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 «Алгоритми захисту інформації та системне програмування»
ступінь вищої освіти – бакалавр
галузь знань – F Інформаційні технології
спеціальність – F5 Кібербезпека та захист інформації
освітня програма – Кібербезпека

Кафедра кібербезпеки

Силабус склав(ла) доцент кафедри кібербезпеки, к.т.н., доцент Сергій ГРИНЮК

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/206

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Алгоритми захисту інформації та системне програмування»

Освітня програма	Кібербезпека
Галузь знань / Спеціальність	F Інформаційні технології / F5 Кібербезпека та захист інформації
Рівень вищої освіти	перший (бакалаврський)
Статус дисципліни	нормативна
Мова викладання	українська
Обсяг	6 кредитів ECTS / 180 годин, семестр 2
Форма контролю	екзамен
Викладач(і)	к.т.н., доцент Сергій ГРИНЮК електронна пошта: sgrunjuk@lutsk-ntu.com.ua

1. Мета і завдання дисципліни

Мета: формування у здобувачів вищої освіти системи базових теоретичних знань і практичних навичок щодо фундаментальних алгоритмів криптографічного захисту інформації та засад системного програмування, необхідних для розробки, аналізу й супроводу захищеного програмного забезпечення в галузі кібербезпеки.

Завдання: — ознайомити здобувачів з класифікацією та математичними основами базових криптографічних алгоритмів;
— сформувати практичні навички реалізації симетричних (DES, AES) та асиметричних (RSA, Діффі–Хеллман, Ель-Гамаль) алгоритмів шифрування, геш-функцій та електронного цифрового підпису;
— сформувати розуміння архітектури операційних систем та принципів взаємодії прикладних програм з ядром ОС;
— навчити розробляти багатопроцесні та багатопотокові застосунки з коректною синхронізацією;
— сформувати навички безпечного програмування та аналізу типових вразливостей системного рівня;
— навчити застосовувати криптографічні бібліотеки для побудови захищених програмних рішень.

Пререквізити: Програмування та реверс-інжиніринг, Дискретна математика

2. Компетентності

ІК — інтегральна компетентність: Здатність розв’язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.

ЗК06 — Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні.

СК02 — Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

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. Базові алгоритми захисту інформації								

№	Назва теми	Лекції денна/ заочна	Лаб. денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
1	Тема 1. Вступ до дисципліни. Загрози інформаційній безпеці та моделі порушника	2/0,5	2/0,75	7/10	11/11,25	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	ЗК06, СК02
2	Тема 2. Класифікація методів і алгоритмів захисту інформації. Основні поняття криптографії	2/0,25	2/0,75	7/10	11/11	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
3	Тема 3. Симетричні блокові шифри. Алгоритми DES і 3DES	2/0,25	2/0,5	7/10	11/10,75	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
4	Тема 4. Стандарт симетричного шифрування AES (Rijndael)	2/0,25	2/0,5	7/10	11/10,75	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
5	Тема 5. Математичні основи асиметричної криптографії. Алгоритм RSA	2/0,25	2/0,5	7/10	11/10,75	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
6	Тема 6. Протокол Діффі–Хеллмана та алгоритм Ель-Гамаля	2/0,25	2/0,5	7/10	11/10,75	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
7	Тема 7. Криптографічні геш-функції. Коди автентифікації повідомлень	2/0,25	2/0,5	7/10	11/10,75	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
8	Тема 8. Електронний цифровий підпис. Інфраструктура відкритих ключів	2/0,25	2/0,5	7/9,75	11/10,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
Змістовий модуль 2. Основи системного програмування								

№	Назва теми	**Лекції** денна/ заочна	**Лаб.** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**ЗК та СК**
9	Тема 9. Основи системного програмування. Системні виклики та інтерфейс ядра ОС	2/0,25	2/0,5	7/9,75	11/10,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
10	Тема 10. Управління процесами та міжпроцесна взаємодія	2/0,25	2/0,5	7/9,75	11/10,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
11	Тема 11. Багатопотокове програмування та синхронізація	2/0,25	2/0,5	6/9,75	10/10,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
12	Тема 12. Управління пам'яттю в системному програмуванні	2/0,25	2/0,5	6/9,75	10/10,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
13	Тема 13. Захищене системне програмування	2/0,25	2/0,5	6/9,75	10/10,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
14	Тема 14. Криптографічні бібліотеки в системному програмному забезпеченні	2/0,25	2/0,5	6/9,75	10/10,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
15	Тема 15. Комплексна розробка захищеного програмного забезпечення	2/0,25	2/0,5	6/9,75	10/10,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
	ІЗ/КПІЗ			20/20	20/20			
	Разом	**30/4**	**30/8**	**120/168**	**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); 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).

