК14, СК19
3	Тема 3. Математичні основи криптографічних перетворень	2/1	2/1	4/6	8/8	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО1, МО2, МО3, МО4, МО5, МО7	ЗК01, ЗК02, ЗК04, ЗК05, ЗК12, СК01, СК10, СК11, СК12, СК13, СК14, СК19
4	Тема 4. Класичні шифри заміни та перестановки	2/0	2/0	4/8	8/8	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО1, МО2, МО3, МО4, МО5, МО7	ЗК01, ЗК02, ЗК05, ЗК04, ЗК12, СК01, СК10, СК11, СК12, СК13, СК14, СК19
5	Тема 5. Поліграмні та поліалфавітні криптографічні системи	2/0	2/0	4/8	8/8	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО1, МО2, МО3, МО4, МО5, МО7	ЗК01, ЗК02, ЗК04, ЗК05, ЗК12, СК01, СК10, СК11, СК12, СК13, СК14, СК19
6	Тема 6. Методи криптоаналізу класичних шифрів	2/0	2/0	4/8	8/8	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО1, МО2, МО3, МО4, МО5, МО7	ЗК01, ЗК02, ЗК04, ЗК05, ЗК12, СК01, СК10, СК11, СК12, СК13, СК14, СК19

№	Назва теми	Лекції денна/ заочна	Лаб. денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
7	Тема 7. Криптографічна стійкість шифрів та основні типи криптографічних атак	2/0	2/0	4/8	8/8	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО1, МО2, МО3, МО4, МО5, МО7, модульна контрольна робота	ЗК01, ЗК02, ЗК04, ЗК05, ЗК12, СК01, СК10, СК11, СК12, СК13, СК14, СК19
Змістовий модуль 2. Сучасні криптографічні алгоритми та технології шифрування								
8	Тема 8. Принципи симетричної криптографії та потокового шифрування	2/1	2/1	4/6	8/8	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО1, МО2, МО3, МО4, МО5, МО7	ЗК01, ЗК02, ЗК04, ЗК05, ЗК12, СК01, СК10, СК11, СК12, СК13, СК14, СК19
9	Тема 9. Генератори псевдовипадкових чисел у криптографічних системах	2/1	2/1	4/6	8/8	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО1, МО2, МО3, МО4, МО5, МО7	ЗК01, ЗК02, ЗК04, ЗК05, ЗК12, СК01, СК10, СК11, СК12, СК13, СК14, СК19
10	Тема 10. Потокові алгоритми шифрування RC4, ChaCha20 та «Струмок»	2/1	2/1	4/6	8/8	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО1, МО2, МО3, МО4, МО5, МО7	ЗК01, ЗК02, ЗК04, ЗК05, ЗК12, СК01, СК10, СК11, СК12, СК13, СК14, СК19
11	Тема 11. Блокові симетричні шифри. Мережа Фейстеля та алгоритм DES	2/0	2/0	4/8	8/8	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО1, МО2, МО3, МО4, МО5, МО7	ЗК01, ЗК02, ЗК04, ЗК05, ЗК12, СК01, СК10, СК11, СК12, СК13, СК14, СК19

№	Назва теми	Лекції денна/ заочна	Лаб. денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
12	Тема 12. Алгоритми шифрування ГОСТ 28147 та IDEA	2/0	2/0	4/8	8/8	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО1, МО2, МО3, МО4, МО5, МО7	ЗК01, ЗК02, ЗК04, ЗК05, ЗК12, СК01, СК10, СК11, СК12, СК13, СК14, СК19
13	Тема 13. Сучасний стандарт блокового шифрування AES	2/0	2/0	4/8	8/8	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО1, МО2, МО3, МО4, МО5, МО7	ЗК01, ЗК02, ЗК04, ЗК05, ЗК12, СК01, СК10, СК11, СК12, СК13, СК14, СК19
14	Тема 14. Національний стандарт блокового шифрування ДСТУ 7624:2014 «Калина»	2/0	2/0	4/8	8/8	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО1, МО2, МО3, МО4, МО5, МО7	ЗК01, ЗК02, ЗК04, ЗК05, ЗК12, СК01, СК10, СК11, СК12, СК13, СК14, СК19
15	Тема 15. Режими роботи блокових шифрів та практичне застосування криптографії	2/0	2/0	4/8	8/8	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО1, МО2, МО3, МО4, МО5, МО7, модульна контрольна робота	ЗК01, ЗК02, ЗК04, ЗК05, ЗК12, СК01, СК10, СК11, СК12, СК13, СК14, СК19
	Разом	**30/6**	**30/6**	**60/108**	**120/120**			

