

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра програмних систем і технологій

«ЗАТВЕРДЖУЮ»

Заступник декана

з навчально-виховної роботи

Наталія ТМЄНОВА

« 29 » серпня 2026 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«КРИПТОПРОГРАМУВАННЯ»

для здобувачів вищої освіти

галузь знань	І Інформаційні технології
спеціальність	І2 Інженерія програмного забезпечення
освітній рівень	бакалавр
освітня	Інженерія програмного забезпечення
програма	
вид дисципліни	вибіркова

Форма навчання	денна
Навчальний рік	2026/2027
Семестр	4
Кількість кредитів ECTS	5
Мова викладання, навчання та оцінювання	українська
Форма заключного контролю	іспит

Викладачі: *Курченко О.А., кандидат технічних наук, доцент*

Пролонговано: на 2027/2028 н.р. _____ (_____) «__» _____ 2027 р.

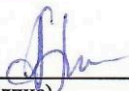
на 2028/2029 н.р. _____ (_____) «__» _____ 2028 р.

на 2029/2030 н.р. _____ (_____) «__» _____ 2029 р.

КИЇВ – 2026

Розробник: Курченко О.А., кандидат технічних наук, доцент, доцент кафедри програмних систем і технологій

Завідувач кафедри
програмних систем і технологій

 проф. Олексій БИЧКОВ
(підпис)

Протокол № 18 від 17 червня 2026 року

Схвалено науково-методичною комісією факультету інформаційних технологій

Протокол № 11 від 26 червня 2026 року

Голова науково-методичної комісії  Ганна КРАСОВСЬКА
(підпис)

© Курченко О. А. _____, 2026 рік
© _____, 20__ рік
© _____, 20__ рік

ВСТУП

1. Мета дисципліни - вивчення студентами методологічних та методичних питань щодо дослідження проєктування, безпечної реалізації та інтеграції криптографічних алгоритмів і протоколів у сучасне програмне забезпечення.

2. Попередні вимоги до опанування або вибору навчальної дисципліни:

1. Знати базові поняття інженерії програмного забезпечення і обчислювальної техніки.
2. Вміти аналізувати та обирати оптимальний метод розв'язання задач обчислювального та інформаційного характеру, користуватись послугами локальних комп'ютерних мереж, глобальної мережі Інтернет для пошуку, отримання, аналізу і пересилання необхідної інформації.
3. Володіти навичками алгоритмізації та програмування на будь-якій мові високого рівня.

3. Анотація навчальної дисципліни:

Навчальна дисципліна «Криптопрограмування» є вибірковою дисципліною підготовки фахівців за освітньо-кваліфікаційним рівнем «бакалавр» галузі знань F Інформаційні технології зі спеціальності F2 Інженерія програмного забезпечення, за освітньою програмою «Інженерія програмного забезпечення». Навчальна дисципліна формує інженерно-науковий світогляд фахівця в області ІТ.

4. Завдання вивчення дисципліни є опанування понятійним апаратом дисципліни, основних теоретичних положень і методів, формування вмінь і напрацювання навичок застосування теоретичних знань для розв'язання практичних і прикладних задач. У результаті вивчення навчальної дисципліни студент повинен знати архітектуру криптографічних бібліотек та API; опанувати програмування симетричних та асиметричних методів шифрування; навчитися уникати типових вразливостей при реалізації криптоалгоритмів у коді. Забезпечити СК15.3 що пов'язане з результатами ПР26.3 освітньої програми «Інженерія програмного забезпечення» за спеціальністю F2 «Інженерія програмного забезпечення».

5. Результати навчання за дисципліною:

Код	Результат навчання (1. знати; 2. вміти; 3. комунікація)	Форми (та / або методи і технології) викладання і навчання	Методи оцінювання та пороговий критерій оцінювання ¹	Відсоток у підсумковій оцінці з дисципліни
1.1	Знати сучасні методи захисту програмного забезпечення	лекції за інноваційною інформаційною методикою викладання «перевернутий клас»	тести, модульні контрольні роботи, 60 % правильних відповідей	до 60%
1.2	Модель SSDLC			
1.3	Вимоги безпеки для програмного забезпечення			
1.4	Методи та засоби обмеження доступу до програмного забезпечення			
1.5	Класифікацію вразливостей програмного забезпечення			
1.6	Особливості вразливостей у програмному забезпеченні			
1.7	Особливості конфігурування систем безпеки			

