МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС
вибіркового освітнього компонента

КРИПТОГРАФІЯ ТА СТЕГАНОГРАФІЯ МОВОЮ PYTHON

підготовки бакалавра

Луцьк – 2026

Силабус навчальної дисципліни «Криптографія та стеганографія мовою Python**»** підготовки бакалавра.

Розробник: Головін Микола Борисович, кандидат фізико-математичних наук, доцент кафедри комп'ютерних наук та кібербезпеки

Погоджено
Гарант освітньо-професійної програми:  Наталія ЧЕРНЯЩУК

Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

Протокол 6 від 15.01.2026 р.

Завідувач кафедри:  Тетяна ГРИШАНОВИЧ

І. Опис освітнього компонента

Найменування показників	Характеристика освітнього компонента
	Вибірковий
Денна форма навчання	Рік підготовки 3
150/5 кредитів	Семестр 6
	Лекції 10 год.
	Лабораторні 20 год.
	Самостійна робота 110 год.
ІНДЗ: немає	Консультації 10 год.
	Форма контролю: залік

ІІ. Інформація про викладача (- ів)

Викладач	Головін Микола Борисович
Науковий ступінь	Кандидат фізико-математичних наук
Вчене звання	Доцент
Посада	Доцент кафедри комп'ютерних наук та кібербезпеки
Телефон	+380634575757
e-mail	Golovin_Mykola@vnu.edu.ua
Дні занять	https://ps.vnu.edu.ua/cgi-bin/timetable.cgi

ІІІ. Опис освітнього компонента

1. Анотація курсу

Силабус навчальної дисципліни «Криптографія та стеганографія мовою Python» складено з урахуванням можливості формування індивідуальної освітньої траєкторії здобувачів освіти рівня бакалавр.

2. Мета та завдання освітнього компонента

Метою викладання навчальної дисципліни «Криптографія та стеганографія мовою Python» є ознайомлення з основами криптографії і стеганографії, а також практична реалізація мовою Python програм сучасних шифраторів, дешифраторів та програм приховування інформації в медійних файлах.

Очікувані результати

Знання:

- технологій шифрування та дешифрування інформації;
- приховування інформації в медійних файлах та вилучення її звідти ;
- методів криптоаналізу повідомлень та зламу простих шифрів;
- мови Python.

Вміння :

- мовними засобами Python реалізовувати шифратори, дешифратори;

- мовними засобами Python реалізовувати різноманітні способи стеганографічного приховування інформації в графічних та звукових файлах на практиці;
- мовними засобами Python реалізовувати програми криптоаналізу простих шифрів;
- аналізувати медіа файли на предмет приховування в них інформації.

3.Soft skills

- Формування складно організованого причинно - наслідкового мислення впродовж написання, випробовування та відлагодження програм криптографічного та стеганографічного гатунку.
- Формування витонченого абстрактно логічного мислення впродовж багатократних індуктивно-дедуктивних дій, що супроводжують перезавантаження свідомості в процесі програмування.
- Формування строгого критичного мислення на основі, взаємозв'язку власних практичних, матеріалізованих, алгоритмічно-структурованих дій в складному інформаційному середовищі і тих наслідків до яких ці складно організовані дії можуть призвести.
- Формування основних патернів професійного мислення програмістів, що базуються на структурному, функціональному, об'єкно орієнтованому та подіє-орієнтованому програмуванні.

4. Структура освітнього компонента.

Назви змістових модулів і тем	Усього	Лек.	Лабор.	Сам.	Конс.	Бали
Змістовий модуль 1. Концепції криптографії та шифри з закритим ключем						
Тема 1. Симетричні та асиметричні криптосистеми. Кодування текстової та числової інформації. ASCII.	15	1	2	11	1	Л/5 Т/4
Тема 2. Реалізації простих симетричних шифрів мовою Python: зміщенням коду, перестановкою, підстановокою. Книжний шифр. Шифр Виженера. Інші.	15	1	2	11	1	Л/5 Т/4
Тема 3. Реалізація моделі механічного шифратору Джеферсона. Комп'ютерна модель електромеханічної шифрувальної машини «Енігма».	15	1	2	11	1	Л/5 Т/4
Тема 4. Програмні реалізацій зламу шифрів на базі частотного анализу, зокрема, шифрів Цезаря, Виженера. Комп'ютерна модель електромеханічної машини «Бомба», що зламала шифр «Енігма»	15	1	2	11	1	Л/5 Т/4
Тема 5. Приклад програмної реалізації сучасного шифратора AES (Advanced Encryption Standard).	15	1	2	11	1	Л/5 Т/4
Усього годин за перший модуль	75	5	10	55	5	45
Змістовий модуль 2. Криптосистеми із відкритим ключем та стеганографія						
Тема 6. Концепції асиметричного шифрування. Програмна реалізація розрахунку обміну ключами Діффі-Хеллмана (Python)	15	1	2	11	1	Л/5 Т/4
Тема 7. Алгоритм RSA. Реалізація алгоритму RSA для малих значень на мові Python. Програмна реалізація шифрування з відкритим ключем	15	1	2	11	1	Л/5 Т/4
Тема 8. Алгоритм Ель-Гамаля. Програмна реалізація шифрування Ель-Гамаля	15	1	2	11	1	Л/5 Т/4

Тема 9. Технологія LSB (Least Significant Bit) приховування тексту в графічному файлі на основі зміни найменшого значущого біту пікселя, що відповідає за складову коліру. Програмна реалізація.	15	1	2	11	1	Л/5 Т/4
Тема 10. Технологія PVD (Pixel Value Difference), алгоритми, якої кодують біти секретного повідомлення як різницю між модифікованими значеннями пікселів графіки. Програмна реалізація.	15	1	2	11	1	Л/5 Т/4
Захисти проектів (ІНДЗ)						П/10
Усього годин за другий модуль	75	5	10	55	5	55
Усього годин за семестр	150	10	20	110	10	100

Примітка. Проекти захищаються по мірі їх створення на лабораторних роботах.
Позначення методів контролю*: Т- поточний тест, Л-виконана лабораторна, П-захист проекту5.
Завдання для самостійного опрацювання

Самостійна робота студента складається з кількох наступних напрямків.

1. Опрацювання лекційного матеріалу, що дублюється і розширюється матеріалами інформаційної частини відповідного дистанційного курсу на платформі MOODLE.
2. Самостійна підготовка до лабораторних занять полягає в виконанні тематичних тренажерних та тестових завдань на дистанційній платформі MOODLE. Кожна тема курсу має відповідну підтримку. Ці завдання забезпечують вивчення понятійного апарату по всіх темах та відтворення різноманітних схем.
3. Самостійне виконання (**ІНДЗ**) індивідуальних програмних проектів студентами. Тематика проектів безпосередньо пов'язана з відповідними темами курсу. В ході виконання цих проектів передбачається пошук та засвоєння додаткових матеріалів необхідних для реалізації проекту. Маються на увазі матеріали, які дотичні до основного курсу, однак не розглядаються в курсі лекцій.
4. Самостійне проходження інших, зовнішніх відповідних тематиці дисципліни дистанційних курсів, на кшталт, курсів з пакету Prometheus (https://prometheus.org.ua/) або SoloLearn (https://www.sololearn.com/). Відповідний сертифікат зараховується як **ІНДЗ.**

IV. Політика оцінювання

Політика викладача щодо здобувача освіти.

Підсумковий контроль успішності навчання формується **поточним контролем**. Оцінювання знань здійснюється із використанням **100** бальної шкали. **Поточний контроль успішності** реалізується за сукупністю балів, що набрані: в тестах, на лабораторних та за проект.

Таблиця Розподілу балів по формам контролю

Поточний контроль			Загальна кількість балів
Змістовий модуль 1	Змістовий модуль 2	ІНДЗ	
Тематичні тести та лабораторні		10 балів	100 балів
45 балів	45 балів		

Про тести поточного контролю. Інформація стосовно виконань тестових завдань поточного контролю знаходиться в журналі MOODLE курсу. Оцінка за виконаний тест лабораторного заняття вказує на ступінь ознайомлення студента з новим матеріалом відповідної теми. Використання інформаційної складової курсу під час виконання тестів поточного контролю допускається. Обмеження по часу виконання тематичного пакету завдань

відсутнє. Припустиме дистанційне виконання тестів. Після завершення вивчення теми можливість виконання тесту припиняються. Останнє має мотивувати студенів до систематичної роботи при дистанційному навчанні.

Лабораторні роботи забезпечують практичні навчальні дії в курсі, зокрема, з теоретичним матеріалом, програмним забезпеченням, що вивчається або створюється. Цінність цього пласту лабораторних тематичних завдань в підтримці практичної роботи студентів. Лабораторні дозволяють реалізувати перевірку складніших ніж в MOODLE завдань. Зокрема, в темі керування ходом проходження програми, можна перевірити засвоєння стандартних програмних конструкцій, які можуть включати кілька простих конструкцій, наприклад, вкладені одні в одні цикли, розгалуження, функції, рекурсії. Використання інформаційної складової курсу під час виконання завдань лабораторної на оцінку не допускається. Вважається, що на цьому етапі навчання студенти закріплюють новий матеріал теми і **вчаться застосовувати їх на практиці**.

Робота над проектами (**ІНДЗ**) та їх захист має в подальшому вивести студентів на рівень, коли вони зможуть **застосовувати отримані знання на практиці**. Можливості стосовно **застосування отриманих** знань на практиці оцінюються по проекту, який виконує студент. Проект вважається індивідуальним завданням (**ІНДЗ**). За проект в поточному оцінюванні студент може отримати максимум **10** балів. Ці 10 балів начисляються, як за змістовне наповнення проекту, так і за його очний захист в присутності групи. Захист передбачає: усну доповідь з використанням наочності, демонстрацію роботи програмних засобів створених впродовж виконання ІНДЗ. Бали нараховуються також за участь в дебатах по захисту проекту. Оцінюється, як запитання опонентів в дебатах, так і відповіді доповідача.

Альтернативним індивідуальним завданням (ІНДЗ), що оцінюється в **10** балів, є проходження зовнішніх відповідних тематиці дисципліни дистанційних курсів, на кшталт, курсу https://www.coursera.org/learn/crypto#syllabus або інших подібних (по домовленості з викладачем). Свідченням про завершення зовнішнього курсу є посилання в Інтернеті на відповідний сертифікат про успішне закінчення курсу.

Політика щодо академічної доброчесності.

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту (https://vnu.edu.ua/uk/statut-snu-imeni-lesi-ukrayinki) і Правил внутрішнього розпорядку ВНУ імені Лесі Українки (https://vnu.edu.ua/uk/public-nformation/pravilavnutrishnogo-rozporyadku-snu-imeni-lesi-ukrayinki), загальноприйнятих моральних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності. Атмосфера на заняттях повинна бути творчою, відкритою до конструктивної критики. Недопустимі запізнення на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття; списування. Очікується, що всі студенти відвідають усі лекції і лабораторні заняття курсу.

Кожен студент повинен ознайомитися і слідувати Кодексу академічної доброчесності Волинського національного університету імені Лесі Українки (https://ra.vnu.edu.ua/naukovizahody-ta-konkursy/konferentsiyi-ta-seminary/), дотримуватись етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової діяльності.

Дотримання академічної доброчесності здобувачами передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей, тверджень, відомостей; дотримання норм законодавства про авторське право; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

Під час оцінювання результатів навчання студенти не користуються забороненими засобами (мобільний телефон, планшет, конспект, навчальна література, інші джерела

інформації, в тому числі Інтернет-ресурси), самостійно виконують запропоновані завдання.

Політика щодо дедлайнів та перескладання.

Можливе, як очне, так і дистанційне проходження курсу. Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, він/вона вивчають теоретичний матеріал самостійно використовуючи інформаційну складову відповідного Moodle курсу та навчальні посібники. Тематичні завдання поточного тестового контролю виконують вчасно, адже після завершення вивчення теми можливість виконувати завдання теми припиняються. Прозвітуватися про виконання завдань можна у встановлені викладачем терміни під час консультацій.

Роботи над власними проектами (**ІНДЗ**) та їх захисти творяться впродовж семестру. Захисти проектів відбуваються в присутності студентів групи і з їх участю. Останнє може бути реалізовано, як в очному, так і в дистанційному режимі. Бали з **ІНДЗ** є поточним оцінюванням. Тому захисти проводяться до сесії.

V. Підсумковий контроль

Залік проводиться в тестовій формі в середовищі Moodle. Залік здають студенти незадоволені своєю оцінкою за курс. Пакет залікових завдань формується з всієї сукупності завдань курсу. Завдання з пакету вибираються випадковим чином. Час проведення заліку обмежений. Дається одна спроба на виконання пакету залікових завдань. Використання інформаційної складової курсу на заліку забороняється.

VI. Шкала оцінювання

Шкала оцінювання знань (форма контролю –)

Оцінка в балах	Лінгвістична оцінка
90–100	Зараховано
82–89	
75–81	
67–74	
60–66	
0–59	Незараховано (необхідне перескладання)

VII. Рекомендована література та інтернет-ресурси

Методичне забезпечення

Дисципліна має підтримку дистанційного курсу «Криптографія та стеганографія» на платформі MOODLE URL: https://moodle.vnu.edu.ua/course/view.php?id=156 та «Прикладна криптологія» URL: https://moodle.vnu.edu.ua/mod/page/view.php?id=158394 . В цих курсах крім інформаційної частини є потужна інтерактивна складова в вигляді пакетів тестових завдань, що сприяють систематизації, усвідомленню та закріпленню нового матеріалу по кожній темі. Також безпосередньо в курсі можна запускати та відлагоджувати програми online.

Основна література

1. Євсеєв С.П. , Король О.Г. , Шматко О.В. Кібербезпека: криптографія з PYTHON]. — Новий світ-2000, 2024. — 120с
2. Конахович Г.Ф., Прогонов Д.О., Пузиренко О.Ю. Комп'ютерна стеганографічна обробка

й аналіз мультимедійних даних [підручник]. — К. : «Центр навчальної літератури», 2018. — 558 с.
3. Al Sweigart Cracking codes with Python: an introduction to building and breaking ciphers Description: San Francisco :No Starch Press,Inc., [2018] https://elhacker.info/manuales/Lenguajes%20de%20Programacion/Python/Cracking%20Codes%20with%20Python.pdf
4. Дурняк Б.В., Музика Д.В., Сабат В.І. Стеганографічні методи захисту документів — Львів : Укр. акад. друкарства, 2014. — 159 с.
5. Кузнецов О.О., С.П. Євсеєв, О.Г. Король. Стеганографія: навчальний посібник – Х. : Вид. ХНЕУ, 2011. – 232 с.
6. Блінцов В.С., Гальчевський Ю.Л. Математичні основи криптології + CD : Навчальний посібник для студ. вищих навч. закл. Національний ун-т кораблебудування ім. адмірала Макарова. - Миколаїв : НУК, 2006. - 232с.
7. Горбенко І.Д., Гріненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах : Навч. посіб. для студ. Ч. 1. Криптографічний захист інформації. Харк. нац. ун-т радіоелектрон. - Х., 2004. - 368 с.
8. Задірака В.К., Олексюк О.С. Комп'ютерна криптологія : Підручник. - Тернопільська академія народного господарства; НАН України; Інститут кібернетики ім. В.М.Глушкова. - К., 2002. - 504с.
9. Блінцов В.С., Гальчевський Ю.Л. Математичні основи криптології + CD : Навч. посіб. для студ. вищ. навч. закл. Нац. ун-т кораблебудування ім.Адмірала Макарова. - Миколаїв, 2006. - 232 с.
10. Маракова І.І., Рибак А.І., Ямпольський Ю.С. Захист інформації. Криптографічні методи : Підруч. для вищ. навч. закл. - Одес. держ. Політехн. ун-т, Ін-т радіоелектрон. і телекомунікацій. - О., 2001. - 174 с.
11. Антонов В.М., Пермяков О.Ю. Комп'ютерні мережі військового призначення . - К.: "МК-Прес", 2005. - 320 с.
12. Кузнецов О.О., Євсеєв С.П., Король О.Г. Стеганографія:навчальний посібник . – Х. : Вид. ХНЕУ, 2011. – 232 с.
13. Головін М.Б., Головіна Н.А., Яцюк С.М., Сачук Ю.В. Захист інформації стеганографічним способом мовою Python засобами графічної бібліотеки Pillow. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. Луцьк, 2020. Випуск № 40 с.110-115. URI: https://evnuir.vnu.edu.ua/handle/123456789/19701
14. Головін М.Б., Головіна Н.А. Навчальний приклад маскування інформації в акустичному сигналі. Наукові записки Бердянського державного педагогічного університету. Серія: Педагогічні науки. Бердянськ, 2021. Випуск 2. С. 203-210. URI: https://evnuir.vnu.edu.ua/handle/123456789/20108
15. Mykola Holovin, Nina Holovina Educational example of masking textual information in a photographic signal. Journal «ScienceRise: Pedagogical Education» No4(49)2022 pp24-28 URL: http://journals.uran.ua/sr_edu/article/view/261051/258566
16. Головін М.Б., Головіна Н.А. Фур'є перетворення в якості аплікації спектрального аналізу звуків у курсах комп'ютерної фізики та захисту інформації. Комп'ютерно- інтегровані технології: освіта, наука, виробництво. Луцьк, 2021. Випуск № 42. С.37-42. URI: https://evnuir.vnu.edu.ua/handle/123456789/19750