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); 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: МО1 — екзамен; МО2 — усне або письмове опитування; МО3 — колоквіум; МО4 — тестування; МО5 — командні проєкти; МО7 — презентації результатів виконаних завдань та досліджень.

4. Результати навчання

ПРН07. Демонструє знання основ фундаментальних і прикладних наук (відповідно до предметної спеціальності), оперує базовими категоріями та поняттями предметної області

спеціальності.

ПРН09. Застосовує сучасні інформаційно-комунікаційні та цифрові технології у професійній діяльності.

ПРН14. Визначає структуру предметної галузі інформатики, її місце в системі наук, пояснює перспективи розвитку інформатики та інформаційних технологій, їхнє суспільне значення.

ПРН15. Знає та розуміє фізичні, логічні та математичні основи інформаційних технологій; пояснює та застосовує способи двійкового кодування текстової, числової, графічної, звукової та відеоінформації.

ПРН18. Визначає та застосовує методи розроблення та дослідження алгоритмів розв’язування задач з інформатики, описує і застосовує методи оцінювання ефективності алгоритмів.

ПРН19. Знає та розуміє етико-правові засади використання інформаційно-комунікаційних технологій; застосовує засоби й методи захисту інформації та безпеки в мережі Інтернет.

ПРН22. Уміє реалізувати алгоритми розв’язання задач мовами програмування, вибирати й застосовувати інформаційно-комунікаційні технології; розв'язує задачі шкільного курсу інформатики різного рівня складності.

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 (30 %) + модульний контроль (30 %) + 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. Основи комп'ютерної та інформаційної безпеки

Поняття інформаційної, комп'ютерної та кібербезпеки, їх взаємозв'язок і значення в сучасному цифровому середовищі. Інформаційні ресурси як об'єкти захисту. Основні принципи забезпечення інформаційної безпеки: конфіденційність, цілісність і доступність інформації. Автентичність, неспростовність та підзвітність як додаткові властивості захищених інформаційних систем. Класифікація загроз інформаційній безпеці, джерела їх виникнення та можливі наслідки. Поняття вразливості, ризику та інциденту інформаційної безпеки. Основні види комп'ютерних атак і порушень безпеки даних. Фізичні, апаратні, програмні, організаційні та криптографічні методи захисту інформації. Особливості забезпечення комп'ютерної безпеки в освітньому середовищі. Роль криптографічних методів у комплексній системі захисту інформації.

Тема 2. Теоретичні засади криптології та класифікація криптографічних систем

Поняття криптології, її предмет, завдання та основні напрями розвитку. Криптографія і криптоаналіз як взаємопов'язані складові криптології. Історичні етапи становлення криптографічних методів захисту інформації. Основні поняття криптографії: відкритий текст, шифротекст, шифр, криптографічний алгоритм, криптографічний ключ, шифрування та

розшифрування. Структура криптографічної системи та математична модель процесу шифрування. Основні принципи побудови криптосистем, зокрема принцип Керкхоффа. Класифікація криптографічних систем за типом ключів, способом перетворення інформації та технологією шифрування. Симетричні й асиметричні криптосистеми, їх особливості, переваги та обмеження. Блокові та потокові шифри. Основні напрями застосування криптографії в комп'ютерних системах, мережевих технологіях, електронному документообігу та цифрових комунікаціях.