2.1	Вміти аналізувати та досліджувати вразливості програмного забезпечення за допомогою сучасних програмних засобів	лабораторні роботи	звіти по лабораторних роботах, залік	до 30%
2.2	Розробляти захищене програмне забезпечення відповідно до моделі SSDLC			
2.3	Виконувати адміністрування прав доступу до комп'ютерної системи з метою перешкоди призначення невинуватених привілеїв			
2.4	Виконувати постійний моніторинг з пошуку програмних закладок та каналів витоку інформації			
2.5	Використовувати основні прийоми та програмні засоби хакерів для перевірки надійності захисту інформації та стійкості його щодо хакерських атак			
2.6	Забезпечувати обґрунтований підбір програмно-апаратних та програмних засобів для забезпечення необхідного рівня захисту інформації	самостійна робота	звіти по лабораторних роботах, кейс-задачі	до 10%
3.1	Комунікація: здатність працювати в команді, вироблення у студентів практичних навиків проведення дослідження і оптимального групового вирішення актуальних проблем із застосуванням відповідних методів і прийомів.			

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання

Результати навчання дисципліни	1.1	1.2	1.3	1.4	1.5	1.6	1.7	2.1	2.2	2.3	2.4	2.5	2.6	3.1
Програмні результати навчання														
ПР-26.3 Знати, розуміти, вміти застосовувати засоби та методи розробки захищеного програмного забезпечення, вміти застосовувати методи криптографії, криптології, криптоаналізу для написання захищених програм, вміти застосовувати моделі захисту відповідно до вимог сучасних стандартів кібербезпеки та критеріїв безпеки захищених програм.	+	+	+	+	+	+	+	+	+	+	+	+	+	+

7. Схема формування оцінки:

7.1. Форми оцінювання студентів: рівень досягнення всіх запланованих результатів навчання визначається за результатами написання письмових контрольних робіт.

Питома вага результатів навчання у підсумковій оцінці за умови її опанування на належному рівні така:

Результати навчання – **1 (знання)** – до 60%;

Результати навчання – **2 (вміння)** – до 30%;

Результати навчання – **3 (комунікація)** – до 10%;

7.2. Організація оцінювання

Контроль знань студентів здійснюється за модульно-рейтинговою системою. Результати навчальної діяльності студентів оцінюються за 100-бальною шкалою. Робота в

семестрі поділяється на два змістових модуля. Підсумковий контроль (екзамен) проводиться у формі письмової роботи – 40 балів.

У змістовий модуль 1 (ЗМ1) входять теми 1-6, а у змістовий модуль 2 (ЗМ2) – теми 7-12. Обов'язковим для іспиту є виконання та захист студентом індивідуальних лабораторних робіт, передбачених робочою програмою навчальної дисципліни, здача двох модульних контрольних робіт. При цьому сумарна мінімальна кількість балів – 18.

Оцінювання за формами контролю:

	Змістовий модуль 1	Змістовий модуль 2	Екзамен	Підсумкова оцінка
<i>Мінімум</i>	18	18	24	60
Максимум	30	30	40	100

Поточне семестрове оцінювання:

- оцінюванню підлягають дві модульні контрольні роботи, звіти та захист індивідуальних лабораторних робіт;

- упродовж семестру, після завершення лекційного матеріалу по змістовним модулям 1 та 2 (теми 1-6 та 7-12), орієнтовно на 3 та на 6 тижнях навчання при умові здачі звітів та захисту індивідуальних лабораторних робіт, відповідно, проводиться письмова модульна контрольна робота № 1 та № 2 із відкритими питаннями.

У випадку відсутності студента з поважних причин відпрацювання та перездачі МКР здійснюються у відповідності до «Положення про порядок оцінювання знань студентів при кредитномодульній системі організації навчального процесу» від 1 жовтня 2010 року. Перескладення індивідуальної чи модульної контрольної роботи з метою підвищення оцінки не допускається.

Для студентів, які набрали сумарно меншу кількість балів ніж критично-розрахунковий мінімум (36 балів), для одержання іспиту обов'язковими є перездача модульних контрольних робіт, виконання та захист запланованих індивідуальних самостійних робіт.

Для студентів які упродовж семестру не досягли мінімального рубіжного рівня оцінки (60% від максимально можливої кількості балів, тобто 36 балів) проводиться заключна семестрова комплексна контрольна робота, максимальна оцінка за яку не може перевищувати 40% підсумкової оцінки (до 40 балів за стобальною шкалою).

Підсумкове оцінювання (у формі екзамену):

- екзаменаційний білет складається з двох частин: теоретична частина (3 завдання) та практична (2 завдання), які оцінюються 24 та 16 балів відповідно;

- максимальна кількість балів які можуть бути отримані студентом 40 балів на екзамені по 100-бальній шкалі;

- студент не допускається до екзамену, якщо під час семестру набрав менше ніж 36 балів;

- для отримання загальної позитивної оцінки з дисципліни оцінка за екзамен не може бути меншою 24 балів.

