ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНОЇ ІНЖЕНЕРІЇ (ФІС)

КАФЕДРА КІБЕРБЕЗПЕКИ

1. Загальна інформація про дисципліну:

Назва дисципліни	**БЕЗПЕКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ**
Викладач	Козак Руслан Орестович
Профайл викладача	https://library.tntu.edu.ua/personaliji/a/k/kozak-ruslan-orestovych/
Контактний тел.	Комутатор (0352) 51-97-00, внутрішній 1804 (із зовнішніх телефонів через комутатор, тоді в режимі тонального набору набрати внутрішній номер)
E-mail:	kozak@tntu.edu.ua
Сторінка дисципліни в A-Tutor	https://dl.tntu.edu.ua, ID4968
Консультації	Згідно графіку консультацій у першому семестрі

2. Коротка анотація до дисципліни

Навчальна дисципліна «**Безпека програмного забезпечення**» належить до вибіркових дисциплін циклу професійної підготовки освітньої програми «Інформаційні системи та технології» першого (бакалаврського) рівня вищої освіти. Галузь знань 12 «Інформаційні технології», спеціальності 126 «Інформаційні системи та технології». Викладається у 7 семестрі (четвертий курс) обсягом 4,5 кредитів ECTS. Формою підсумковою контролю є залік.

3. Мета та завдання дисципліни

Мета дисципліни «**Безпека програмного забезпечення**» полягає у вивченні студентами теоретичних та методичних питань щодо дослідження вразливостей та захисту програмного забезпечення, набуття спеціальних знань і практичних навиків застосування методів та засобів побудови ефективних систем захисту програмного забезпечення.

Завданням дисципліни є оволодіння студентами теоретичних та практичних основ роботи з методами та засобами дослідження вразливостей програмного забезпечення та дозволить надати студентам знання щодо сучасних підходів, методів та засобів захисту програмного забезпечення. Оволодіння цією дисципліною виробить у студентів навички практичного використання сучасних прийомів і методів захисту програмного забезпечення.

4. Формат дисципліни:

Дисципліна передбачає проведення лекційних, лабораторних занять та консультацій. Для кращого розуміння та засвоєння викладеного матеріалу дисципліна має супровід у вигляді електронного навчального курсу в системи A-Tutor (https://dl.tntu.edu.ua). Електронний навчальний курс має лекційний матеріал, лабораторні роботи, питання підсумкового контролю та систему оцінювання.

5. Результати навчання:

В результаті вивчення дисципліни студент повинен **знати:**

- ✓ способи розробки Shellcode;
- ✓ особливості вразливості Buffer Overflow;
- ✓ прийоми проведення атаки Return-to-libc;
- ✓ вразливості при використанні Environment Variables, Set-UID Program, Format String and Race Condition;
- ✓ прийоми проведення атаки TCP/IP Attack and DNS Attack;
- ✓ способи проведення атаки Cross-Site Request Forgery Attack and Cross-Site Scripting Attack;
- ✓ прийоми проведення атаки SQL Injection Attack.

В результаті вивчення дисципліни студент повинен **вміти:**

- ✓ використовувати засоби розробки та дослідження Shellcode;

- ✓ враховувати особливості вразливості Buffer Overflow при розробці програмного забезпечення;
- ✓ використовувати стандартні засоби захисту від вразливостей Environment Variables, Set-UID Program, Format String and Race Condition;
- ✓ організовувати захист від атак Cross-Site Request Forgery Attack and Cross-Site Scripting Attack;
- ✓ боротися із атаками SQL Injection.

Вивчення навчальної дисципліни передбачає формування та розвиток у студентів **загальних компетентностей (КЗ) та спеціальних (фахових) компетентностей (КС)** згідно освітньої програми.

Загальні:

КЗ 2. Здатність застосовувати знання у практичних ситуаціях;

КЗ 3. Здатність до розуміння предметної області та професійної діяльності;

КЗ 6. Здатність до пошуку, оброблення та узагальнення інформації з різних джерел.

