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

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Савченко Віталій Анатолійович,
доктор технічних наук, професор,
професор кафедри Управління кібербезпекою та захистом інформації</td><td colspan="2">Контактна інформація лектора (e-mail), сторінка курсу в GWE</td><td colspan="2">e-mail: v.savchenko@duikt.edu.ua
сторінка курсу в Classroom -
https://classroom.google.com/c/NzA4MzAxMjcxNDE5?cjc=nkprc4p
код доступу - nkprc4p</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="2"></td><td colspan="2">Рівень вищої освіти</td><td colspan="2">магістр</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="2"></td><td colspan="2">Семестр</td><td colspan="2"></td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="2"></td><td colspan="2">Тип дисципліни</td><td colspan="2">Вибіркова компонента</td></tr>
<tr><td rowspan="3">Обсяг:</td><td>Кредитів ECTS</td><td>Годин</td><td colspan="6">За видами занять:</td></tr>
<tr><td></td><td></td><td>Лекцій</td><td>Семінарських занять</td><td>Практичних занять</td><td>Лабораторних занять</td><td>Самостійна підготовка</td></tr>
<tr><td>5</td><td>150</td><td>18</td><td>–</td><td>36</td><td>–</td><td>96</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"></td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="6"></td></tr>
<tr><td>Мета курсу:</td><td colspan="8">Формування знань та вмінь щодо застосування методів та засобів виявлення злоякісного програмного забезпечення інформаційної системи організації їх аналіз, виявлення недоліків та протиріч для постановки та вирішення наукових завдань</td></tr>
<tr><td colspan="9">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="4">Soft- skills / Загальні компетентності (ЗК)</td><td colspan="5">Hard-skills / Спеціальні компетентності (СК)</td></tr>
<tr><td colspan="4">Здатність застосовувати знання у практичних ситуаціях.
Здатність оцінювати та забезпечувати якість виконуваних робіт
Знання та розуміння предметної області і професійної діяльності.
Здатність використовувати інформаційні та комунікаційні технології.
Здатність застосовувати кращі практики у професійній діяльності.</td><td colspan="5">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.
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.
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.
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.</td></tr>
<tr><td colspan="9">Програмні результати навчання (ПРН)</td></tr>
<tr><td colspan="9">Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або</td></tr>
</table>

мультидисциплінарних контекстах.
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.
Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
Ставити та вирішувати складні інженерно -прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
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.

ОРГАНІЗАЦІЯНАВЧАННЯ

Тема,опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Тема 1: Поняття «Шкідливе програмне забезпечення». Комп'ютерні віруси. Статичний та динамічний аналіз шкідливих програм. **Знати**: Основні поняття щодо безпеки інформаційної системи. Поняття «шкідливе програмне забезпечення». Класифікація комп'ютерних вірусів. Основні комп'ютерні віруси (файлові, завантажувальні, резидентні, поліморфні, стелс-віруси, макро-віруси). Класифікація технологій виявлення вірусів. Способи захисту від вірусів. Зміст статичного та динамічного аналізу шкідливих програм. Інструменти та шаблони виявлення, що використовуються при аналізі шкідливих програм. Ефективні програми боротьби з вірусами. **Вміти**: Аналізувати прояви та ознаки шкідливого ПЗ. Визначати види шкідливого ПЗ. Проводити пошук шкідливого ПЗ за допомогою антивірусних програм. Застосовувати методи виявлення ШПЗ за допомогою професійних пакетів антивірусних інструментів. Застосовувати статичний та динамічний аналіз діагностування комп'ютерних систем на наявність ШПЗ. **Рекомендовані джерела:** 1-15.			
Шкідливе програмне забезпечення. Проблема виявлення та протидії шкідливому програмному забезпеченню в інформаційних системах.	Лекція 1 2 год		Лекція-візуалізація
Виявлення та видалення зловмисних програм.	Практичне заняття 1 4 год	4 бали	Оволодіти навичками виявлення та видалення зловмисних програм за допомогою сучасних інструментів. Ознайомитися з процесами ідентифікації, аналізу та очищення системи від шкідливого ПЗ.
Комп'ютерні віруси (частина 1).	Лекція 2 2 год		Лекція-візуалізація, експрес-опитування здобувачів.
Аналіз шкідливого програмного забезпечення.	Практичне заняття 2 4 год	4 бали	Оволодіти навичками статичного аналізу зловмисних програм за допомогою сучасних інструментів. Ознайомитися з процесами ідентифікації, аналізу та очищення системи від шкідливого ПЗ.

Комп’ютерні віруси (частина 2).	Лекція 3 2 год		Лекція-візуалізація, експрес-опитування здобувачів.
Динамічний аналіз шкідливих програм.	Практичне заняття 3 4 год	4 бали	Ознайомитися з методами та технологіями динамічного аналізу ШПЗ на платформі OpenCTI, призначеній для надання організаціям засобів керування CTI за допомогою зберігання, аналізу, візуалізації та представлення загроз, зловмисного програмного забезпечення та індикаторів компрометації.
Тема 1: Поняття «Шкідливе програмне забезпечення». Комп’ютерні віруси. Статичний та динамічний аналіз шкідливих програм.	Самостійна робота 1 12 год	8 балів	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекціями та практичними заняттями. Отримати навички виявлення ознак різновидів ШПЗ.
Тема 2: Шкідливе програмне забезпечення. Основні ознаки шкідливого програмного забезпечення. Методи боротьби з шкідливим програмним забезпеченням. **Знати:** Шкідливе програмне забезпечення (Spyware, Ad-ware, Malware, мережеві хробаки та інші види ШПЗ**).** Основні уразливості програмного забезпечення. Методи аналізу експлойтів (віддалений експлойт , локальний експлойт). Аналізатори вихідного коду програми. Фішинг. Визначення фішингу, види фішингових атак, технології захисту від фішингу. Ботнети. Визначення та зміст ботнетів. Методи виявлення ботнет-програм; захист від ботнетів. Реверс-інжиніринг. Аналіз програм з використанням дизасемблера (інтерактивні, автоматичні). Покращене розпакування. **Вміти**: Аналізувати прояви та ознаки шкідливого ПЗ. Визначати види шкідливого ПЗ: комп'ютерний вірус, троянська програма, мережевий черв'як, руткіти. Проводити моніторинг факту наявності шкідливого ПЗ. Проводити аналіз експлойтів (фрагментів коду, які використовують вразливості в ПЗ та ОС для здійснення атаки на систему). Здійснювати заходи для протидії фішингу. Виявляти та протидіяти ботнетам. Застосовувати технології реверс-інжинірингу. Здійснювати покращене розпакування. **Рекомендовані джерела:** 1-15.			
Шкідливе програмне забезпечення.	Лекція 4 2 год		Лекція-візуалізація, експрес-опитування здобувачів.
Аналіз проломів в програмному забезпеченні.	Практичне заняття 4 4 год	4 бали	Ознайомитися з основами мережевої безпеки та аналізу трафіку, а також з основними концепціями цих напрямів, щоб зрозуміти аналіз трафіку/пакетів.
Фішинг. Методи та засоби протидії фішингу	Лекція 5 2 год		Лекція-візуалізація, експрес-опитування здобувачів.
Реверс інжиніринг	Практичне заняття 5 4 год	4 бали	Ознайомитися з основами реверс-інжинірингу, а також з основними концепціями цих напрямів, щоб зрозуміти процес аналізу шкідливого програмного коду.
Ботнети. Методи та засоби протидії мережевим атакам.	Лекція 6 2 год		Лекція-візуалізація, експрес-опитування здобувачів.
Покращене розпакування	Практичне заняття 6 4 год	4 бали	Ознайомитися з основами кодування шелл-коду, упаковки, підшивки та шифрувальників, а також з основними концепціями процесу аналізу шелл-коду, упаковки, підшивок та шифрувальників.
Тема 2: Шкідливе програмне забезпечення. Основні ознаки шкідливого програмного забезпечення. Методи боротьби з	Самостійна робота 2	8 балів	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекціями та

шкідливим програмним забезпеченням.	12 год		практичними заняттями. Отримати навички застосування методів боротьби з ШПЗ.
Тема 3: Атаки в соціальних мережах. Руткіти. Шкідливе програмне забезпечення мобільних пристроїв. **Знати:** Типи атак в соціальних мережах. Методи соціальної інженерії. Руткіти: механізми проникнення, маскування руткітів на ПК та методи захисту від них. Головні загрози для мобільних пристроїв. Принципи та інструменти безпеки Apple та Android. **Вміти**: Аналізувати прояви та ознаки шкідливого ПЗ. Протидіяти атакам в соціальних мережах. Виявляти руткіти та здіснювати заходи протидії руткітам. Застосовувати інструменти захисту ОС Apple та Android. **Рекомендовані джерела:** 1-15.			
Кібератаки в соціальних мережах	Лекція 7 2 год		Лекція-візуалізація, експрес-опитування здобувачів.
Руткіти	Практичне заняття 7 4 год	4 бали	Навчитися використовувати інструменти Sysinternals для аналізу систем або програм Windows.
Шкідливе програмне забезпечення мобільних пристроїв.	Лекція 8 2 год		Лекція-візуалізація, експрес-опитування здобувачів.
Виявлення ШПЗ у мобільних пристроях.	Практичне заняття 8 4 год	4 бали	Отримати навички аналізу шкідливого програмного забезпечення для мобільних пристроїв на основі Mobile Malware Analysis.
Сучасні рішення для виявлення шкідливих програм.	Лекція 9 2 год		Лекція-візуалізація, експрес-опитування здобувачів.
Основи моделювання загроз.	Практичне заняття 9 4 год	4 бали	Отримати навички досягнення кіберстійкості шляхом моделювання загроз з Threat Modelling. **Залік.**
Тема 3: Атаки в соціальних мережах. Руткіти. Шкідливе програмне забезпечення мобільних пристроїв.	Самостійна робота 2 12 год	8 балів	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекціями та практичними заняттями. Отримати навички протидії атакам в соціальних мережах, руткітам та ШПЗ мобільних пристроїв.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Комп’ютерне обладнання, мережа Інтернет. Віртуальне навчальне середовище. Навчальна платформа TryHackMe.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Козачок В.А., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів – Київ: ДУТ ННІЗІ, 2020. – 167 с. https://duikt.edu.ua/uploads/l_2225_57006111.pdf
2. 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
3. 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
4. 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
5. 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
6. 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
7. 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
8. 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
9. 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
10. 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
11. 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
12. 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
13. 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.
14. 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
15. 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

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	36 балів
	• Самостійна робота	24 бали
ПІДСУМКОВЕ ОЦІНЮВАННЯ	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків.	40 балів

Залік	Залік: оцінюється завчасно виконане Ессе.	

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.	5 балів
- Стаття в іноземному рецензованому виданні.	10 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 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 (A)
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. 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.	**Достатній** Забезпечує здобувачу самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни.	Добре / Зараховано (B)
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 /	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (C)

	контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.		
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.