7.3. Шкала відповідності оцінок

Відмінно / Excellent	90-100
Добре / Good	75-89
Задовільно / Satisfactory	60-74
Незадовільно / Fail	0-59

Оцінювання проводиться відповідно до «Рекомендацій щодо оцінювання освітніх STEM-проектів», затверджених на засіданні кафедри програмних систем і технологій

8. Структура навчальної дисципліни. Тематичний план лекцій і лабораторних занять

№ п/п	Назва теми	Кількість годин		
		Лекції	Лабораторні заняття	СР
Змістовий модуль 1.				
1	Тема 1. Вступ до криптопрограмування. Огляд інструментарію (OpenSSL, Libsodium, PyCryptodome, Web Crypto API).	2	4	6
2	Тема 2. Програмна генерація випадкових чисел. Криптографічно стійкі генератори псевдовипадкових чисел (CSPRNG).	4	4	8
3	Тема 3. Практична реалізація та використання хеш-функцій (SHA-2, SHA-3, BLAKE3). Керування паролями (Argon2, bcrypt, scrypt).	4	4	8
4	Тема 4. Програмування симетричного шифрування. Режими блочного шифрування (AES-GCM, AES-CBC, ChaCha20-Poly1305). Автентифіковане шифрування (AEAD).	4	4	8
5	Модульна контрольна робота 1		2	4
Змістовий модуль 2.				
6	Тема 5. Реалізація асиметричних алгоритмів. Керування ключами RSA та криптографія на еліптичних кривих (ECC: Ed25519, Secp256k1).	4	4	8
7	Тема 6. Програмування електронного цифрового підпису (ECDSA, EdDSA) та протоколів обміну ключами (Diffie-Hellman, ECDH).	4	4	8
8	Тема 7. Розробка безпечних мережеских з'єднань. Конфігурування TLS/SSL на рівні коду додатків.	4	4	8
9	Тема 8. Типові помилки криптопрограмування (Side-channel атаки, атаки за часом, повторне використання ініціалізаційних векторів IV) та методи їх запобігання.	4	4	8
10	Тема 9. Перспективи: Вступ до постквантового криптопрограмування (алгоритми CRYSTALS-Kyber, CRYSTALS-Dilithium).	4	4	6
11	Модульна контрольна робота 2		2	4
	ВСЬОГО	34	40	76

Загальний обсяг 150 год., в тому числі:

лекцій – 34 год.;
 лабораторні заняття – 40 год.;
 самостійна робота – 76 год.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА:

Основи:

1. Кузнецов О. О. Захист інформації в інформаційних системах : навч. посіб. Х. : ХНЕУ, 2015. – 510 с.
2. Microsoft Security Development Lifecycle (SDL) – Process Guidance
<https://msdn.microsoft.com/en-us/library/windows/desktop/84aed186-1d75-4366-8e61-d258746bopq.aspx>

3. OWASP Foundation. OWASP Testing Guide v4.0. URL: https://www.owasp.org/index.php/Web_Application_Penetration_Testing.
4. Heiderich M., Nava E., Heyes G., Lindsay D. Web Application Obfuscation. –ISBN-10: 1597496049.
5. McNab C. Network Security Assessment : Know Your Network, second edition. – ISBN-10:0-596- 51030-6.
6. Ristic I. Bulletproof SSL and TLS: Understanding and deploying SSL/TLS and PKI to secure servers and web applications. – ISBN10: 1907117040.
7. Stuttard D., Pinto M. The Web Applicaion Hackers’s Handbook: Finding and Exploiting Security Flaws. – ISBN-10: 1118026470.

Додаткова:

1. Zalewski M. The Tangled Web: A Guide to Securing Modern Web Applications. – ISBN-10: 1593273886.
2. HTML5 Security Cheatsheet. URL: <https://html5sec.org/>10. Закон України “Про захист інформації в автоматизованих системах” від 05.07.1994.
3. Schneier B. and Whiting D. Fast software encryption: Designing encryption algorithms for optimal software speed on the Intel Pentium processor // Fast Software Encryption: 4th International Workshop. Lecture Notes in Computer Science, Vol 1267. – Springer-Verlag: 1997. – P. 242 – 259.
4. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 – 368 с.

Додаткові ресурси:

1. <https://starlight.media/korysnosti/informacijna-bezpeka-resursi-dlja-zahistu-osobistih-danih>