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

4. Результати навчання

ПРН04. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв’язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

ПРН07. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

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 (30 %) + ІЗ/КПІЗ (10 %) + 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. Вступ до дисципліни. Загрози інформаційній безпеці та моделі порушника

Предмет, мета і завдання дисципліни, її зв'язок з іншими дисциплінами ОП. Основні поняття інформаційної безпеки: конфіденційність, цілісність, доступність, автентичність, неспростовність. Класифікація загроз інформаційній безпеці та каналів витоку інформації. Модель порушника: внутрішній і зовнішній порушник, його можливості й мотивація. Поняття атаки, вразливості, ризику. Місце алгоритмів захисту інформації та системного програмування в забезпеченні кібербезпеки.

Тема 2. Класифікація методів і алгоритмів захисту інформації. Основні поняття криптографії

Організаційні, технічні, програмні та криптографічні методи захисту інформації. Основні поняття криптографії: відкритий текст, шифротекст, шифр, ключ, криптостійкість. Принцип Керкгоффса. Класифікація криптосистем: симетричні й асиметричні, блокові й потокові. Класичні шифри заміни (Цезаря, Віженера) і перестановки. Основи криптоаналізу класичних шифрів: частотний аналіз, атака повним перебором.

Тема 3. Симетричні блокові шифри. Алгоритми DES і 3DES

Принципи побудови блокових шифрів: розсіювання та перемішування за Шенноном. Мережа Фейстеля та SP-мережа. Алгоритм DES: структура раунду, функція F, S-блоки, генерація підключів. Слабкості DES і причини переходу до 3DES. Режими роботи блокових шифрів: ECB, CBC, CFB, OFB.

Тема 4. Стандарт симетричного шифрування AES (Rijndael)

Історія конкурсу AES та стандарт NIST FIPS 197. Математичні основи: арифметика в полі Галуа GF(2^8). Структура раунду AES: SubBytes, ShiftRows, MixColumns, AddRoundKey. Розширення ключа, кількість раундів залежно від довжини ключа. Порівняння режимів шифрування ECB,

CBC, CTR, GCM: властивості, переваги, сфери застосування. Автентифіковане шифрування.

Тема 5. Математичні основи асиметричної криптографії. Алгоритм RSA

Концепція криптографії з відкритим ключем, односторонні функції та функції з «лазівкою». Модульна арифметика: конгруенції, найбільший спільний дільник, розширений алгоритм Евкліда, обернений елемент за модулем. Функція Ейлера, мала теорема Ферма. Задачі факторизації та дискретного логарифмування. Генерація простих чисел, тести простоти. Алгоритм RSA: генерація ключів, шифрування та розшифрування, вимоги до параметрів, відомі атаки.

Тема 6. Протокол Діффі–Хеллмана та алгоритм Ель-Гамаля

Задача узгодження ключів у відкритому каналі. Протокол Діффі–Хеллмана: принцип роботи, вибір параметрів, атака «людина посередині». Криптосистема Ель-Гамаля: генерація ключів, шифрування, розшифрування. Порівняння симетричних і асиметричних систем шифрування за стійкістю, швидкодією, довжиною ключів. Гібридні криптосистеми.

Тема 7. Криптографічні геш-функції. Коди автентифікації повідомлень

Поняття та призначення геш-функції. Вимоги до криптографічних геш-функцій: стійкість до знаходження прообразу, другого прообразу та колізій. Парадокс днів народження. Конструкція Меркла–Дамгора. Алгоритми MD5, SHA-1, SHA-2, SHA-3 (Keccak, губчаста конструкція). Застосування для контролю цілісності даних і зберігання паролів. Коди автентифікації повідомлень, алгоритм HMAC.

