СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Методи виявлення уразливостей та протидії злоякісному програмному забезпеченню»

Лектор курсу			**Іванченко Ігор Сергійович,** кандидат технічних наук, доцент, професор кафедри технічних систем кіберзахисту.		**Контактна інформація лектора (e-mail), сторінка курсу в GWE**	**e-mail:** i.ivanchenko@duikt.edu.ua **сторінка курсу в Classroom:** https://classroom.google.com/c/ODc3ODgyMzI4NTA3?cjc=fzcvzyj3 **код доступу** – fzcvzyj3	
Галузь знань			F Інформаційні технології		**Рівень вищої освіти**	магістр	
Спеціальність			F5 Кібербезпека та захист інформації		**Семестр**	1, 2	
			F2 Інженерія програмного забезпечення			3	
Освітня програма			Інформаційна та кібернетична безпека Технічні системи інформаційного та кібернетичного захисту Інженерія програмного забезпечення		**Тип дисципліни**	Вибіркова компонента освітньо-професійної програми	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	150	24	–	18	12	96

АНОТАЦІЯ КУРСУ

Взаємозв'язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	Дисципліни професійної підготовки
Освітні компоненти для яких є базовою	Кваліфікаційна робота

Мета курсу:	Формування знань та вмінь щодо застосування методів та засобів виявлення уразливостей та злоякісного програмного забезпечення в інформаційних системах організацій, їх аналізу, виявлення недоліків та протиріч для постановки та вирішення наукових завдань у галузі кібербезпеки та захисту інформації.

Компетентності відповідно до освітньої програми

Soft-skills / Загальні компетентності (КЗ)	**Hard-skills / Фахові компетентності спеціальності (КФ)**
КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ6. Вміння визначати підприємницькі можливості чи вид діяльності або громадського впливу, здатність приймати обґрунтовані рішення, здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ8. Вміння розробляти математичні моделі завдань забезпечення інформаційної безпеки та захисту інформації. КЗ10. Здатність застосовувати кращі практики у професійній діяльності.	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

Програмні результати навчання (ПРН)

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема,опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Тема 1: Вступ. Основи виявлення уразливостей та шкідливого програмного забезпечення **Знати:** базові поняття кіберзагроз і етапи атак за моделлю Cyber Kill Chain, принципи роботи шкідливого ПЗ та методи його аналізу, типові веб-уразливості OWASP Top 10 – 2021, основи керування уразливостями, підходи офенсивної й дефенсивної безпеки, а також основи кіберрозвідки загроз і пошуку технічної інформації. **Вміти:** визначати фази атаки, розпізнавати і класифікувати шкідливе ПЗ, виконувати базовий статичний аналіз, ідентифікувати поширені уразливості, використовувати елементи офенсивної та дефенсивної безпеки, застосовувати методи пошуку загрозової інформації та орієнтуватися в інтерфейсі TryHackMe для виконання навчальних завдань. **Формування компетентностей:** КЗ1, КЗ6, КЗ8, КЗ10, КФ1, КФ2, КФ5, КФ9. **Результати навчання:** РН-2, РН-5, РН-6, РН-7, РН-10, РН-11, РН-20, РН-23. **Рекомендовані джерела:** 1-15.			
Вступ. Основи виявлення уразливостей та шкідливого програмного забезпечення	**Лекція 1 2 год**	1 бал	Лекція-візуалізація
Початок роботи на платформі TryHackMe	Практичне заняття 1 2 год	1 бал	Відпрацювання вправ на платформі TryHackMe: Getting Started; Offensive Security Intro; Defensive Security Intro; Search Skills.
Основи аналізу уразливостей та шкідливого програмного забезпечення	Практичне заняття 2 2 год	1 бал	Відпрацювання вправ на платформі TryHackMe: Vulnerabilities 101; Intro to Malware Analysis.
Основи виявлення уразливостей та шкідливого програмного забезпечення	Самостійна робота 1 11 год	4 бали	Самостійне відпрацювання вправ на платформі TryHackMe: Cyber Kill Chain; Intro to Cyber Threat Intel; Vulnerability Management. Відповідь на контрольні питання в GWE.
Тема 2: Технології мережевої безпеки та аналізу трафіку			

