

## СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

### «ТЕХНОЛОГІЯ ВИЯВЛЕННЯ УРАЗЛИВОСТЕЙ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ WEB-РЕСУРСІВ»

<b>Лектор курсу</b>		Борсуковський Юрій Володимирович, кандидат технічних наук, доцент		<b>Контактна інформація лектора (e-mail), сторінка курсу в Moodle</b>		e-mail: ikbdut@gmail.com; сторінка курсу в Moodle – https://dn.dut.edu.ua/course/view.php	
<b>Галузь знань</b>		12 Інформаційні технології		<b>Рівень вищої освіти</b>		другий (магістерський)	
<b>Спеціальність</b>		125 «Кібербезпека»		<b>Семестр</b>		4	
<b>Освітня програма</b>		Інформаційна та кібернетична безпека		<b>Тип дисципліни</b>		Вибіркова компонента	
<b>Обсяг:</b>	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	150	18	-	18	18	96

#### АНОТАЦІЯ КУРСУ

##### Взаємозв'язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	1. Дисципліни професійної підготовки
Освітні компоненти для яких є базовою	Кваліфікаційна робота
<b>Мета курсу:</b>	Формування знань та вмінь застосування методів та засобів виявлення уразливостей WEB-ресурсів інформаційної системи організації, виявлення недоліків та протиріч для проведення наукових досліджень

##### Компетентності відповідно до освітньої програми

Soft- skills / Загальні компетентності (ЗК)	Hard-skills / Спеціальні компетентності (СК)
<p>К31. Здатність застосовувати знання у практичних ситуаціях.</p> <p>К32. Здатність проводити дослідження на відповідному рівні.</p> <p>К34. Здатність оцінювати та забезпечувати якість виконуваних робіт.</p> <p>К36. Знання та розуміння предметної області і професійної діяльності.</p> <p>К37. Володіння навичками критичного мислення.</p> <p>К38. Здатність використовувати інформаційні та комунікаційні технології.</p> <p>К39. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.</p> <p>К310. Здатність застосовувати кращі практики у професійній діяльності.</p>	<p>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.</p> <p>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.</p> <p>КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.</p>

КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

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.

КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. .

#### **Програмні результати навчання (ПРН)**

ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

ПРН3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

ПРН5. 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.

ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

ПРН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

- PH10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
- PH12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
- PH13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
- PH15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
- PH16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
- PH17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
- PH18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки.
- PH19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
- PH20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
- PH21. Використовувати методи натурального, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
- PH22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
- PH23. 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
<b>Змістовий модуль 1. Сучасні аспекти технологій виявлення вразливостей та забезпечення безпеки WEB-ресурсів</b>			
<p><b>Тема 1.</b> Інформаційні ресурси гетерогенної корпоративної мережі (ГКМ). Основні поняття щодо безпеки WEB-ресурсів та WEB-додатків. Розвідка веб-додатків. Структура сучасних веб-додатків</p> <p><b>Знати:</b></p> <ol style="list-style-type: none"> <li>1. Основні поняття, види мереж, особливості функціонування.</li> <li>2. Перелік номенклатури засобів ТЗІ щодо сучасної нормативно-правової бази.</li> <li>3. Функціональні профілі.</li> <li>4. Характеристики WEB-ресурсів.</li> <li>5. Основні поняття щодо безпеки WEB-ресурсів.</li> <li>6. Розвідка веб-додатків.</li> </ol> <p><b>Вміти:</b></p> <ol style="list-style-type: none"> <li>1. Оперувати поняттями процесу управління вразливістю - стандарт NIST SP 800.</li> <li>2. Оперування понятійним апаратом щодо ТВУЗБ WEB-ресурсів.</li> <li>3. Застосовувати законодавчу, нормативно-правову базу щодо виявлення загроз WEB-ресурсів.</li> </ol> <p><b>Формування компетенцій:</b> КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7</p> <p><b>Програмні результати навчання:</b> РН-18 - РН-19, РН-20</p> <p><b>Рекомендовані джерела:</b> 1-24</p>	<p>Лекція 1 4 год</p> <p>Практичне заняття 1 2 год</p>	2*	<p>Лекція-візуалізація</p> <p>Нормативно-правова база, міжнародні документи в напрямку забезпечення безпеки WEB-ресурсів. Методи збору інформації. Карта веб-додатка.</p>
<p>Тема 1. Політика тестування та налаштування сканування вразливостей за допомогою WEB Application Scanning. Пошук субдоменів</p> <p>Вміти:</p> <ol style="list-style-type: none"> <li>1. Основні функції та напрями реалізації WEB Application Scanning.</li> <li>2. Використання можливостей the scanner setup wizard.</li> <li>3. Testing strategies.</li> </ol>	<p>Лабораторне заняття 1 2 год</p>	5*	<p>Визначення політика тестування та налаштування параметрів сканування вразливостей за допомогою WEB Application Scanning.</p>

