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 № 16/23 від 7 вересня 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

Львів - 2023

Назва дисципліни	**Застосування Python в кібербезпеці**
Адреса викладання дисципліни	Львівський національний університет імені Івана Франка, вул. Університетська 1, м. Львів, Україна, 79000
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра кібербезпеки
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 125 – кібербезпека та захист інформації
Викладачі дисципліни	Квасниця Галина Андріївна, канд. фіз.-мат. наук, доцент кафедри кібербезпеки (лекції та лабораторні заняття)
Контактна інформація викладачів	halyna.kvasnytsya@lnu.edu.ua; https://ami.lnu.edu.ua/employee/kvasnytsia; Головний корпус ЛНУ ім. І. Франка, каб. 380. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	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.
Сторінка курсу	https://ami.lnu.edu.ua/course/zastosuvannia-python-u-kiberbezpetsi
Інформація про дисципліну	Дисципліна “Застосування Python в кібербезпеці” є вибірковою дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається в шостому семестрі в обсязі 4-ох кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	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.
Мета та цілі дисципліни	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.
Література для вивчення дисципліни	*Основна* 1. Ortega J.M. Python for Security and Networking: Leverage Python modules and tools in securing your network and applications - Packt Publishing, 2023, 586 p. 2. Chou E. Mastering Python Networking. - Packt Publishing, 2023, 576 p. 3. Seitz J., Arnold T. Black Hat Python: Python Programming for Hackers and Pentesters - No Starch Press, 2021, 216 p. 4. Gracam D.G. Ethical Hacking: A Hands-on Introduction to Breaking In - No Starch Press, 2021, 376 p. *Допоміжна* 5. Duffy C. Python: Penetration Testing for Developers - Packt Publishing, 2016. -666 p. 6. Lutz M. Learning Python - O'Reilly Media, 2013. 1643 p. 7. Rehim R. Effective Python Penetration Testing - Packt Publishing, 2016, 164 p.

	8. Buchanan C. Python Web Penetration Testing Cookbook - Packt Publishing Ltd, 2015. – 224 p. 9. O'Connor TJ. Violent Python. A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers. Elsevier, 2013. – 269 p. *Он-лайн курси*: 1. Python for cybersecurity (Coursera) 2. Python for penetration testers (Udemy) 3. Learn Python and ethical hacking (Udemy)
Обсяг курсу	Загальний обсяг: 120 годин. Аудиторних занять: 48 год., з них 16 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 72 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** -бібліотеки Python, призначені для низькорівневого мережевого програмування, збору і аналізу інформації про мережевий трафік; - основи взаємодії з Web за допомогою Python; - механізми створення шкідливого програмного забезпечення та засоби для його виявлення і знешкодження. **вміти:** - розробляти сценарії Python у вигляді виконуваних файлів та модулів; - перехоплювати мережевий трафік, розробляти власні інструменти для його аналізу, - створювати і модифікувати сценарії для атак на веб-застосунки; - збирати відкриту і приховану інформацію з веб-сайтів для подальших атак; - виконувати та виявляти SQL- ін'єкції, експлуатувати файли –cookies; - виявляти вразливості та шкідливе програмне забезпечення, - здійснювати розробку інструментів кіберзахисту при здійсненні професійної діяльності. **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.**
Ключові слова	Кібербезпека, загроза, вразливість, цілісність, безпека даних, мережевий трафік, веб-скрапінг.
Формат курсу	Очний Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми подані у Схемі курсу нижче
Підсумковий контроль, форма	Залік у кінці 6 семестру
Пререквізити	Для вивчення курсу студенти потребують базових знань з : основ кібербезпеки, операційних систем, безпеки комп'ютерних мереж, математичної та прикладної криптології, програмування мовою Python.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції Модульний контроль. Лабораторні заняття у вигляді виконання практичних завдань і презентації отриманих результатів, обговорення написаних програм, самостійна робота з опрацювання пропонованих модулів

Необхідне обладнання	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.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • лабораторні роботи: 70% семестрової оцінки; максимальна кількість балів – 70. • контрольний тест: 20% семестрової оцінки; кількість балів – 20. • додаткові бали за активну участь у лекціях і лабораторних роботах 10% семестрової оцінки; максимальна кількість балів – 10. Підсумкова максимальна кількість балів – 100. **Академічна доброчесність**: 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 незарахуванння викладачем, незалежно від масштабів плагіату чи обману. **Відвідання занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні зайняття 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. **Література.** 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. **Політика виставлення балів.** 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 запізнень 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. Жодні форми порушення академічної доброчесності не толеруються.
Питання до заліку.	Залік – за результатами поточного контролю протягом семестру і усне опитування. Питання відповідають темам курсу.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу

Тиж.	Тема, план, короткі тези	Форма діяльності (заняття)	Література	Завдання, год.	Термін виконання
1	**Тема 1. Особливості застосування Python в кібербезпеці.** (Python: особливості, роль у кібербезпеці, корисні бібліотеки; робота з інтерпретатором Python та використання інтерактивного режиму)	лекція, самостійна робота	[1-9]	2 9	1 тиждень
	Тема 1. Особливості застосування Python в кібербезпеці. (Запуск скриптів з командного рядка. Модуль argparse)	лаб.	[1-9]	2	
2	**Тема 1. Особливості застосування Python в кібербезпеці.** (Виконання команд операційної системи зі скрипту - модуль subprocess)	лаб.	[1-9]	2	1 тиждень
3	**Тема 2. Робота з рядками та регулярні вирази в Python для обробки текстової інформації.** (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
	Тема 2 Робота з рядками в Python для обробки текстової інформації. (основні операції з текстом)	лаб.	[1-9]	2	
4	**Тема 2. Регулярні вирази в Python.** (Використання модуля re для пошуку патернів та обробки текстової інформації)	лаб.	[1-9]	2	1 тиждень
5	**Тема 3. Робота з файлами та взаємодія з файловою системою** (Читання та запис файлів в Python, взаємодія з файловою системою для обробки даних (модулі os, sys, shutils), робота з форматом JSON для обміну та збереження структурованих даних)	лекція, самостійна робота	[1-9]	2 9	1 тиждень
	Тема 3. Робота з файлами та взаємодія з файловою системою (Модулі os, sys, shutils та засоби python для роботи з файловою системою)	лаб.	[1-9]	2	
6	**Тема 3. Робота з файлами та взаємодія з файловою системою** (Дослідження файлів і каталогів. Пошук особистої інформації)	лаб.	[1-9]	2	1 тиждень
7	**Тема 4. Мережеве програмування на Python** (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

	Тема 4 Мережеве програмування на Python. (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	**Тема 4. Мережеве програмування на Python.** (Робота з модулем http.server. Розробка веб-сервера та веб-клієнта. Фільтрація даних.)	лаб.	[1-9]	2	1 тиждень
9	**Тема 5. Засоби Python для аналізу мережевого трафіку** (Збір та запис мережевого трафіку; використання бібліотеки scapy для захоплення 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)	лекція, самостійна робота	[1-9]	2 9	1 тиждень
	Тема 5. Засоби Python для аналізу мережевого трафіку). (бібліотека scapy; розробка простого ARP-сканера)	лаб.	[1-9]	2	
10	**Тема 5. Засоби Python для аналізу мережевого трафіку.** (атака ARP -спуфінгу та детектор атаки, DNS-спуфінг. Сніфер пакетів)	лаб.	[1-9]	2	1 тиждень
11	**Тема 6. Криптографічні аспекти в Python.** (Основи криптографії та їх використання в Python; шифрування та кодування даних, бібліотека pycrypto; атаки на шифри та способи їх запобігання)	лекція, самостійна робота	[1-9]	2 9	1 тиждень
	Тема 6. Криптографічні аспекти в Python. (Шифрування та кодування повідомлень. Використання зашифрованих каналів)	лаб.	[1-9]	2	
12	**Тема 6. Криптографічні аспекти в Python.** (Шифрування файлів. Програми-вимагачі)	лаб.	[1-9]	2	1 тиждень
13	**Тема 7. Бібліотеки Python для взаємодії з Web. Захист веб-додатків.** (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
	Тема 7. Бібліотеки Python для взаємодії з Web. Захист веб-додатків. (Модуль requests. Надсилання та обробка запитів до сервера)	лаб.	[1-9]	2	

14	**Тема 7. Бібліотеки Python для взаємодії з Web. Захист веб-додатків.** (Веб-скрапінг та парсинг даних з HTML. Використання BeautifulSoup для HTML-парсингу)	лаб.	[1-9]	2	1 тиждень
15	**Тема 8. Захист від зловмисних програм** (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
	Тема 8. Захист від зловмисних програм. **(**Шкідливе програмне забезпечення. Бекдори. Конвертація скриптів у виконувані файли. Трояни**)**	лаб.	[1-9]	2	
16	**Тема 8. Захист від зловмисних програм.** **(**Сканер вразливостей на Python**)**	лаб.	[1-9]	2	1 тиждень