<table>
<tr><td colspan="4">Знати: основи мережевих технологій, архітектуру безпечних мереж, принципи роботи мережевих протоколів, атак на рівні L2 (наприклад, ARP-spoofing), методи маніпуляції DNS, управління сесіями, поняття C2-інфраструктури, типи мережевих атак і засоби їх виявлення (фаєрволи, IDS/IPS), а також методи пасивної та активної розвідки.
Вміти: використовувати Nmap для сканування мережі та виявлення хостів, застосовувати Wireshark для аналізу трафіку, ідентифікувати ознаки мережевих атак, аналізувати мережеві взаємодії, виявляти потенційно небезпечні служби, оцінювати рівень захищеності мережевої архітектури, та розпізнавати ознаки C2-комунікацій у трафіку.
<u>Формування компетентностей:</u> К31, К36, К38, К310, КФ1, КФ2, КФ5, КФ9.
<u>Результати навчання:</u> РН-2, РН-5, РН-6, РН-7, РН-10, РН-11, РН-20, РН-23.
<u>Рекомендовані джерела:</u> 1-15.</td></tr>
<tr><td>Технології мережевої безпеки та аналізу трафіку</td><td>Лекція 2
2 год</td><td>1 бал</td><td>Лекція-візуалізація</td></tr>
<tr><td>Сканування мережі з Nmap</td><td>Практичне заняття 3
2 год</td><td>1 бал</td><td>Відпрацювання вправ на платформі TryHackMe: Nmap: The Basics; Nmap Live Host Discovery.</td></tr>
<tr><td>Технології моніторингу та аналізу мережевого трафіку</td><td>Лекція 3
2 год</td><td>1 бал</td><td>Лекція-візуалізація</td></tr>
<tr><td>Аналіз трафіку з Wireshark</td><td>Лабораторна робота 1
2 год</td><td>1 бал</td><td>Відпрацювання вправ на платформі TryHackMe: Wireshark: The Basics.</td></tr>
<tr><td>Технології мережевої безпеки та аналізу трафіку</td><td>Самостійна робота 2
11 год</td><td>4 бали</td><td>Самостійне відпрацювання вправ на платформі TryHackMe: Networking Secure Protocols; Network Security Solutions; Firewalls
Відповідь на контрольні питання в GWE.</td></tr>
<tr><td colspan="4">Тема 3: Уразливості та захист операційних систем (Windows, Linux)
Знати: основи безпеки операційних систем Windows і Linux, типові уразливості ОС, принципи ескалації привілеїв, способи обходу UAC у Windows, можливості PowerShell для пентестерів, методи жорсткої конфігурації (hardening) систем, а також інструменти для виявлення слабких місць у привілеях користувачів.
Вміти: виявляти і використовувати уразливості для ескалації привілеїв у Windows та Linux, обходити контроль облікових записів (UAC), застосовувати PowerShell для аналізу безпеки, виконувати аудит ОС, аналізувати налаштування безпеки, та впроваджувати базові заходи укріплення систем (hardening) для підвищення їх стійкості до атак.
<u>Формування компетентностей:</u> К31, К36, К38, К310, КФ1, КФ2, КФ5, КФ9.
<u>Результати навчання:</u> РН-2, РН-5, РН-6, РН-7, РН-10, РН-11, РН-20, РН-23.
<u>Рекомендовані джерела:</u> 1-15.</td></tr>
<tr><td>Уразливості та технології захисту операційних систем Windows</td><td>Лекція 4
2 год</td><td>1 бал</td><td>Лекція-візуалізація</td></tr>
<tr><td>Ескалація привілеїв у Windows</td><td>Практичне заняття 4
2 год</td><td>1 бал</td><td>Відпрацювання вправ на платформі TryHackMe: Windows Privilege Escalation.</td></tr>
<tr><td>Уразливості та технології захисту операційних систем Linux</td><td>Лекція 5
2 год</td><td>1 бал</td><td>Лекція-візуалізація</td></tr>
<tr><td>Ескалація привілеїв у Linux</td><td>Практичне заняття 5
2 год</td><td>1 бал</td><td>Відпрацювання вправ на платформі TryHackMe: Linux Privilege Escalation.</td></tr>
</table>