<p>Формування компетенцій: КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7</p> <p>Програмні результати навчання: РН-1 - РН-19, РН-20, РН-22, РН-23</p> <p>Рекомендовані джерела: 1-24</p>			
<p><b>Тема 2.</b> Мережеве обладнання та середовища передачі інформації в корпоративних системах. Пошук слабких місць в архітектурі додатків. Вимоги та механізми ЗІ WEB-систем від НСД</p> <p><b>Знати:</b></p> <ol style="list-style-type: none"> <li>1. Аналіз актуальних проблем та нормативної бази щодо ЗІ WEB-систем.</li> <li>2. Технічні вимоги за критеріями ТЗІ відповідно до функціонального профілю з рівнем гарантій Г-2.</li> <li>3. Механізми ЗІ управління доступом до ресурсів ГКМ.</li> <li>4. Структура сучасних веб-додатків.</li> </ol> <p><b>Вміти:</b></p> <ol style="list-style-type: none"> <li>1. Проводити оцінку ризиків ІБ щодо забезпечення безпеки WEB-ресурсів.</li> <li>2. Застосовувати законодавчу, нормативно-правову базу в виявленні, прогнозуванні, оцінюванні загроз WEB-ресурсів.</li> </ol> <p><b>Формування компетенцій:</b> КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7</p> <p><b>Програмні результати навчання:</b> РН-18 - РН-19, РН-20</p> <p><b>Рекомендовані джерела:</b> 1-19</p>	<p>Лекція 2 4 год</p> <hr/> <p>Практичне заняття 2 2 год</p>	<p>2*</p>	<p>Лекція-візуалізація</p> <hr/> <p>Аналіз української нормативно-правової бази та міжнародних стандартів в напрямку забезпечення безпеки WEB-ресурсів. Основні версії додатків. REST API. Формат JSON.</p>
<p><b>Тема 2.</b> Сканування захищеності WEB-ресурсів за допомогою WEB Application Scanning. Способи управління етапом аналізу</p> <p><b>Вміти:</b></p> <ol style="list-style-type: none"> <li>1. Операції, що виконуються під час сканування.</li> <li>2. Способи управління етапом аналізу вручну і експорт результатів сканування.</li> </ol> <p><b>Формування компетенцій:</b> КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7</p> <p><b>Програмні результати навчання:</b> РН-1 - РН-19, РН-20, РН-22, РН-23</p> <p><b>Рекомендовані джерела:</b> 1-24</p>	<p>Лабораторне заняття 2 2 год</p>	<p>5*</p>	<p>Проведення сканування захищеності WEB-ресурсів за допомогою WEB Application Scanning. Способи управління етапом аналізу.</p>

<p><b>Тема 3.</b> Уразливості та дестабілізуючі чинники інформаційного простору. Технології виявлення вразливостей WEB-ресурсів. Типові методи атак на веб-додатки</p> <p><b>Знати:</b></p> <ol style="list-style-type: none"> <li>1. Основні поняття, види мереж, особливості функціонування.</li> <li>2. Перелік номенклатури засобів ТЗІ щодо сучасної нормативно-правової бази.</li> <li>3. Функціональні профілі.</li> <li>4. Характеристики WEB-ресурсів.</li> <li>5. Основні поняття щодо безпеки WEB-ресурсів.</li> <li>6. Структура сучасних веб-додатків.</li> </ol> <p><b>Вміти:</b></p> <ol style="list-style-type: none"> <li>1. Впроваджувати законодавчу, НПБ щодо виявлення, прогнозування, оцінювання загроз WEB-ресурсів до вибору раціональних технологій безпеки WEB-ресурсів.</li> </ol> <p><b>Формування компетенцій:</b> КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7</p> <p><b>Програмні результати навчання:</b> РН-18 - РН-20, РН-22, РН-23</p> <p><b>Рекомендовані джерела:</b> 1-24</p>	<p>Лекція 3 4 год</p> <p>Практичне заняття 3 2 год</p>	<p>6*</p>	<p>Лекція-візуалізація</p> <p>Аналіз української нормативно-правової бази та міжнародних стандартів в напрямку забезпечення безпеки WEB-ресурсів. Змінні javascript і їх область видимості. Функції javascript. Контекст javascript. Прототипне спадкування javascript. Асинхронне виконання коду javascript. Фреймворки для SPA. Системи аутентифікації і авторизації. Веб-сервери. Бази даних на стороні сервера. Зберігання даних на стороні клієнта.</p>
<p><b>Тема 3.</b> Аналіз API. Базова конфігурація сканера для оцінки захищеності WEB-ресурсів за допомогою WEB Application Scanning</p> <p><b>Вміти:</b></p> <ol style="list-style-type: none"> <li>1. Сканування WEB-служб.</li> <li>2. Configuring the scan, Running the scan, Reviewing Scan Results WEB Application Scanning.</li> </ol> <p><b>Формування компетенцій:</b> КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7</p> <p><b>Програмні результати навчання:</b> РН-1 - РН-19, РН-20, РН-22, РН-23</p> <p><b>Рекомендовані джерела:</b> 1-24</p>	<p>Лабораторне заняття 3 2 год</p>	<p>5*</p>	<p>Проведення конфігурування сканера для оцінки захищеності WEB-ресурсів за допомогою WEB Application Scanning.</p>
<p><b>Тема 3.</b> Уразливості та дестабілізуючі чинники інформаційного простору. Технології виявлення вразливостей WEB-ресурсів</p>	<p>Самостійна робота</p>		<p>Аналіз технологій виявлення вразливостей WEB-ресурсів. Структура сучасних веб-додатків.</p>

<p><b>Тема 4.</b> Інформаційні ресурси гетерогенної корпоративної мережі (ГКМ). Основні поняття щодо безпеки WEB-ресурсів та WEB-додатків. Типові методи атак на веб-додатки</p> <p><b>Знати:</b></p> <ol style="list-style-type: none"> <li>1. Основні поняття, види мереж, особливості функціонування.</li> <li>2. Перелік номенклатури засобів ТЗІ щодо сучасної нормативно-правової бази.</li> <li>3. Функціональні профілі.</li> <li>4. Характеристики WEB-ресурсів.</li> <li>5. Основні поняття щодо безпеки WEB-ресурсів.</li> <li>6. Аналіз API.</li> </ol> <p><b>Вміти:</b></p> <ol style="list-style-type: none"> <li>1. Методи оцінки вразливостей на основі the Ten Most Critical WEB Application Security Risks.</li> <li>2. Найбільш актуальні методи і ЗЗІ від загроз WEB-додатків.</li> </ol> <p><b>Формування компетенцій:</b> КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7</p> <p><b>Програмні результати навчання:</b> РН-18, РН-20, РН-21</p> <p><b>Рекомендовані джерела:</b> 1-24</p>	<p>Лекція 4 4 год</p> <p>Практичне заняття 4 2 год</p>	<p>6*</p>	<p>Лекція-візуалізація</p> <p>Середа тестування захищеності WEB-додатків сканерами класу AST systems. WEB-сканери вразливостей провідних виробників. Аналіз API. Виявлення кінцевої точки- механізми аутентифікації. Різновиди кінцевих точок- базові різновиди. Різновиди кінцевих точок- спеціалізовані різновиди.</p>
<p><b>Тема 4.</b> Повне сканування, налаштування сканування вразливостей WEB Application Scanning. Вибір методів сканування</p> <p><b>Вміти:</b></p> <ol style="list-style-type: none"> <li>1. Визначати конфігурацію сканування.</li> <li>2. Проводити вибір та застосовувати analysis systems DAST, SAST scanning.</li> </ol> <p><b>Формування компетенцій:</b> КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7</p> <p><b>Програмні результати навчання:</b> РН-1 - РН-19, РН-20, РН-22, РН-23</p> <p><b>Рекомендовані джерела:</b> 1-24</p>	<p>Лабораторне заняття 4 2 год</p>	<p>5*</p>	<p>Проведення повного сканування, налаштування сканування вразливостей WEB Application Scanning. Вибір базових методів сканування.</p>
<p><b>Тема 4.</b> Інформаційні ресурси гетерогенної корпоративної мережі (ГКМ). Основні поняття щодо безпеки WEB-ресурсів та WEB-додатків. Пошук слабких місць в архітектурі додатків. Міжсайтовий скриптинг</p>	<p>Самостійна робота</p>		<p>Аналіз технологій забезпечення безпеки WEB-ресурсів та WEB-додатків. Аналіз API.</p>

<p><b>Тема 5.</b> Безпека рівня мережевої інфраструктури. Захист WEB-додатків і сучасні напрями розвитку інформаційної та кібербезпеки</p> <p><b>Знати:</b></p> <ol style="list-style-type: none"> <li>1. Сучасні методи тестування WEB-ресурсів від руйнівних кіберзагроз.</li> <li>2. Security vulnerability testing для WEB services.</li> <li>3. Основні уразливості мережевих WEB-додатків.</li> <li>4. Методи усунення вразливостей.</li> </ol> <p><b>Вміти:</b></p> <ol style="list-style-type: none"> <li>1. Загальні принципи, що реалізовані в сканерах вразливостей.</li> <li>2. Класифікація вразливостей відповідно до WASC, небезпечні атаки на WEB-ресурси.</li> <li>3. Принципи роботи WEB Application Scanning.</li> <li>4. Виявлення сторонніх залежностей.</li> </ol> <p><b>Формування компетенцій:</b> КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7</p> <p><b>Програмні результати навчання:</b> РН-1 - РН-19, РН-20, РН-21</p> <p><b>Рекомендовані джерела:</b> 1-24</p>	<p>Лекція 5 4 год</p> <p>Практичне заняття 5 2 год</p>	6*	<p>Лекція-візуалізація</p> <p>Тестування захищеності WEB-додатків AST systems. WEB-сканер вразливостей - WEB Application Scanning. Клієнтські фреймворки- фреймворки для односторінкових додатків. Клієнтські фреймворки- бібліотеки JavaScript. Клієнтські фреймворки- бібліотеки CSS. Фреймворки на стороні сервера- заголовки. Фреймворки на стороні сервера- стандартні повідомлення про помилку і сторінки 404. Фреймворки на стороні сервера- бази даних.</p>
<p><b>Тема 5.</b> Інтегрований клієнт GSC та файл WSDL WEB-служби</p> <p><b>Вміти:</b></p> <ol style="list-style-type: none"> <li>1. Інтегрований клієнт GSC</li> <li>2. Склад, призначення та функції components.</li> </ol> <p><b>Формування компетенцій:</b> КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7</p> <p><b>Програмні результати навчання:</b> РН-1 - РН-19, РН-20, РН-22, РН-23</p> <p><b>Рекомендовані джерела:</b> 1-24</p>	Лабораторне заняття 5 2 год	5*	Інтегрований клієнт GSC та файл WSDL WEB-служби.
<p><b>Тема 5.</b> Безпека рівня мережевої інфраструктури. Захист WEB-додатків і сучасні напрями розвитку інформаційної та кібербезпеки</p>	Самостійна робота		Аналіз технологій захисту WEB-додатків. Виявлення сторонніх залежностей.
<p><b>Тема 6.</b> Методи та технології забезпечення ІБ у WEB-додатках. Автентифікація та ідентифікація сесій WEB-додатків. Пошук слабких місць в архітектурі додатків. Підробка міжсайтових запитів.</p> <p><b>Знати:</b></p>	<p>Лекція 6 4 год</p> <p>Практичне заняття 6 2 год</p>	6*	<p>Лекція-візуалізація</p> <p>Нормативно-правова база, міжнародні документи в напрямку забезпечення безпеки WEB-ресурсів. Ознаки безпечної і небезпечної архітектури.</p>



<ol style="list-style-type: none"> <li>1. Методи автентифікації WEB-додатків.</li> <li>2. Уразливості автентифікації.</li> <li>3. Передбачуване значення ідентифікатора session.</li> <li>4. Недостатня авторизація.</li> <li>5. Пошук слабких місць в архітектурі додатків.</li> </ol> <p><b>Вміти:</b></p> <ol style="list-style-type: none"> <li>1. Основні функції і процедури роботи WEB Application Scanning.</li> <li>2. WEB Application Scanning full scan, додаткові функції.</li> </ol> <p><b>Формування компетенцій:</b> КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7</p> <p><b>Програмні результати навчання:</b> РН-1 - РН-19, РН-20, РН-21</p> <p><b>Рекомендовані джерела:</b> 1-24</p>			<p>Рівні безпеки. Запозичення і перекроювання.</p>
<p><b>Тема 15.</b> Утиліти Power Tools. Інтегровані засоби сканування WEB-сервісів</p> <p><b>Вміти:</b></p> <ol style="list-style-type: none"> <li>1. Визначати конфігурацію сканування.</li> <li>2. Проводити вибір та застосовувати analysis systems DAST, SAST scanning.</li> </ol> <p><b>Формування компетенцій:</b> КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7</p> <p><b>Програмні результати навчання:</b> РН-1 - РН-19, РН-20, РН-22, РН-23</p> <p><b>Рекомендовані джерела:</b> 1-24</p>	<p>Лабораторне заняття 6 2 год</p>	<p>6*</p>	<p>Використання інтегрованих засобів сканування WEB-сервісів.</p>
<p><b>Тема 6.</b> Методи та технології забезпечення ІБ у WEB-додатках. Автентифікація та ідентифікація сесій WEB-додатків</p>	<p>Самостійна робота</p>		<p>Методи та технології забезпечення кібернетичної та інформаційної безпеки у WEB-додатках. Аналіз методів пошуку слабких місць в архітектурі додатків.</p>
<p><b>Тема 7.</b> Мульти-користувальницькі рішення для забезпечення безпеки WEB-додатків що реалізовані в AST systems. Сканери вразливостей WEB Application Scanning. Атака на зовнішні сутності. Перевірка безпеки коду</p> <p><b>Знати:</b></p> <ol style="list-style-type: none"> <li>1. Основні підходи та принципи роботи.</li> <li>2. Базові функції та напрями реалізації WEB Application Scanning.</li> <li>3. Black-box scanning, white-box scanning, glass box scanning.</li> </ol>	<p>Лекція 7 4 год</p> <p>Практичне заняття 7 2 год</p>	<p>6*</p>	<p>Лекція-візуалізація</p> <p>Основи виявлення вразливостей WEB-додатків за допомогою WEB Application Scanning. Міжсайтовий скриптинг (XSS). Підробка міжсайтових запитів (CSRF). Атака на зовнішні сутності XML (XXE). Впровадження коду. Відмова в обслуговуванні (DoS). Експлуатація сторонніх залежностей.</p>

<p>4. Особливості тестування WEB-додатків. 5. Типові методи атак на веб-додатки.</p> <p><b>Вміти:</b></p> <ol style="list-style-type: none"> <li>1. Налаштування сканування та політики WEB Application Scanning.</li> <li>2. Автоматичний потік операцій сканування WEB Application Scanning.</li> </ol> <p><b>Формування компетенцій:</b> КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7</p> <p><b>Програмні результати навчання:</b> PH-1 - PH-19, PH-20, PH-22, PH-23</p> <p><b>Рекомендовані джерела:</b> 1-24</p>			
<p><b>Тема 16.</b> Створення звіту щодо захищеності WEB-ресурсів, Industry Standard and Compliance reports</p> <p><b>Вміти:</b></p> <ol style="list-style-type: none"> <li>1. Генерація спеціалізованих звітів для розробників, внутрішніх аудиторів та тестувальників загроз.</li> <li>2. Створення expansive reports.</li> </ol> <p><b>Формування компетенцій:</b> КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7</p> <p><b>Програмні результати навчання:</b> PH-1 - PH-19, PH-20, PH-22, PH-23</p> <p><b>Рекомендовані джерела:</b> 1-24</p>	Лабораторне заняття 7 2 год	6*	Створення типових звітів щодо захищеності WEB-ресурсів.
<p><b>Тема 7.</b> Мульти-користувальницькі рішення для забезпечення безпеки WEB-додатків що реалізовані в AST systems. Сканери вразливостей WEB Application Scanning</p>	Самостійна робота		Порівняльний аналіз сканерів вразливостей WEB Application Scanning. Аналіз типових методів атак на веб-додатки.
<b>Змістовий модуль 2. Технології щодо забезпечення виявлення вразливостей та забезпечення безпеки WEB-ресурсів</b>			
<p><b>Тема 8.</b> Призначення та функціональні можливості сучасних AST system. Характеристика Vulnerability Management Software (VMS). Виявлення вразливостей. Управління вразливостями. Протидія атакам</p> <p><b>Знати:</b></p> <ol style="list-style-type: none"> <li>1. Основи застосування та можливості.</li> </ol>	Лекція 8 4 год	6*	Лекція-візуалізація

<p>2. Принципи роботи, функції та можливості Vulnerability Scanner Software (VSS).</p> <p>3. Особливості тестування VSS.</p> <p><b>Вміти:</b></p> <p>4. Підходи та методи зниження ризику витоків даних і атак на WEB-додатки.</p> <p><b>Формування компетенцій:</b> КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7</p> <p><b>Програмні результати навчання:</b> РН-1 - РН-19, РН-20, РН-22, РН-23</p> <p><b>Рекомендовані джерела:</b> 1-24</p>			
<p><b>Тема 8.</b> Виявлення вразливостей WEB-додатків за допомогою WEB Application Scanning</p> <p><b>Вміти:</b></p> <ol style="list-style-type: none"> <li>1. Black-box scanning.</li> <li>2. White-box scanning</li> <li>3. Glass box scanning Security WEB Application Scanning.</li> </ol> <p><b>Формування компетенцій:</b> КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7</p> <p><b>Програмні результати навчання:</b> РН-1 - РН-19, РН-20, РН-22, РН-23</p> <p><b>Рекомендовані джерела:</b> 1-24</p>	<p>Практичне заняття 8 2 год</p>	<p>5*</p>	<p>Виявлення вразливостей WEB-додатків за допомогою WEB Application Scanning.</p>
<p><b>Тема 8.</b> Інтегровані засоби сканування WEB-сервісів. Vulnerability Testing та WEB Applications Analysis</p> <p><b>Вміти:</b></p> <ol style="list-style-type: none"> <li>1. Інтегровані засоби сканування WEB-сервісів.</li> <li>2. Базові інструменти щодо Vulnerability Testing та WEB Applications Analysis.</li> </ol> <p><b>Формування компетенцій:</b> КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7</p> <p><b>Програмні результати навчання:</b> РН-1 - РН-19, РН-20, РН-22, РН-23</p> <p><b>Рекомендовані джерела:</b> 1-24</p>	<p>Практичне заняття 9 2 год</p>	<p>6*</p>	<p>Зниження ризику від атак і витоків даних WEB-ресурсів та WEB-додатків перед розгортанням сайту. Методи захисту веб-додатків.</p>
<p><b>Тема 8.</b> Виявлення вразливостей WEB-додатків за допомогою WEB Application Scanning</p>	<p>Самостійна робота</p>		<p>Методи та технології виявлення вразливостей WEB-додатків за допомогою WEB Application Scanning. Аналіз типових методів атак на веб-додатки.</p>

<b>Тема 8.</b> Характеристика Vulnerability Management Software (VMS)			Порівняльні характеристики Vulnerability Management Software
<b>Тема 9.</b> Методи та сучасні інструменти дослідження вразливостей WEB-ресурсів. Переваги та недоліки спеціалізованих сканерів вразливостей <b>Знати:</b> <ol style="list-style-type: none"> <li>1. Класифікація загроз безпеки WEB-ресурсів - WASC Threat Classification.</li> <li>2. Застосування WAS, WASS, WAVS system.</li> <li>3. Функціональні можливості.</li> <li>4. Планування установки у своєму середовищі.</li> <li>5. Механізми захисту WEB-ресурсів. Основні напрями реалізації.</li> </ol> <b>Вміти:</b> <ol style="list-style-type: none"> <li>1. Підходи та методи зниження ризику витоків даних і атак на WEB-додатки.</li> </ol> <b>Формування компетенцій:</b> КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7 <b>Програмні результати навчання:</b> РН-1 - РН-19, РН-20, РН-22, РН-23 <b>Рекомендовані джерела:</b> 1-24	Лекція 9 4 год  Практичне заняття 9 2 год	6*	Лекція-візуалізація  Зниження ризику від атак і витоків даних WEB-ресурсів та WEB-додатків перед розгортанням сайту. Безпечна архітектура додатків. Перевірка безпеки коду. Виявлення вразливостей. Управління вразливостями. