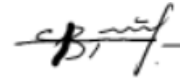


**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**Львівський національний університет імені Івана Франка**  
**Факультет прикладної математики та інформатики**  
**Кафедра кібербезпеки**

**Затверджено**

На засіданні кафедри кібербезпеки  
факультету прикладної математики та  
інформатики  
Львівського національного університету  
імені Івана Франка  
(протокол № 15/23 від 29 серпня 2023 р.)



Завідувач кафедри П.С.Венгерський

**Силабус з навчальної дисципліни**  
**“Застосування Python в кібербезпеці”,**  
**що викладається в межах ОПП Кібербезпека**  
**першого (бакалаврського) рівня вищої освіти для здобувачів з**  
**спеціальності 125 – Кібербезпека та захист інформації**

<b>Назва дисципліни</b>	<b>Застосування Python в кібербезпеці</b>
<b>Адреса викладання дисципліни</b>	Львівський національний університет імені Івана Франка, вул. Університетська 1, м. Львів, Україна, 79000
<b>Факультет та кафедра, за якою закріплена дисципліна</b>	Факультет прикладної математики та інформатики Кафедра кібербезпеки
<b>Галузь знань, шифр та назва спеціальності</b>	12 – інформаційні технології 125 – кібербезпека та захист інформації
<b>Викладачі дисципліни</b>	Квасниця Галина Андріївна, канд. фіз.-мат. наук, доцент кафедри кібербезпеки (лекції та лабораторні заняття)
<b>Контактна інформація викладачів</b>	<a href="mailto:halyna.kvasnytsya@lnu.edu.ua">halyna.kvasnytsya@lnu.edu.ua</a> ; <a href="https://ami.lnu.edu.ua/employee/kvasnytsia">https://ami.lnu.edu.ua/employee/kvasnytsia</a> ; Головний корпус ЛНУ ім. І. Франка, каб. 380. м. Львів, вул. Університетська, 1
<b>Консультації з питань навчання по дисципліні відбуваються</b>	Консультації в день проведення лекцій/практичних занять (а також за розкладом консультацій кафедри). Можливі он-лайн консультації через Microsoft Teams. Для погодження часу он-лайн конультації слід писати на електронну пошту викладача.
<b>Сторінка курсу</b>	<a href="https://ami.lnu.edu.ua/course/zastosuvannia-python-u-kiberbezpetsi">https://ami.lnu.edu.ua/course/zastosuvannia-python-u-kiberbezpetsi</a>
<b>Інформація про дисципліну</b>	Дисципліна “Застосування Python в кібербезпеці” є вибірковою дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається в 6-му семестрі в обсязі 5-ох кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
<b>Коротка анотація дисципліни</b>	Курс спрямований на поглиблене вивчення засобів мови програмування Python, що можуть бути використані як для проведення кібератак, так і з метою їх знешкодження та ефективної протидії.
<b>Мета та цілі дисципліни</b>	Метою курсу вибіркової дисципліни “Застосування Python в кібербезпеці” є набуття студентами теоретичних знань та практичних умінь для застосування Python у розробці власних та модифікації існуючих інструментів у галузі кібербезпеки.
<b>Література для вивчення дисципліни</b>	<i>Основна</i> <ol style="list-style-type: none"> <li>Ortega J.M. Python for Security and Networking: Leverage Python modules and tools in securing your network and applications - Packt Publishing, 2023, 586 p.</li> <li>Chou E. Mastering Python Networking. - Packt Publishing, 2023, 576 p.</li> <li>Seitz J., Arnold T. Black Hat Python: Python Programming for Hackers and Pentesters - No Starch Press, 2021, 216 p.</li> <li>Gracam D.G. Ethical Hacking: A Hands-on Introduction to Breaking In - No Starch Press, 2021, 376 p.</li> </ol> <i>Допоміжна</i> <ol style="list-style-type: none"> <li>Duffy C. Python: Penetration Testing for Developers - Packt Publishing, 2016. - 666 p.</li> <li>Lutz M. Learning Python - O'Reilly Media, 2013. 1643 p.</li> <li>Rehim R. Effective Python Penetration Testing - Packt Publishing, 2016, 164 p.</li> <li>Buchanan C. Python Web Penetration Testing Cookbook - Packt Publishing Ltd, 2015. – 224 p.</li> <li>O'Connor TJ. Violent Python. A Cookbook for Hackers, Forensic</li> </ol>

	<p>Analysts, Penetration Testers and Security Engineers. Elsevier, 2013. – 269 p.</p> <p><i>Он-лайн курси:</i></p> <ol style="list-style-type: none"> <li>1. <a href="#">Python for cybersecurity (Coursera)</a></li> <li>2. <a href="#">Python for penetration testers (Udemy)</a></li> <li>3. <a href="#">Learn Python and ethical hacking (Udemy)</a></li> </ol>
<b>Обсяг курсу</b>	Загальний обсяг: 150 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 86 год.
<b>Очікувані результати навчання</b>	<p>У результаті вивчення навчальної дисципліни студент має набути таких компетентностей:</p> <p><b>знати:</b></p> <ul style="list-style-type: none"> <li>-бібліотеки Python, призначені для низькорівневого мережевого програмування, збору і аналізу інформації про мережевий трафік;</li> <li>- основи взаємодії з Web за допомогою Python;</li> <li>- механізми створення шкідливого програмного забезпечення та засоби для його виявлення і знешкодження.</li> </ul> <p><b>вміти:</b></p> <ul style="list-style-type: none"> <li>- розробляти сценарії Python у вигляді виконуваних файлів та модулів;</li> <li>- перехоплювати мережевий трафік, розробляти власні інструменти для його аналізу,</li> <li>- створювати і модифікувати сценарії для атак на веб-застосунки;</li> <li>- збирати відкриту і приховану інформацію з веб-сайтів для подальших атак;</li> <li>- виконувати та виявляти SQL- ін'єкції, експлуатувати файли –cookies;</li> <li>- виявляти вразливості та шкідливе програмне забезпечення,</li> <li>- здійснювати розробку інструментів кіберзахисту при здійсненні професійної діяльності.</li> </ul> <p><b>Курс забезпечує набуття таких компетентностей: ІК, ЗК 1, ЗК 5, ФК 3, ФК 5, ФК 11, ФК 12; та програмних результатів навчання: ПРН 2-4, ПРН 6, ПРН 14, ПРН 15, ПРН 16, ПРН 18, ПРН 20, ПРН 22, ПРН 27-31, ПРН 49-53.</b></p>
<b>Ключові слова</b>	Кібербезпека, загроза, вразливість, цілісність, безпека даних, мережевий трафік, веб-скрапінг.
<b>Формат курсу</b>	Очний
<b>Теми</b>	Теми подані у Схемі курсу нижче
<b>Підсумковий контроль, форма</b>	Залік у кінці семестру
<b>Пререквізити</b>	Для вивчення курсу студенти потребують базових знань з: основ кібербезпеки, операційних систем, безпеки комп'ютерних мереж, математичної та прикладної криптології, програмування мовою Python.
<b>Навчальні методи та техніки, які будуть використовуватися під час викладання курсу</b>	<p>Презентації, лекції</p> <p>Модульний контроль.</p> <p>Лабораторні заняття у вигляді виконання практичних завдань і презентації отриманих результатів, обговорення написаних програм, самостійна робота з опрацювання пропонованих модулів :</p>
<b>Необхідне обладнання</b>	Лабораторія з обладнаними робочими станціями, з'єднаними в комп'ютерну мережу. Можливість підключення робочих станцій до мережі Інтернет. Можливість встановлення віртуальних машин та резервної операційної системи Kali Linux.

<p><b>Критерії оцінювання (окремо для кожного виду навчальної діяльності)</b></p>	<p>Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:</p> <ul style="list-style-type: none"> <li>• лабораторні роботи: 70% семестрової оцінки; максимальна кількість балів – 70.</li> <li>• контрольний тест: 30% семестрової оцінки; кількість балів – 30.</li> </ul> <p>Підсумкова максимальна кількість балів – 100.</p> <p><b>Академічна доброчесність:</b> Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману.</p> <p><b>Відвідання занять</b> є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні заняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів визначених для виконання всіх лабораторних робіт, передбачених курсом.</p> <p><b>Література.</b> Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих.</p> <p><b>Політика виставлення балів.</b> Враховуються бали набрані при самостійній роботі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час практичного заняття; недопустимість пропусків та запізнь на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін.</p> <p>Жодні форми порушення академічної доброчесності не толеруються.</p>
<p><b>Опитування</b></p>	<p>Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.</p>

### Схема курсу

Тиж.	Тема, план, короткі тези	Форма діяльності (заняття)	Література	Завдання, год.	Термін виконання
1	<p><b>Тема 1. Особливості застосування Python в кібербезпеці.</b> (Python: особливості, роль у кібербезпеці, корисні бібліотеки; робота з інтерпретатором Python та використання інтерактивного режиму)</p>	лекція, самостійна робота	[1-9]	2 9	1 тиждень
	<p><b>Тема 1. Особливості застосування Python в кібербезпеці.</b></p>	лаб.	[1-9]	2	