Уразливості та захист операційних систем (Windows, Linux)	Самостійна робота 3 11 год	4 бали	Самостійне відпрацювання вправ на платформі TryHackMe: Operating System Security; PowerShell for Pentesters; Microsoft Windows Hardening; Linux System Hardening. Відповідь на контрольні питання в GWE.
Тема 4: Web-уразливості: методи виявлення та протидії **Знати:** основні веб-уразливості згідно з переліком OWASP Top 10 – 2021, принципи їх експлуатації та наслідки, а також можливості інструменту Burp Suite для виявлення та аналізу веб-загроз, включаючи перехоплення, модифікацію та повторну відправку HTTP-запитів. **Вміти:** розпізнавати поширені уразливості веб-додатків (SQLi, XSS, IDOR тощо), аналізувати веб-запити та відповіді, використовувати Burp Suite для тестування безпеки веб-додатків, застосовувати техніки мануального тестування та формувати звіти про виявлені загрози. **Формування компетентностей:** К31, К36, К38, К310, КФ1, КФ2, КФ5, КФ9. **Результати навчання:** РН-2, РН-5, РН-6, РН-7, РН-10, РН-11, РН-20, РН-23. **Рекомендовані джерела:** 1-15.			
Web-уразливості: методи виявлення та протидії	**Лекція 6 2 год**	1 бал	Лекція-візуалізація
Виявлення та дослідження поширених Web-уразливостей	Практичне заняття 6 2 год	1 бал	Відпрацювання вправ на платформі TryHackMe: OWASP Top 10 – 2021.
Основи тестування Web-додатків з Burp Suite	Лабораторна робота 2 2 год	1 бал	Відпрацювання вправ на платформі TryHackMe: Burp Suite: The Basics.
Web-уразливості: методи виявлення та протидії	Самостійна робота 4 11 год	4 бали	Самостійне відпрацювання вправ на платформі TryHackMe: OWASP Top 10; OWASP Broken Access Control; OWASP API Security Top 10 – 1. Відповідь на контрольні питання в GWE.
Тема 5: Виявлення та аналіз шкідливих програм **Знати:** основні типи та ознаки шкідливого програмного забезпечення, підходи до його класифікації, методи статичного та динамічного аналізу, структуру виконуваних файлів (наприклад, PE), а також базові інструменти, що використовуються для аналізу поведінки шкідливого ПЗ. **Вміти:** виконувати статичний аналіз шкідливих файлів без їх запуску (перевірка хешів, аналіз метаданих, рядків тощо), застосовувати динамічний аналіз у контрольованому середовищі для виявлення активності зразка, розпізнавати індикатори компрометації (IoCs) та інтерпретувати результати аналізу для виявлення загроз. **Формування компетентностей:** К31, К36, К38, К310, КФ1, КФ2, КФ5, КФ9. **Результати навчання:** РН-2, РН-5, РН-6, РН-7, РН-10, РН-11, РН-20, РН-23. **Рекомендовані джерела:** 1-15.			
Технології статичного аналізу шкідливого програмного забезпечення	**Лекція 7 2 год**	1 бал	Лекція-візуалізація
Базовий статичний аналіз	Практичне заняття 7 2 год	1 бал	Відпрацювання вправ на платформі TryHackMe: Basic Static Analysis.
Технології динамічного аналізу шкідливого програмного забезпечення	**Лекція 8 2 год**	1 бал	Лекція-візуалізація
Базовий динамічний аналіз	Лабораторна робота 3	1 бал	Відпрацювання вправ на платформі TryHackMe: Basic Dynamic Analysis.