Спеціальні (фахові):

КС 1. Здатність аналізувати об'єкт проектування або функціонування та його предметну область;

КС 3. Здатність до проектування, розробки, налагодження та вдосконалення системного, комунікаційного та програмно-апаратного забезпечення інформаційних систем та технологій, Інтернету речей (IoT), комп'ютерно-інтегрованих систем та системної мережної структури, управління ними.

КС 4. Здатність проектувати, розробляти та використовувати засоби реалізації інформаційних систем, технологій та інфокомунікацій (методичні, інформаційні, алгоритмічні, технічні, програмні та інші).

КС 6. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків.

Вивчення навчальної дисципліни передбачає формування у студентів таких прикладних **результатів навчання (ПР)** згідно освітньої програми:

ПР 3. Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій;

ПР 5. Аргументувати вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій;

ПР 9. Здійснювати системний аналіз архітектури підприємства та його IT-інфраструктури, проводити розроблення та вдосконалення її елементної бази і структури.

6. Обсяг дисципліни

Вид заняття	Загальна кількість годин
лекції	**32**
лабораторні заняття	**32**
самостійна робота	**71**
Всього за дисципліну	**145**

7. Ознаки дисципліни:

Рік викладання	Семестр	Курс	Спеціальність	Нормативна/ вибіркова
2020	7	4	122 «Комп'ютерні науки»	Вибіркова
2020	7	4	126 «Інформаційні системи та технології»	Вибіркова

8. Пререквізити

Студенти повинні володіти базовими знаннями з таких дисцилін: Архітектура та проєктування програмного забезпечення, Об'єктно-орієнтоване програмування, Програмування, Тестування програмного забезпечення, Комп'ютерні мережі, Операційні системи, Веб-технології, Організація баз даних.

9. Технічне й програмне забезпечення /обладнання:

Студент повинен мати рівень впевненого користувача assembler and disassembler nasm, disassembler objdump, xxd utility, Python, linker ld, compiler gcc, debugging tool gdb, Netwox tool, Scapy for Python, telnet utility, netcat utility, network analyzer Wireshark, Apache server, browser Firefox, Web Developer Network Tool, Firefox's Developer Tool, MySQL console.

10. Політика дисципліни

Усі процедури навчального процесу під час викладання дисципліни відповідають положенню про академічну доброчесність учасників освітнього процесу та недопущення академічного плагіату в Тернопільському національному технічному університеті імені Івана Пулюя.