Тема 8. Електронний цифровий підпис. Інфраструктура відкритих ключів

Призначення та властивості електронного цифрового підпису. Загальна схема формування й перевірки підпису з використанням геш-функції. Підпис на основі RSA, алгоритм DSA (стандарт FIPS 186). Інфраструктура відкритих ключів (PKI): центри сертифікації, ланцюги довіри, відкликання сертифікатів (CRL, OCSP). Структура сертифіката X.509.

Тема 9. Основи системного програмування. Системні виклики та інтерфейс ядра ОС

Поняття системного програмування. Архітектура обчислювальної системи, рівні абстракції, роль операційної системи. Режим ядра і режим користувача. Мова C як інструмент системного програмування: вказівники, робота з пам'яттю, процес компіляції та компонування. Системні виклики та стандарт POSIX API. Робота з файлами через файлові дескриптори. Обробка помилок (errno). Сигнали та їх обробка.

Тема 10. Управління процесами та міжпроцесна взаємодія

Поняття процесу, його атрибути та дескриптор. Життєвий цикл процесу, стани процесу. Створення процесів (fork), заміна образу процесу (exec), очікування завершення (wait, waitpid). Процеси-зомбі та процеси-сироти. Механізми міжпроцесної взаємодії: канали (pipe, FIFO), черги повідомлень, розділювана пам'ять. Безпекові аспекти взаємодії процесів.

Тема 11. Багатопотокове програмування та синхронізація

Потоки виконання та їхні відмінності від процесів. Бібліотека POSIX Threads (pthreads): створення, завершення, приєднання потоків. Проблеми конкурентного доступу: стан гонитви, критична секція. Засоби синхронізації: м'ютекси, семафори, умовні змінні. Взаємне блокування (deadlock) і методи запобігання йому. Класичні задачі синхронізації, зокрема «виробник–споживач».

Тема 12. Управління пам'яттю в системному програмуванні

Адресний простір процесу: сегменти коду, даних, купи та стека. Віртуальна пам'ять, сторінкова організація, таблиці сторінок. Відображення файлів у пам'ять (mmap). Динамічний розподіл пам'яті (malloc, free) та принципи роботи менеджера пам'яті. Типові помилки роботи з пам'яттю: витоки, подвійне звільнення, звернення до звільненої пам'яті. Засоби діагностики (Valgrind).

Тема 13. Захищене системне програмування

Класифікація вразливостей системного програмного забезпечення: переповнення буфера в стеку та купі, race condition (TOCTOU), use-after-free, вразливості форматного рядка, цілочисельне

переповнення. Принципи експлуатації вразливостей. Механізми захисту від експлойтів: ASLR, DEP/NX, стек-канарки. Правила безпечного кодування мовою C (стандарт SEI CERT C), безпечні аналоги небезпечних функцій.

Тема 14. Криптографічні бібліотеки в системному програмному забезпеченні

Огляд криптографічних бібліотек: OpenSSL, libsodium. Архітектура та основні інтерфейси OpenSSL (EVP API). Програмна реалізація симетричного та асиметричного шифрування, гешування й цифрового підпису засобами бібліотек. Протоколи SSL/TLS: етапи встановлення з'єднання (handshake), набори шифрів. Побудова захищеного з'єднання «клієнт–сервер». Типові помилки використання криптографічних бібліотек.

Тема 15. Комплексна розробка захищеного програмного забезпечення

Інтеграція криптографічних алгоритмів і механізмів системного програмування в межах одного застосунку. Архітектура захищеного застосунку: криптографічний модуль, керування ключами, безпечна робота з пам'яттю та процесами. Принципи безпечної розробки ПЗ (Secure SDLC). Тестування та аудит захищеності програмного коду. Узагальнення та систематизація матеріалу курсу.

9. Опис ІЗ/КПІЗ

Індивідуальні завдання з дисципліни «Алгоритми захисту інформації та системне програмування» виконується самостійно кожним студентом. КПІЗ охоплює усі основні теми дисципліни «Алгоритми захисту інформації та системне програмування».