Тема 3. Математичні основи криптографічних перетворень

Роль математичного апарату в побудові та функціонуванні криптографічних алгоритмів. Основи теорії чисел у криптографії. Подільність цілих чисел, прості числа та найбільший спільний дільник. Поняття конгруенції та основні операції модульної арифметики. Додавання, віднімання, множення й піднесення до степеня за модулем. Обернені елементи за модулем та їх визначення. Алгоритм Евкліда і розширений алгоритм Евкліда. Двійкова система числення та особливості подання інформації у вигляді бітових послідовностей. Логічні операції над бітами, зокрема XOR, AND, OR і NOT. Поняття скінченних полів GF(2) та $GF(2^n)$. Основні алгебраїчні операції у скінченних полях. Використання модульної арифметики, бітових операцій і скінченних полів у симетричних криптографічних алгоритмах. Приклади реалізації математичних криптографічних перетворень засобами програмування.

Тема 4. Класичні шифри заміни та перестановки

Історія виникнення та розвитку класичних методів шифрування інформації. Основні принципи криптографічних перетворень на основі заміни та перестановки символів. Моноалфавітні шифри заміни, їх структура та принципи функціонування. Шифр Цезаря: математична модель, алгоритми шифрування та розшифрування повідомлень. Квадрат Полібія та особливості його використання. Шифри перестановки та їх класифікація. Шифр Скитала, принципи формування й відновлення зашифрованих повідомлень. Шифр частоколу та особливості перестановки символів. Поняття криптографічного ключа в класичних шифрах. Аналіз переваг, недоліків і обмежень класичних методів шифрування. Практична реалізація алгоритмів заміни та перестановки засобами програмування. Використання класичних шифрів для демонстрації принципів криптографії в навчанні інформатики.

Тема 5. Поліграмні та поліалфавітні криптографічні системи

Поняття поліграмного та поліалфавітного шифрування. Передумови розвитку складніших криптографічних систем на основі класичних шифрів. Принципи шифрування груп символів та використання декількох алфавітів заміни. Шифр Плейфера: структура ключової таблиці, правила формування біграм, алгоритми шифрування та розшифрування повідомлень. Криптосистема Хілла та використання матричних перетворень у криптографії. Математичні основи шифру Хілла, побудова ключових матриць та умови їх оборотності. Шифр Віженера: принцип поліалфавітної заміни, формування ключової послідовності, алгоритми шифрування та розшифрування. Порівняльна характеристика моноалфавітних, поліграмних і поліалфавітних шифрів. Особливості застосування математичних методів у класичних криптографічних системах. Програмна реалізація поліграмних і поліалфавітних алгоритмів шифрування.

Тема 6. Методи криптоаналізу класичних шифрів

Поняття криптоаналізу, його мета, завдання та місце в оцінюванні безпеки криптографічних систем. Основні підходи до аналізу зашифрованих повідомлень. Статистичні закономірності природних мов та їх використання в криптоаналізі. Частотний аналіз символів, біграм і триграм у відкритих та зашифрованих текстах. Побудова й інтерпретація частотних таблиць і гістограм. Методи криптоаналізу моноалфавітних шифрів заміни. Визначення ключів шифрування методом повного перебору. Особливості криптоаналізу поліалфавітних шифрів. Метод Казіскі та його застосування для визначення довжини ключа. Метод Фрідмана та поняття індексу збігу. Порівняльний аналіз ефективності методів криптоаналізу класичних шифрів. Використання програмних засобів для автоматизації статистичного аналізу зашифрованих повідомлень. Оцінювання обмежень класичних криптографічних алгоритмів.