	2 год		
Виявлення та аналіз шкідливих програм	Самостійна робота 5 11 год	4 бали	Самостійне відпрацювання вправ на платформі TryHackMe: MAL: Malware Introductory; Dissecting PE Headers. Відповідь на контрольні питання в GWE.
Тема 6: Реверс-інжиніринг та дебагінг **Знати:** принципи реверс-інжинірингу, відмінності між статичним і динамічним аналізом, структуру виконуваних файлів (PE), основи дизасемблювання та дебагінгу, призначення таких інструментів, як Ghidra, x64dbg, Immunity Debugger та ін. **Вміти:** виконувати розширений статичний аналіз шкідливого або підозрілого коду, використовувати дебагери для дослідження поведінки програм у реальному часі, встановлювати точки зупину (breakpoints), аналізувати інструкції мовою assembly, а також відслідковувати зміни в пам'яті й регістрах під час виконання. **Формування компетентностей:** К31, К36, К38, К310, КФ1, КФ2, КФ5, КФ9. **Результати навчання:** РН-2, РН-5, РН-6, РН-7, РН-10, РН-11, РН-20, РН-23. **Рекомендовані джерела:** 1-15.			
Реверс-інжиніринг та дебагінг	**Лекція 9 2 год**	1 бал	Лекція-візуалізація
Розширений статичний аналіз	Практичне заняття 8 2 год	1 бал	Відпрацювання вправ на платформі TryHackMe: Advanced Static Analysis.
Розширений динамічний аналіз: дебагінг	Лабораторна робота 4 2 год	1 бал	Відпрацювання вправ на платформі TryHackMe: Dynamic Analysis: Debugging.
Реверс-інжиніринг та дебагінг	Самостійна робота 6 11 год	4 бали	Самостійне відпрацювання вправ на платформі TryHackMe: Basic Malware RE; Advanced Static Analysis; Dynamic Analysis: Debugging. Відповідь на контрольні питання в GWE.
Тема 7: Анти-реверс-інжиніринг та обхід антивірусних засобів **Знати:** основні техніки анти-реверс-інжинірингу та обфускації, методи, які ускладнюють статичний і динамічний аналіз, принципи роботи антивірусного ПЗ і способи його обходу, зокрема під час впровадження шеллкоду. **Вміти:** розпізнавати й аналізувати антидебаг, антидизасемблінг та інші захисні механізми в коді, застосовувати методи обфускації для приховування логіки програми, створювати або модифікувати шеллкод для обходу антивірусів, тестувати його в ізольованому середовищі та оцінювати ефективність виявлення. **Формування компетентностей:** К31, К36, К38, К310, КФ1, КФ2, КФ5, КФ9. **Результати навчання:** РН-2, РН-5, РН-6, РН-7, РН-10, РН-11, РН-20, РН-23. **Рекомендовані джерела:** 1-15.			
Анти-реверс-інжиніринг та обхід антивірусних засобів	**Лекція 10 2 год**	1 бал	Лекція-візуалізація
Анти-реверс-інжиніринг	Практичне заняття 7.1 2 год	1 бал	Відпрацювання вправ на платформі TryHackMe: Anti-Reverse Engineering.
Обхід антивірусних засобів: шеллкод	Лабораторна робота 5 2 год	1 бал	Відпрацювання вправ на платформі TryHackMe: AV Evasion: Shellcode.
Анти-реверс-інжиніринг та обхід антивірусних засобів	Самостійна робота 7	4 бали	Самостійне відпрацювання вправ на платформі TryHackMe: Signature Evasion; Sandbox Evasion.

	11 год		Відповідь на контрольні питання в GWE.
Тема 8: Електронна пошта та фішинг **Знати:** основи фішингових атак, їх типи (зокрема spear phishing), характерні ознаки фішингових листів, методи доставки шкідливого вмісту через електронну пошту, інструменти для аналізу підозрілих вкладень (наприклад, документів із макросами), а також техніки запобігання фішингу. **Вміти:** виявляти та аналізувати фішингові повідомлення, перевіряти вкладення за допомогою статичного аналізу, використовувати інструменти для дослідження шкідливих документів (наприклад, MalDoc, oledump), розпізнавати ознаки соціальної інженерії, та застосовувати методи профілактики фішингу в організаційному середовищі. **Формування компетентностей:** К31, К36, К38, К310, КФ1, КФ2, КФ5, КФ9. **Результати навчання:** РН-2, РН-5, РН-6, РН-7, РН-10, РН-11, РН-20, РН-23. **Рекомендовані джерела:** 1-15.			
Фішинг, соціальна інженерія та технології аналізу шкідливих електронних повідомлень	**Лекція 11** **2 год**	1 бал	Лекція-візуалізація
Технології протидії фішингу	Практичне заняття 8.1 2 год	1 бал	Відпрацювання вправ на платформі TryHackMe: Phishing Prevention.
Аналіз фішингових листів	Лабораторна робота 6 2 год	1 бал	Відпрацювання вправ на платформі TryHackMe: MalDoc: Static Analysis.
Електронна пошта та фішинг	Самостійна робота 8 11 год	4 бали	Самостійне відпрацювання вправ на платформі TryHackMe: Phishing; Phishing Emails in Action. Відповідь на контрольні питання в GWE.
Тема 9: Сучасні комплексні загрози та методи протидії: APT атаки **Знати:** характерні риси APT-атак (Advanced Persistent Threats), їхні етапи та цілі, тактики і техніки групи APT28 (Fancy Bear), ознаки цільових кібератак, механізми довготривалого прихованого проникнення, а також методи виявлення та реагування на складні загрози. **Вміти:** розпізнавати типові поведінкові шаблони APT-угруповань, аналізувати індикатори компрометації (IoCs), досліджувати ланцюг атаки за моделлю Cyber Kill Chain, використовувати інструменти для виявлення активностей APT-груп, та застосовувати базові методи протидії та мінімізації наслідків таких атак. **Формування компетентностей:** К31, К36, К38, К310, КФ1, КФ2, КФ5, КФ9. **Результати навчання:** РН-2, РН-5, РН-6, РН-7, РН-10, РН-11, РН-20, РН-23. **Рекомендовані джерела:** 1-15.			
Сучасні комплексні кіберзагрози: APT-атаки, C2-інфраструктура та технології протидії — 2 год.	**Лекція 12** **2 год**	1 бал	Лекція-візуалізація
Дослідження APT-атаки	Практичне заняття 9 2 год	1 бал	Відпрацювання вправ на платформі TryHackMe: APT28 in the Snare.
Сучасні комплексні загрози та методи протидії: APT атаки	Самостійна робота 9 8 год	2 бали	Самостійне відпрацювання вправ на платформі TryHackMe: Intro to C2. Відповідь на контрольні питання в GWE.
Залік	Практичне заняття 9.2 2 год	40 балів	Самостійне виконання завдань тесту в GWE.
МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ			
Комп’ютерне обладнання, мережа Інтернет. Віртуальне навчальне середовище.			

Навчальна платформа TryHackMe https://tryhackme.com .

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Технології захисту інформації в інформаційно-телекомуні-каційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с. https://ela.kpi.ua/server/api/core/bitstreams/d99a0045-e907-4d17-afc1-5431f67d2444/content
2. Комплексна безпека інформаційних мережевих систем: навчальний посібник для студентів спеціальності 174 «Автоматизація, комп'ютерноінтегровані технології та робототехніка» / Укладачі: А.Г. Микитишин,М.М. Митник, О.С. Голотенко, В.В. Карташов. – Тернопіль : ФОП Паляниця В.А., 2023. – 324 с. https://elartu.tntu.edu.ua/handle/123456789/889
3. Безпека інформаційних систем [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», освітня програма «Цифрові технології в енергетиці» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 1,98 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2023. – 161 с. https://ela.kpi.ua/server/api/core/bitstreams/71eb3ad4-103b-494a-b80e-d58a49033cd5/content
4. І.А. Терейковський, О.Г. Корченко, В.В. Погорелов. Методи розпізнавання кібератак: розпізнавання комп'ютерних вірусів. Навчальний посібник. Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського». 2022. 127 с. https://files.znu.edu.ua/files/Bibliobooks/Inshi79/0059154.pdf
5. Сучасні інформаційні технології в кібербезпеці : монографія / А. С. Довбиш, В. К. Ободяк, І. В. Шелехов та ін. ; за ред. В. К. Ободяка, І. В. Шелехова. – Суми : Сумський державний університет, 2021. – 348 с. https://essuir.sumdu.edu.ua/bitstream-download/123456789/82619/3/Obodiak_kiberbezpeka.pdf
6. Atacak İ, Kılıc K, Doğru İA. 2022. Android malware detection using hybrid ANFIS architecture with low computational cost convolutional layers. PeerJ Comput. Sci. 8:e1092 http://doi.org/10.7717/peerj-cs.1092
7. Hossain, M.A., Islam, M.S. Enhanced detection of obfuscated malware in memory dumps: a machine learning approach for advanced cybersecurity. Cybersecurity 7, 16 (2024). https://doi.org/10.1186/s42400-024-00205-z
8. Alhussen, A. 2024. Advanced Android Malware Detection through Deep Learning Optimization. Engineering, Technology & Applied Science Research. 14, 3 (Jun. 2024), 14552–14557. DOI: https://doi.org/10.48084/etasr.7443
9. Sergii Banin. Malware detection and classification using low-level features. Thesis for the Degree of Philosophiae Doctor. Norwegian University of Science and Technology. 2023. 263 p. https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/3043791/PhD_Sergii_Banin_NY.pdf?sequence=5&isAllowed=y
10. Luo, Jiale et al. 'Sequence-based Malware Detection Using a Single-bidirectional Graph Embedding and Multi-task Learning Framework'. 1 Jan. 2024 : 141 – 163. https://content.iospress.com/download/journal-of-computer-security/jcs230041?id=journal-of-computer-security%2Fjcs230041
11. Moldovan, Darius & Simona Mirela, Riurean. (2022). Cyber-Security Attacks, Prevention and Malware Detection Application. Journal of Digital Science. 4. 3-19. https://doi.org/10.33847/2686-8296.4.2_1
12. Савченко, В. А., & Бичков, В. В. (2024). Дослідження потенційних уразливостей роутерів CISCO до зовнішніх ін'єкцій. Сучасний захист інформації, 2(58), 6–12. https://doi.org/10.31673/2409-7292.2024.020001.
13. Савченко, В. А. (2024). Дослідження потенційного впливу соціальної інженерії на процеси цифрової трансформації. Зв'язок, 3(169). 12-17. https://doi.org/10.31673/2412-9070.2024.031217
14. Хавер, А. В.,& Савченко, В. А. (2023). Математична модель захисту об'єкта критичної інфраструктури від троянських програм. Сучасний захист інформації, 3(55), 12–21. https://doi.org/10.31673/2409-7292.2023.030002
15. Савченко В. А., Хавер А. В. Метод розрахунку кіберстійкості 2-1 рівнів моделі Purdue проти спеціалізованого технологічного троянського програмного забезпечення. Системи і технології зв'язку, інформатизації та кібербезпеки. 2025, № 7, 147-164. https://doi.org/10.58254/viti.7.2025.14.147

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій, практичних і лабораторних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.

- Якщо здобувач відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації здобувач повинен вказати джерело, використане в ході виконання завдання.

КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є набрання здобувачем 30 балів у сукупності за всіма темами дисципліни.

Форми контролю	**Види навчальної роботи**	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	• Відвідування занять та виконання практичних робіт	26 балів
	• Самостійна робота	34 бали
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Залік***	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Залік: тестування на платформі GWE.	40 балів

Додаткова оцінка

Види навчальної роботи	**Оцінювання**
Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:	
- Тези доповіді на фаховій конференції	3 бали
- Стаття у фаховому виданні категорії Б	5 балів
- Стаття у рецензованому виданні (Scopus, Web of Science)	10 балів
Сертифікат про підвищення кваліфікації за тематикою дисципліни	5 балів

Максимальна кількість додаткових балів, які можуть бути зараховані здобувачу освіти – **10 балів**.

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в заліковій відомості*
90-100	Здобувач демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних і лабораторних занять, при виконанні індивідуальних/контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або Здобувач проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції здобувача в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (А)
82-89	Здобувач демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною.	**Достатній** Забезпечує здобувачу самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами,	Добре / Зараховано (В)

	Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних і лабораторних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	що розглянуті при вивчені дисципліни.	
75-81	Здобувач в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних і лабораторних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (C)
67-74	Здобувач засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача. .	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни.	Задовільно / Зараховано (D)
60-66	Здобувач має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, здобувач з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни.	Задовільно / Зараховано (E)
35-59	Здобувач може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни здобувач виконав, працював він пасивно, його відповіді під час практичних і лабораторних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у здобувача відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни.	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
0-34	Здобувач повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Здобувач не допущений до здачі екзамену/заліку.	**Незадовільний** Здобувач не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни.	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В залікову книжку не проставляється*

ВПЛИВ ПОТУЖНИХ ПОЛІВ НА ЕЛЕКТРОННІ ЗАСОБИ ТА МЕТОДИ ЇХ ЗАХИСТУ **ПОЛІТИКА ДОБРОЧЕСНОСТІ**

Здобувач вищої освіти виконуючи самостійну або індивідуальну роботу повинен дотримуватись політики доброчесності. У разі наявності плагіату в будь-яких видах робіт здобувача, він отримує незадовільну оцінку і повинен повторно виконати завдання, які передбачені у Силабусі.