	(Запуск скриптів з командного рядка. Модуль argparse)				
2	<b>Тема 1. Особливості застосування Python в кібербезпеці.</b> (Виконання команд операційної системи зі скрипту - модуль subprocess )	лаб.	[1-9]	2	1 тиждень
3	<b>Тема 2. Робота з рядками та регулярні вирази в Python для обробки текстової інформації.</b> (Символи та кодування. Рядки, основні операції з текстом; використання регулярних виразів для пошуку та обробки текстової інформації, модуль re; застосування у кібербезпеці: фільтрація та пошук патернів в лог-файлах, аналіз текстових даних)	лекція, самостійна робота	[1-9]	2 9	1 тиждень
	<b>Тема 2 Робота з рядками в Python для обробки текстової інформації.</b> (основні операції з текстом)	лаб.	[1-9]	2	
4	<b>Тема 2. Регулярні вирази в Python.</b> (Використання модуля re для пошуку патернів та обробки текстової інформації)	лаб.	[1-9]	2	1 тиждень
5	<b>Тема 3. Робота з файлами та взаємодія з файловою системою</b> (Читання та запис файлів в Python, взаємодія з файловою системою для обробки даних (модулі os, sys, shutil), робота з форматом JSON для обміну та збереження структурованих даних)	лекція, самостійна робота	[1-9]	2 9	1 тиждень
	<b>Тема 3. Робота з файлами та взаємодія з файловою системою</b> (Модулі os, sys, shutil та засоби python для роботи з файловою системою)	лаб.	[1-9]	2	
6	<b>Тема 3. Робота з файлами та взаємодія з файловою системою</b> (Дослідження файлів і каталогів. Пошук особистої інформації)	лаб.	[1-9]	2	1 тиждень
7	<b>Тема 4. Мережеве програмування на Python</b> (Знайомство з концепціями мережевого програмування; сокети як основний механізм мережевої взаємодії в Python; основні мережеві протоколи: HTTP, FTP, SMTP, SNMP; приклади коду для створення простих клієнтських та серверних додатків)	лекція, самостійна робота	[1-9]	2 9	1 тиждень
	<b>Тема 4 Мережеве програмування на Python.</b> (Розробка простих клієнта та сервера з використанням бібліотеки socket, створення та налаштування сокетів для обміну даними між клієнтом та сервером; розробка сканера відкритих портів)	лаб.	[1-9]	2	
8	<b>Тема 4. Мережеве програмування на Python.</b> (Робота з модулем http.server. Розробка веб-сервера та веб-клієнта. Фільтрація даних.)	лаб.	[1-9]	2	1 тиждень
9	<b>Тема 5. Засоби Python для аналізу мережевого трафіку</b> (Збір та запис мережевого трафіку; використання бібліотеки scapy для захоплення	лекція, самостійна робота	[1-9]	2 9	1 тиждень

	пакетів; запис мережевого трафіку у форматі PCAP; аналіз заголовків пакетів: IP адреси, порти, протоколи; виявлення незвичних патернів у трафіку; визначення та аналіз аномалій у мережі)				
	<b>Тема 5. Засоби Python для аналізу мережевого трафіку).</b> (бібліотека scapy; розробка простого ARP-сканера)	лаб.	[1-9]	2	
10	<b>Тема 5. Засоби Python для аналізу мережевого трафіку.</b> (атака ARP -спуфінгу та детектор атаки, DNS-спуфінг. Сніфер пакетів)	лаб.	[1-9]	2	1 тиждень
11	<b>Тема 6. Криптографічні аспекти в Python.</b> (Основи криптографії та їх використання в Python; шифрування та кодування даних, бібліотека rucrypto; атаки на шифри та способи їх запобігання)	лекція, самостійна робота	[1-9]	2 9	1 тиждень
	<b>Тема 6. Криптографічні аспекти в Python.</b> (Шифрування та кодування повідомлень. Використання зашифрованих каналів)	лаб.	[1-9]	2	
12	<b>Тема 6. Криптографічні аспекти в Python.</b> (Шифрування файлів. Програми-вимагачі)	лаб.	[1-9]	2	1 тиждень
13	<b>Тема 7. Бібліотеки Python для взаємодії з Web. Захист веб-додатків.</b> (Веб-додатки та важливість їх захисту; огляд основних вразливостей веб-додатків та способи їх усунення; модулі для взаємодії з веб – requests, urllib, urllib2, BeautifulSoup; розробка скриптів для тестування веб-додатків на вразливості)	лекція, самостійна робота	[1-9]	2 9	1 тиждень
	<b>Тема 7. Бібліотеки Python для взаємодії з Web. Захист веб-додатків.</b> (Модуль requests. Надсилання та обробка запитів до сервера)	лаб.	[1-9]	2	
14	<b>Тема 7. Бібліотеки Python для взаємодії з Web. Захист веб-додатків.</b> (Веб-скрапінг та парсинг даних з HTML. Використання BeautifulSoup для HTML-парсингу)	лаб.	[1-9]	2	1 тиждень
15	<b>Тема 8. Захист від зловмисних програм</b> (Огляд зловмисних програм та їх типів; способи захисту від зловмисних програм; розробка скриптів для виявлення та блокування зловмисних програм)	лекція, самостійна робота	[1-9]	2 9	1 тиждень
	<b>Тема 8. Захист від зловмисних програм.</b> (Шкідливе програмне забезпечення. Бекдори. Конвертація скриптів у виконуваний файли. Трояни)	лаб.	[1-9]	2	

16	<b>Тема 8. Захист від зловмисних програм.</b> (Сканер вразливостей на Python)	лаб.	[1-9]	2	1 тиждень
----	--	------	-------	---	-----------