Метою виконання КПІЗ є оволодіння навичками застосування теоретичних знань. КПІЗ оформлюється у відповідності з встановленими вимогами. Виконання КПІЗ є одним із обов'язкових складових модулів залікового кредиту з дисципліни «Алгоритми захисту інформації та системне програмування».

Індивідуальне завдання оцінюється за 100-бальною шкалою. Виконання індивідуального завдання є одним із обов'язкових складових модулів залікового кредиту з дисципліни «Алгоритми захисту інформації та системне програмування».

Тематика	Обсяг	Вимоги до виконання та захисту
Розробка захищеного застосунку, що поєднує криптографічний алгоритм і механізм системного програмування (конкретна пара — за варіантом із 30 можливих: DES/AES/RSA/Діффі–Хеллмана/Ель-Гамаля/SHA-256+HMAC у поєднанні з IPC, потоками, сокетами чи OpenSSL/TLS)	Вихідний код застосунку, де криптомодуль і системний модуль взаємодіють між собою (наприклад, дані шифруються перед передачею через канал/чергу/сокет); звіт обсягом до 15 сторінок з описом алгоритму, архітектури застосунку та результатів тестування	Криптоалгоритм реалізується самостійно (без готової функції саме цього алгоритму з бібліотеки, крім варіантів на основі TLS); системний механізм — через виклики POSIX API без сторонніх high-level обгорток; коректна обробка помилок системних викликів, відсутність витоку ресурсів (дескриптори, пам'ять, IPC-об'єкти); варіант із переповненням буфера — лише у віртуальній машині. Захист: демонстрація повного циклу роботи обох компонентів разом, пояснення забезпеченої властивості захисту інформації (конфіденційність/цілісність/автентичність) та обґрунтування вибору системного механізму

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 автора силабуса:

1. Пех П. А., Чернящук Н. Л., Гринюк С.В. та ін. Методи обчислень та моделювання. Лабораторний практикум: навч. посіб для студ. тех. спец. закл. вищ. освіти I-IV рівн. акредит. Луцьк: Вежа-Друк, 2023. 168 с. URL: https://repository.lntu.edu.ua/handle/123456789/3677.

Праці інших авторів:

2. Кібербезпека: основи кодування та криптографії / С. П. Євсеєв, О. В. Мілов, С. Е. Остапов, О. В. Сєвєрінов. Харків : Новий Світ-2000, 2023. 657 с.

3. Ковтун В. Ю., Євсеєв С. П., Аксьонова І. В. Кібербезпека та новітні технології захисту інформації : навч. посіб. Харків : НТУ «ХПІ» ; Львів : Новий Світ-2000, 2024. 285 с.

4. Операційні системи. Управління процесами : навч. посіб. / В. І. Панченко, Г. В. Гейко, М. І. Главчев, В. В. Скородєлов. Харків : НТУ «ХПІ», 2025. 350 с.

5. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації : навч. посіб. 2-ге вид., стер. Львів : Новий Світ-2000, 2024. 678 с.

II. Наукові праці

Праці автора силабуса:

6. 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. URL: https://repository.lntu.edu.ua/handle/123456789/2012

7. 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. URL: https://repository.lntu.edu.ua/handle/123456789/4596

8. Римчук І., Костючко С., Поліщук М., Гринюк С., Конкевич Л. Безпека комунікаційних процесів з використанням візуальної криптографії. Кібербезпека: освіта, наука, техніка. 2024. № 2(26). С. 258–267. URL: https://repository.lntu.edu.ua/handle/123456789/4595

9. Гринюк С. В., Поліщук М. М., Гринюк М. В., Шульгат В. В., Терешкович В. І. Інтелектуальна система керування освітленням на базі Arduino Uno. Комп’ютерно-інтегровані технології: освіта, наука, виробництво. Луцьк: ЛНТУ. 2023. Вип. 53. С. 98-103. URL: https://repository.lntu.edu.ua/handle/123456789/4592

III. Інформаційні ресурси

10. OpenSSL Documentation. URL: https://docs.openssl.org/ (дата звернення: 13.10.2026).

11. The Linux man-pages project. URL: https://man7.org/linux/man-pages/ (дата звернення: 13.10.2026).