Тема 7. Криптографічна стійкість шифрів та основні типи криптографічних атак

Поняття криптографічної стійкості та її значення для забезпечення безпеки криптографічних систем. Основні критерії оцінювання криптостійкості алгоритмів шифрування. Абсолютна та обчислювальна стійкість криптосистем. Теоретичні засади абсолютно стійкого шифру та принцип одноразового блокнота. Вплив довжини ключа, розміру ключового простору та складності алгоритму на криптографічну стійкість. Поняття криптографічної атаки, її мета та основні характеристики. Класифікація атак за характером взаємодії з криптосистемою, способом пошуку ключа та рівнем доступу до даних. Атаки на основі відомого відкритого тексту, обраного відкритого тексту та обраного шифротексту. Метод повного перебору ключів. Диференціальний і лінійний криптоаналіз. Атаки на криптографічні протоколи, програмні реалізації та побічні канали. Загальні принципи протидії криптографічним атакам. Роль криптоаналізу в оцінюванні надійності сучасних криптографічних алгоритмів.

Тема 8. Принципи симетричної криптографії та потокового шифрування

Поняття симетричної криптографії та її місце в сучасних системах захисту інформації. Основні принципи симетричного шифрування. Використання спільного секретного ключа для шифрування та розшифрування повідомлень. Переваги й обмеження симетричних криптографічних систем. Класифікація симетричних алгоритмів шифрування. Порівняльна характеристика потокових і блокових шифрів. Поняття потокового шифрування та його основні властивості. Принцип формування ключового потоку та його використання для криптографічного перетворення інформації. Операція XOR як основа реалізації потокового шифрування. Синхронні та самосинхронізовані потокові шифри. Поняття початкового вектора та одноразового значення (nonce). Вимоги до секретності ключів і неповторюваності ключових потоків. Переваги, недоліки та сфери практичного застосування потокового шифрування в цифрових комунікаціях.

Тема 9. Генератори псевдовипадкових чисел у криптографічних системах

Поняття випадкових і псевдовипадкових чисел та їх роль у криптографії. Вимоги до випадковості й непередбачуваності послідовностей, що використовуються в криптографічних системах. Класифікація генераторів випадкових і псевдовипадкових чисел. Принципи побудови та функціонування генераторів псевдовипадкових чисел (PRNG). Поняття початкового значення генератора (seed) та його вплив на формування послідовності. Лінійний конгруентний генератор (LCG): математична модель, алгоритм роботи, переваги й обмеження. Генератори на основі регістрів зсуву з лінійним зворотним зв'язком (LFSR). Генератор Блюма — Блюма — Шуба (BBS) та його математичні засади. Криптографічно стійкі генератори псевдовипадкових чисел (CSPRNG). Основні підходи до оцінювання статистичних властивостей псевдовипадкових послідовностей. Застосування генераторів у формуванні криптографічних ключів, початкових векторів і ключових потоків. Програмна реалізація та дослідження властивостей генераторів псевдовипадкових чисел.

Тема 10. Потокові алгоритми шифрування RC4, ChaCha20 та «Струмок»

Загальна характеристика потокових криптографічних алгоритмів та особливості їх практичного застосування. Історія розвитку потокових шифрів. Алгоритм RC4: принцип побудови, структура внутрішнього стану, процедура ініціалізації ключа та формування ключового потоку. Основні етапи шифрування й розшифрування даних засобами RC4. Відомі вразливості RC4 та причини відмови від його використання в сучасних захищених системах. Сучасний потоковий алгоритм ChaCha20: принципи побудови, структура стану, основні операції та раундові перетворення. Поняття ключа, nonce та лічильника блоків у ChaCha20. Особливості застосування ChaCha20 у сучасних криптографічних протоколах. Національний стандарт потокового шифрування ДСТУ 8845:2019 «Струмок»: призначення, структура та загальні принципи функціонування. Порівняльна характеристика RC4, ChaCha20 та «Струмка» за архітектурою, принципами роботи й криптографічною стійкістю. Практичні аспекти використання потокових шифрів для захисту цифрової інформації.

Тема 11. Блокові симетричні шифри. Мережа Фейстеля та алгоритм DES

Поняття блокового симетричного шифрування та його основні принципи. Відмінності між блоковими та потоковими криптографічними алгоритмами. Поняття блоку даних, секретного

ключа, раунду шифрування та раундового ключа. Принципи побудови ітеративних блокових шифрів. Поняття дифузії та конфузії в криптографії. Мережа Фейстеля як структурна основа побудови блокових алгоритмів. Принципи поділу блока на частини, виконання раундових перетворень і формування раундових ключів. Особливості процесів шифрування та розшифрування в мережі Фейстеля. Історія створення стандарту шифрування даних DES (Data Encryption Standard). Основні параметри DES: розмір блока, довжина ключа та кількість раундів. Початкова й кінцева перестановки, функція раундового перетворення, S-блоки та P-перестановки. Процедура формування раундових ключів. Основні переваги, обмеження та відомі вразливості DES. Історичне значення DES для розвитку сучасних блокових криптографічних алгоритмів.

Тема 12. Алгоритми шифрування ГОСТ 28147 та IDEA

Розвиток блокових криптографічних алгоритмів і підходів до їх стандартизації. Загальна характеристика алгоритму ГОСТ 28147-89 та його застосування в історичних криптографічних системах. Основні параметри алгоритму: розмір блока, довжина ключа та кількість раундів. Принципи побудови алгоритму на основі мережі Фейстеля. Особливості виконання раундових перетворень, використання таблиць заміни та циклічних зсувів. Процеси шифрування й розшифрування інформації. Алгоритм IDEA (International Data Encryption Algorithm): історія створення, призначення та загальна структура. Основні параметри IDEA, принципи формування підключів і виконання раундових перетворень. Використання операцій XOR, додавання за модулем та множення за модулем у структурі IDEA. Особливості реалізації алгоритму та його криптографічні властивості. Порівняльний аналіз DES, ГОСТ 28147 та IDEA за структурою, параметрами, криптографічною стійкістю та практичним значенням. Історична роль цих алгоритмів у розвитку сучасних стандартів симетричного шифрування.

Тема 13. Сучасний стандарт блокового шифрування AES

Передумови створення сучасного стандарту блокового шифрування AES (Advanced Encryption Standard). Історія розроблення та стандартизації алгоритму Rijndael. Основні характеристики AES: розмір блока, допустимі довжини ключів і кількість раундів шифрування. Загальна архітектура алгоритму та принципи побудови мережі підстановок і перестановок. Представлення даних у вигляді матриці стану. Основні етапи раундового перетворення: SubBytes, ShiftRows, MixColumns та AddRoundKey. Математичні засади виконання криптографічних операцій у скінченному полі GF(2^8). Алгоритм розгортання ключа та формування раундових ключів. Особливості початкового, основних і завершального раундів шифрування. Принципи розшифрування інформації засобами AES. Порівняльна характеристика AES-128, AES-192 та AES-256. Криптографічна стійкість AES та особливості його програмної й апаратної реалізації. Практичне застосування AES для шифрування файлів, захисту даних і забезпечення безпеки цифрових комунікацій.

Тема 14. Національний стандарт блокового шифрування ДСТУ 7624:2014 «Калина»

Розвиток національних криптографічних стандартів України та їх значення для забезпечення інформаційної безпеки. Загальна характеристика ДСТУ 7624:2014 «Калина», призначення та сфери застосування. Основні принципи побудови сучасних блокових симетричних шифрів. Архітектура криптографічного алгоритму «Калина». Параметри алгоритму, розміри блоків даних і криптографічних ключів. Структура раундових перетворень і принципи формування раундових ключів. Основні операції криптографічного перетворення даних. Процеси шифрування та розшифрування інформації. Особливості реалізації алгоритму «Калина» в програмних системах. Порівняння основних характеристик алгоритмів «Калина» та AES. Поняття криптографічної стійкості національних стандартів шифрування. Практичні аспекти використання національних криптографічних алгоритмів для захисту цифрової інформації.

Тема 15. Режими роботи блокових шифрів та практичне застосування криптографії

Поняття режиму роботи блокового шифру та його роль у забезпеченні криптографічного захисту інформації. Необхідність використання спеціальних режимів для шифрування повідомлень, довжина яких перевищує розмір одного блока. Класифікація режимів роботи блокових криптографічних алгоритмів. Режим електронної кодової книги ECB (Electronic Codebook):

принцип функціонування, особливості реалізації та обмеження безпеки. Режим зчеплення блоків шифротексту CBC (Cipher Block Chaining): алгоритм шифрування й розшифрування, використання вектора ініціалізації. Режим зворотного зв'язку за шифротекстом CFB (Cipher Feedback) та особливості його функціонування. Режим зворотного зв'язку за виходом OFB (Output Feedback): принципи формування ключового потоку. Режим лічильника CTR (Counter): особливості генерації послідовності блоків і виконання криптографічних перетворень. Порівняльна характеристика режимів ECB, CBC, CFB, OFB та CTR за принципами роботи, продуктивністю й вимогами до безпечного використання. Поняття автентифікованого шифрування та загальна характеристика режиму GCM (Galois/Counter Mode). Забезпечення конфіденційності, цілісності й автентичності інформації під час використання криптографічних алгоритмів. Особливості застосування симетричного шифрування для захисту файлів, електронних документів і даних у цифрових комунікаціях. Практичне використання програмних засобів криптографічного захисту інформації. Вибір алгоритмів і режимів шифрування відповідно до вимог безпеки та особливостей інформаційних ресурсів.

9. Опис ІЗ/КПІЗ

Не передбачено навчальним планом.

10. Самостійна робота

Обсяг самостійної роботи за навчальним планом: 60 годин для денної форми та 108 годин для заочної форми.

Теми	Види самостійної роботи	Денна, год	Заочна, год	Форма звітності	Форма контролю
1–3	Опрацювання конспекту й термінології з інформаційної безпеки та криптології. Розв’язання задач із модульної арифметики та бітових операцій.	12	18	Короткий конспект і письмові розв’язання задач.	Перевірка розв’язань, усне або письмове опитування.
4–7	Шифрування й розшифрування навчальних повідомлень класичними шифрами, частотний аналіз і порівняння стійкості шифрів. Підготовка до МКР №1.	16	32	Таблиці перетворень, код або розрахунки, короткий висновок.	Перевірка завдань і пояснення результатів, МКР №1.
8–10	Дослідження властивостей псевдовипадкових послідовностей і порівняння потокових шифрів RC4, ChaCha20 та «Струмок».	12	18	Звіт із тестовими даними, результатами та висновком.	Перевірка звіту, демонстрація й пояснення результатів.
11–15	Порівняння блокових шифрів і режимів шифрування, виконання вправ із вибору алгоритму й режиму для заданого сценарію. Підготовка до МКР №2 та екзамену.	20	40	Порівняльна таблиця, результати вправ і обґрунтування вибору.	Перевірка завдань, тестування та МКР №2.
Разом		**60**	**108**		

Результати самостійної роботи враховуються під час поточного й модульного контролю

відповідно до розділу «Критерії та форми контролю».

11. 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.

12. Література

I. Навчально-методичні матеріали та розробки

Праці автора силабуса:

1. Комп’ютерна безпека та криптографія : конспект лекцій для здобувачів першого (бакалаврського) рівня освіти освітньої програми «Середня освіта (Інформатика)» / уклад. Ю. Є. Мельничук. Луцьк : ЛНТУ, 2024. 52 с. URL: https://lib.lntu.edu.ua/uk/147258369/15003

2. Комп’ютерна безпека та криптографія : методичні вказівки до виконання лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти / уклад. Ю. Є. Мельничук. Луцьк : ЛНТУ, 2024. 36 с. URL: https://lib.lntu.edu.ua/uk/147258369/15004

Праці інших авторів:

3. Щур Н. О., Покотило О. А. Прикладна криптологія. Симетричні криптографічні системи : навчальний посібник. Житомир : Державний університет «Житомирська політехніка», 2026. 216 с.

4. Яремчук Ю. Є., Салієва О. В., Бондаренко І. О. Основи криптографічного захисту інформації : навчальний посібник. Вінниця : ВНТУ, 2024. 139 с.

5. Самойлов І. В., Матійко А. А., Сторчак А. С. Криптографія : навчальний посібник. Київ : КПІ ім. Ігоря Сікорського, 2023. 372 с.

II. Наукові праці

Праці автора силабуса:

6. Nadolska V., Melnychuk Y. Information security in higher education institutions of Ukraine: analysis of risks and management strategies. Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate. 2026. Vol. 16, No. 1. P. 65–75. DOI: https://doi.org/10.24917/26578549.16.1.4.

Праці інших авторів:

7. Dimitrova D. Evaluating the Effectiveness of Practical Exercises in Cryptography and Authentication Courses of Cybersecurity Education. Mathematics and Education in Mathematics. 2025. Vol. 54. P. 118–124. DOI: https://doi.org/10.55630/mem.2025.54.118-124.

8. Batra G., Zafar H., Dembla P. Teaching Tip: Decryption and Reverse Engineering – An Applied Tutorial for a Security Programming Course. Journal of Information Systems Education. 2025. Vol. 36, No. 2. P. 111–129. DOI: https://doi.org/10.62273/STWE8998.

9. Inoue A., Guo C., Minematsu K. Nonce-misuse Resilience of Romulus-N and GIFT-COFB. IET Information Security. 2023. Vol. 17, No. 3. P. 468–484. DOI: https://doi.org/10.1049/ise2.12110.

10. Rashidi B. High-Performance Hardware Structure of ChaCha20 Stream Cipher Based on Sparse Parallel Prefix Adder. International Journal of Circuit Theory and Applications. 2025. Vol. 53. P. 2947–2957. DOI: https://doi.org/10.1002/cta.4264.

11. Sriramulugari S. K., Gorantla V. A. K. Cyber Security Using Cryptographic Algorithms. International Journal of Computer Trends and Technology. 2024. Vol. 72, No. 1. P. 60–67. DOI: https://doi.org/10.14445/22312803/IJCTT-V72I1P110.

12. Parambil M. M. A., Rustamov J., Ahmed S. G., Rustamov Z., Awad A. I., Zaki N., Alnajjar F. Integrating AI-Based and Conventional Cybersecurity Measures into Online Higher Education Settings: Challenges, Opportunities, and Prospects. Computers and Education: Artificial Intelligence. 2024. Vol. 7. Article 100327. DOI: https://doi.org/10.1016/j.caeai.2024.100327.

III. Інформаційні ресурси

13. Електронна бібліотека Державного університету «Житомирська політехніка». URL: https://eztuir.ztu.edu.ua/

14. Інституційний репозитарій Вінницького національного технічного університету. URL: https://ir.lib.vntu.edu.ua/

15. Електронний архів наукових та освітніх матеріалів КПІ ім. Ігоря Сікорського. URL: https://ela.kpi.ua/

16. Національний інститут стандартів і технологій США (NIST). Ресурси з криптографічних стандартів та алгоритмів. URL: https://csrc.nist.gov/

17. Cryptography I — навчальні матеріали Стенфордського університету на платформі Coursera. URL: https://www.coursera.org/learn/crypto

18. CyberChef — онлайн-інструмент для дослідження кодування, шифрування, хешування та перетворення даних. URL: https://gchq.github.io/CyberChef/

19. CrypTool — освітні програмні засоби для вивчення криптографії та криптоаналізу. URL: https://www.cryptool.org/