11. Схема дисципліни

Тиж./ дата/ год.	Тема, підтеми	Форма заняття, формат	Матеріали	Література, ресурси в інтернеті	Завдання, год	Засоби діагностики	Вага оцінки
1	2	3	4	5	6	7	8
Тиж. 1/ 25.09/ 2 акад. год.	**Тема 0. Structure of Software Security course.** Run SEED VM on VirtualBox. Lab Environment Setup.	Лекція, F2F	Лекційний матеріал, Лаб. роб. № 0	Дистанційний курс	Опрацювання лекцій, 4 лаб. роб., 2	Kahoot!	
Тиж. 2/ 02.10/ 2 акад. год.	**Тема 1. Shellcode Development.** Writing Malicious Code Using C: Main Idea. Explanation of a Shellcode Example. Eliminating Zeros from the Code. Providing Arguments for System Calls. Providing Environment Variables for execve(). Using Code Segment.	Лекція, F2F Лаб. роб. № 1	Лекційний матеріал, Лаб. роб. № 1	Дистанційний курс	Опрацювання лекцій, 4 лаб. роб., 4	захист звіту з лаб. роб.	5
Тиж. 3/ 09.10/ 2 акад. год.	**Тема 2. Buffer Overflow Vulnerability.** Program Memory Layout. Stack and Function Invocation. Stack Buffer-Overflow Attack. Countermeasures: Address Randomization, StackGuard.	Лекція, F2F Лаб. роб. № 2	Лекційний матеріал, Лаб. роб. № 2	Дистанційний курс	Опрацювання лекцій, 4 лаб. роб., 2	захист звіту з лаб. роб.	5
Тиж. 4/ 16.10/ 2 акад. год.	**Тема 3. Return-to-libc Attack.** Understanding the Function Call Mechanism. Understanding the stack layout. Non-Executable Stack. The Attack Experiment. Turning off countermeasures. Launch the Return-to-libc Attack. Finding out the addresses of libc functions. Putting the shell string in the memory. Exploiting the buffer-overflow vulnerability. Turning on address randomization. Defeat Shell's countermeasure	Лекція, F2F Лаб. роб. № 3	Лекційний матеріал, Лаб. роб. № 3	Дистанційний курс	Опрацювання лекцій, 4 лаб. роб., 2	захист звіту з лаб. роб.	5
Тиж. 5/ 23.10/ 2 акад. год.	**Тема 4. Environment Variable and Set-UID Program.** Manipulating Environment Variables. Passing Environment Variables from Parent Process to Child Process. Environment Variables and execve(). Environment Variables and system(). Environment Variable and Set-UID Programs. The PATH Environment Variable and Set-UID Programs. Invoking External Programs Using system() versus execve().Principle of Least Privilege. Capability Leaking.	Лекція, F2F Лаб. роб. № 4	Лекційний матеріал, Лаб. роб. № 4	Дистанційний курс	Опрацювання лекцій, 4 лаб. роб., 2	захист звіту з лаб. роб.	5

Тиж. 6/ 30.10/ 2 акад. год.	**Тема 5. Format String Vulnerability.** Functions with Variable Number of Arguments. Format String with Missing Optional Arguments. Vulnerable Program and Experiment Setup. Exploiting the Format String Vulnerability. Code Injection Attack using Format String Vulnerability. Countermeasures.	Лекція, F2F Лаб. роб. № 5	Лекційний матеріал, Лаб. роб. № 5	Дистанційний курс	Опрацювання лекцій, 4 лаб. роб., 2	захист звіту з лаб. роб.	5
Тиж. 7/ 06.11/ 2 акад. год. **Тиж**. 8/ 13.11/ 2 акад. год.	**Тема 6. Race Condition Vulnerability.** The General Race Condition Problem. Race Condition Vulnerability. Experiment Setup. Exploiting Race Condition Vulnerabilities. Launching the Race Condition Attack. An Improved Attack Method. Countermeasures.	Лекція, F2F Лаб. роб. № 6	Лекційний матеріал, Лаб. роб. № 6	Дистанційний курс	Опрацювання лекцій, 4 лаб. роб., 2	захист звіту з лаб. роб.	5
					Тестові завдання модуля 1, 7	Модульний контроль 1	7
Тиж. 9/ 14.11/ 2 акад. год.	**Тема 7. Attacks on the TCP/IP Protocol.** How the TCP Protocol Works. SYN Flooding Attack. TCP Reset Attack. TCP RST Attacks on telnet and ssh Connections. TCP RST Attacks on Video Streaming Applications. TCP Session Hijacking Attack.	Лекція, F2F Лаб. роб. № 7	Лекційний матеріал, Лаб. роб. № 7	Дистанційний курс	Опрацювання лекцій, 4 лаб. роб., 2	захист звіту з лаб. роб.	5
Тиж. 10/ 20.11/ 2 акад. год.	**Тема 8. The Mitnick Attack.** How the Mitnick Attack Works. Running a remote shell. Simulated SYN flooding. Spoof TCP Connections and rsh Sessions. Set Up a Backdoor.	Лекція, F2F Лаб. роб. № 8	Лекційний матеріал, Лаб. роб. № 8	Дистанційний курс	Опрацювання лекцій, 4 лаб. роб., 2	захист звіту з лаб. роб.	5
Тиж. 11/ 27.11/ 2 акад. год. **Тиж**. 12/ 04.12/ 2 акад. год.	**Тема 9. Domain Name System (DNS) and Attacks.** DNS Hierarchy, Zones, and Servers. DNS Query Process. Set Up DNS Server and Experiment Environment. Configure the User Machine. Set up a Local DNS Server. Attacks on DNS: Modifying the Host File, Directly Spoofing Response to User, DNS Cache Poisoning Attack. Constructing DNS Request and Reply Using Scapy. Protection Against DNS Spoofing Attacks.	Лекція, F2F Лаб. роб. № 9	Лекційний матеріал, Лаб. роб. № 9	Дистанційний курс	Опрацювання лекцій, 8 лаб. роб., 4	захист звіту з лаб. роб.	5
Тиж. 13/ 11.12/ 2 акад. год.	**Тема 10. Cross Site Request Forgery.** Cross-Site Requests and Its Problems. Cross-Site Request Forgery Attack. CSRF Attacks on HTTP GET Services. CSRF Attacks on HTTP POST Services. Countermeasures.	Лекція, F2F Лаб. роб. № 10	Лекційний матеріал, Лаб. роб. № 10	Дистанційний курс	Опрацювання лекцій, 4 лаб. роб., 2	захист звіту з лаб. роб.	5
Тиж. 14/ 18.12/ 2 акад. год.	**Тема 11. Cross-Site Scripting (XSS) Attack.** Understanding of Cross-Site Scripting Attack. XSS Attacks in Action. Achieving Self-Propagation. Preventing XSS attacks. Defeating XSS Attacks Using Content Security Policy (CSP).	Лекція, F2F Лаб. роб. № 11	Лекційний матеріал, Лаб. роб. № 11	Дистанційний курс	Опрацювання лекцій, 4 лаб. роб., 2	захист звіту з лаб. роб.	5

Тиж. 15/ 19.12/ 2 акад. год. **Тиж**. 16/ 25.12/ 2 акад. год.	**Тема 12. Web SQL Injection.** A Brief Tutorial of SQL. Interacting with Database in Web Application. Launching SQL Injection Attacks. The Fundamental Cause. Countermeasures.	Лекція, F2F Лаб. роб. № 12	Лекційний матеріал, Лаб. роб. № 12	Дистанційний курс	Опрацювання лекцій, 4 лаб. роб., 4	захист звіту з лаб. роб.	5
					Тестові завдання модуля 2, 8	Модульний контроль 2	8

12. Система оцінювання та вимоги

Форма підсумкового семестрового контролю – **залік.**

Підсумкова семестрова оцінка заліку складається з суми балів, отриманих студентом при проведенні проміжних (модульних) контролів рівня засвоєння теоретичних знань (за перший та другий модулі) та отриманих балів за лабораторні роботи.

МОДУЛЬ 1			**МОДУЛЬ 2**			**ПІДСУМКОВА СЕМЕСТРОВА ОЦІНКА**	**РАЗОМ З ДИСЦИПЛІНИ**
АУДИТОРНА ТА САМОСТІЙНА РОБОТА			**АУДИТОРНА ТА САМОСТІЙНА РОБОТА**				
ТЕОРЕТИЧНИЙ КУРС (ТЕСТУВАННЯ)	**ЛАБОРАТОРНА РОБОТА**		**ТЕОРЕТИЧНИЙ КУРС (ТЕСТУВАННЯ)**	**ЛАБОРАТОРНА РОБОТА**			
СЕМЕСТРОВА ОЦІНКА						**25**	**100**
7	**30**		**8**	**30**			
№ ЛЕКЦІЙ	**ВИД РОБІТ**	**БАЛ**	**№ ЛЕКЦІЙ**	**ВИД РОБІТ**	**БАЛ**	за кожних три бали семестрової оцінки студент отримує 1 бал підсумкової	
Лекція 0	Лаб. роб. №0	-	Лекція 7	Лаб. роб. №7	5		
Лекція 1	Лаб. роб. №1	5	Лекція 8	Лаб. роб. №8	5		
Лекція 2	Лаб. роб. №2	5	Лекція 9	Лаб. роб. №9	5		
Лекція 3	Лаб. роб. №3	5	Лекція 10	Лаб. роб. №10	5		
Лекція 4	Лаб. роб. №4	5	Лекція 11	Лаб. роб. №11	5		
Лекція 5	Лаб. роб. №5	5	Лекція 12	Лаб. роб. №12	5		
Лекція 6	Лаб. роб. №6	5					

До підсумкового семестрового контролю (складання семестрового заліку) допускаються студенти, які протягом семестру виконали всі види навчальної роботи, успішно пройшли проміжні (модульні) контролі і набрали не менше 45 балів семестрової бальної оцінки та за умови отримання не менше 60% (15) балів за результатами кожного проміжного (модульного) контролю рівня знань.

Підсумкова оцінка записується за 100-бальною шкалою із подальшим переведенням її у шкалу Європейської кредитно-трансферної системи (ECTS) відповідно A, B, C, D, E, F, FX при цьому чотирибальна шкала оцінок (з записом семестрової оцінки «відмінно» - A, «добре» - B,C, «задовільно» - D, E відповідають підсумковому результату «зараховано», «незадовільно» - F, FX відповідає підсумковому результату «незараховано»).

13. Навчально-методичне забезпечення

1. Електронний навчальний курс «Безпека програмного забезпечення» для студентів спеціальностей 122 «Комп'ютерні науки», 126 «Інформаційні системи та технології».

2. Методичні вказівки до виконання лабораторних робіт з дисципліни «Безпека програмного забезпечення» для здобувачів освітнього ступеня «бакалавр», спеціальностей: 122 «Комп`ютерні науки», 126 «Інформаційні системи та технології», всіх форм навчання. Укладачі Р.О. Козак, Г.П. Шмигер: ТНТУ, 2020 р.

3. Конспект лекцій з курсу " Безпека програмного забезпечення " для здобувачів освітнього ступеня «бакалавр», спеціальностей: 122 «Комп`ютерні науки», 126 «Інформаційні системи та технології», всіх форм навчання. Укладачі Р.О. Козак, Г.П. Шмигер: ТНТУ, 2020 р.

14. Рекомендована література

Базова

1. Wenliang Du. Computer & Internet Security: A Hands-on Approach, Second Edition. USA, Syracuse University: Middletown, DE (2019)

2. Aleph One. Smashing The Stack For Fun And Profit. URL: http://cecs.wright.edu/people/faculty/tkprasad/courses/cs781/alephOne.html

3. Chen, Wagner, and Dean. Setuid Demystified. URL: http://www.cis.syr.edu/~wedu/minix/projects/setuid_paper.pdf

4. Bishop. How to write a Set-UID program. URL: http://nob.cs.ucdavis.edu/~bishop/secprog/1987-sproglogin.pdf

5. Pradeep Padala. Playing with ptrace. URL: https://www.linuxjournal.com/article/6100

Допоміжна

1. O'Conor TJ. Violent Python. A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers. Amserdam: Elsevier, Syngress, 2013. 270 p.

2. Кузнецов О. О. Захист інформації в інформаційних системах : навч. посіб. Х. : ХНЕУ, 2018. 510 с.

3. Поляков А. О., Євсеєв С. П., Огурцов В. В. Лабораторний практикум з навчальної дисципліни "Захист інформації в інформаційних системах" : навч.-практ. посіб. - Х. : ХНЕУ, 2017. 208 с.

15. Інформаційні ресурси

1. http://dl.tntu.edu.ua Електронні навчальні курси ТНТУ імені І. Пулюя.

2. https://www.owasp.org/index.php/Web_Application_Penetration_Testing OWASP Foundation. OWASP Testing Guide v4.0. URL: