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

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="3">Савченко Віталій Анатолійович,
доктор технічних наук, професор.</td><td>Контактна інформація лектора (e-mail), код курсу на Google Workspace for Education</td><td colspan="2">e-mail: v.savchenko@duikt.edu.ua
код курсу на Google Workspace for Education –
https://classroom.google.com/c/NzA4MzAxMjcxNDE5?cjc=nkprc4p</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="3">F «Інформаційні технології»</td><td>Рівень вищої освіти</td><td colspan="2">магістр</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="3">F2 Інженерія програмного забезпечення</td><td>Семестр</td><td colspan="2">3</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="3">Інженерія програмного забезпечення</td><td>Тип дисципліни</td><td colspan="2">Обов’язкова</td></tr>
<tr><td rowspan="2">Обсяг:</td><td>Кредитів ECTS</td><td>Годин</td><td colspan="6">За видами занять:</td></tr>
<tr><td>3</td><td>90</td><td>Лекцій
18</td><td>Семінарських занять
–</td><td>Практичних занять
36</td><td>Лабораторних занять
–</td><td colspan="2">Самостійна підготовка
36</td></tr>
<tr><td colspan="9">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td colspan="9">Взаємозв’язок у структурно-логічній схемі</td></tr>
<tr><td colspan="3">Освітні компоненти, які передують вивченню</td><td colspan="6">Дисципліни професійної підготовки</td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="6">Переддипломна практика</td></tr>
<tr><td>Мета курсу:</td><td colspan="8">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.</td></tr>
<tr><td colspan="9">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="5">Soft- skills / Загальні компетентності (ЗК)</td><td colspan="4">Hard-skills / Спеціальні компетентності (СК)</td></tr>
<tr><td colspan="5">ЗК01. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК03. Здатність проводити дослідження на відповідному рівні.
ЗК05. Здатність генерувати нові ідеї (креативність).
ЗК08. Здатність до адаптації та дії в новій ситуації.
ЗК09. Здатність здійснювати професійну діяльність і приймати обґрунтовані рішення, керуючись засадами соціальної відповідальності, правових та етичних норм</td><td colspan="4">СК01. Здатність аналізувати предметні області, формувати, класифікувати вимоги до програмного забезпечення.
СК05. Здатність розробляти, аналізувати та застосовувати специфікації, стандарти, правила і рекомендації в сфері інженерії програмного забезпечення.
СК09. Здатність забезпечувати якість програмного забезпечення.</td></tr>
<tr><td colspan="9">Програмні результати навчання (ПРН)</td></tr>
<tr><td colspan="9">РН01. Знати і застосовувати сучасні професійні стандарти і інші нормативно-правові документи з інженерії програмного забезпечення.
РН02. Оцінювати і вибирати ефективні методи і моделі розроблення, впровадження, супроводу програмного забезпечення та управління відповідними процесами на всіх етапах життєвого циклу.
РН06. Розробляти і оцінювати стратегії проєктування програмних засобів; обґрунтовувати, аналізувати і оцінювати варіанти проектних рішень з точки зору якості кінцевого програмного продукту, ресурсних обмежень та інших факторів.
РН11. Забезпечувати якість на всіх стадіях життєвого циклу програмного забезпечення, у тому числі з використанням релевантних моделей та методів оцінювання, а також засобів автоматизованого тестування і верифікації програмного забезпечення.
РН16. Планувати, організовувати та здійснювати тестування, верифікацію та валідацію програмного забезпечення.</td></tr>
<tr><td colspan="9">ОРГАНІЗАЦІЯ НАВЧАННЯ</td></tr>
</table>

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 **Рекомендовані джерела:** 1-16.			
Вступ. Основи виявлення уразливостей та шкідливого програмного забезпечення	**Лекція 1 2 год**		Лекція-візуалізація
Початок роботи на платформі TryHackMe	Практичне заняття 1.1 2 год	2 бали	Відпрацювання вправ на платформі TryHackMe: Getting Started; Offensive Security Intro; Defensive Security Intro; Search Skills.
Основи аналізу уразливостей та шкідливого програмного забезпечення	Практичне заняття 1.2 2 год	2 бали	Відпрацювання вправ на платформі TryHackMe: Vulnerabilities 101; Intro to Malware Analysis.
Основи виявлення уразливостей та шкідливого програмного забезпечення	Самостійна робота 1 11 год	3 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 **Рекомендовані джерела:** 1-16.			
Технології мережевої безпеки та аналізу трафіку	**Лекція 2 2 год**		Лекція-візуалізація
Сканування мережі з Nmap	Практичне заняття 2.1 2 год	2 бали	Відпрацювання вправ на платформі TryHackMe: Nmap: The Basics; Nmap Live Host Discovery.
Аналіз трафіку з Wireshark	Практичне заняття 2.2 2 год	2 бали	Відпрацювання вправ на платформі TryHackMe: Wireshark: The Basics.
Технології мережевої безпеки та аналізу трафіку	Самостійна робота 2 11 год	3 бали	Самостійне відпрацювання вправ на платформі TryHackMe: Networking Secure Protocols; Network Security Solutions; Firewalls Відповідь на контрольні питання в GWE.
Тема 3: Уразливості та захист операційних систем (Windows, Linux) **Рекомендовані джерела:** 1-16.			
Уразливості та захист операційних систем (Windows, Linux)	**Лекція 3 2 год**		Лекція-візуалізація
Ескалація привілеїв у Windows	Практичне заняття 3.1 2 год	2 бали	Відпрацювання вправ на платформі TryHackMe: Windows Privilege Escalation.
Ескалація привілеїв у Linux	Практичне заняття 3.2 2 год	2 бали	Відпрацювання вправ на платформі TryHackMe: Linux Privilege Escalation.
Уразливості та захист операційних систем (Windows, Linux)	Самостійна робота 3 11 год	3 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 **Рекомендовані джерела:** 1-16.			
Web-уразливості: методи виявлення та протидії	**Лекція 4** **2 год**		Лекція-візуалізація
Виявлення та дослідження поширених Web-уразливостей	Практичне заняття 4.1 2 год	2 бали	Відпрацювання вправ на платформі TryHackMe: OWASP Top 10 – 2021.
Основи тестування Web-додатків з Burp Suite	Практичне заняття 4.2 2 год	2 бали	Відпрацювання вправ на платформі TryHackMe: Burp Suite: The Basics.
Web-уразливості: методи виявлення та протидії	Самостійна робота 4 11 год	3 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 **Рекомендовані джерела:** 1-16.			
Виявлення та аналіз шкідливих програм	**Лекція 5** **2 год**		Лекція-візуалізація
Базовий статичний аналіз	Практичне заняття 5.1 2 год	2 бали	Відпрацювання вправ на платформі TryHackMe: Basic Static Analysis.
Базовий динамічний аналіз	Практичне заняття 5.2 2 год	2 бали	Відпрацювання вправ на платформі TryHackMe: Basic Dynamic Analysis.
Виявлення та аналіз шкідливих програм	Самостійна робота 5 11 год	3 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 **Рекомендовані джерела:** 1-16.			
Реверс-інжиніринг та дебагінг	**Лекція 6** **2 год**		Лекція-візуалізація
Розширений статичний аналіз	Практичне заняття 6.1 2 год	2 бали	Відпрацювання вправ на платформі TryHackMe: Advanced Static Analysis.
Розширений динамічний аналіз: дебагінг	Практичне заняття 6.2 2 год	2 бали	Відпрацювання вправ на платформі TryHackMe: Dynamic Analysis: Debugging.
Реверс-інжиніринг та дебагінг	Самостійна робота 6 11 год	3 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 **Рекомендовані джерела:** 1-16.			
Анти-реверс-інжиніринг та обхід антивірусних засобів	**Лекція 7** **2 год**		Лекція-візуалізація
Анти-реверс-інжиніринг	Практичне заняття 7.1 2 год	2 бали	Відпрацювання вправ на платформі TryHackMe: Anti-Reverse Engineering.
Обхід антивірусних засобів: шеллкод	Практичне заняття 7.2 2 год	2 бали	Відпрацювання вправ на платформі TryHackMe: AV Evasion: Shellcode.
Анти-реверс-інжиніринг та обхід антивірусних засобів	Самостійна робота 7 11 год	3 бали	Самостійне відпрацювання вправ на платформі TryHackMe: Signature Evasion; Sandbox Evasion. Відповідь на контрольні питання в GWE.
Тема 8: Електронна пошта та фішинг **Рекомендовані джерела:** 1-16.			
Електронна пошта та фішинг	**Лекція 8** **2 год**		Лекція-візуалізація
Технології протидії фішингу	Практичне заняття 8.1 2 год	2 бали	Відпрацювання вправ на платформі TryHackMe: Phishing Prevention.
Аналіз фішингових листів	Практичне заняття 8.2 2 год	2 бали	Відпрацювання вправ на платформі TryHackMe: MalDoc: Static Analysis.
Електронна пошта та фішинг	Самостійна робота 8 11 год	3 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 **Рекомендовані джерела:** 1-16.			
Сучасні комплексні загрози та методи протидії: APT атаки	**Лекція 9** **2 год**		Лекція-візуалізація
Дослідження APT-атаки	Практичне заняття 9.1 2 год	2 бали	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.
Іспит	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. (2025). 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
16. Савченко В.А, Хавер А.В. (2025). Оцінка впливу програмних інструментів на основі технологій штучного інтелекту на ресурсну ефективність щодо проведення деструктивних кібероперацііпо відношенню до об'єктів критичної інфраструктури. Сучасний захист інформації, 3(63), 165–175. https://doi.org/10.31673/2409-7292.2025.031896

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 і семінарських 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	●Виконання практичних робіт	34 бали
	●Самостійна робота	26 балів
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Іспит***	Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Іспит: 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 екзаменаційній 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 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	**Достатній** Забезпечує здобувачу самостійне	Добре / Зараховано (В)

	вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, 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 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 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*

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.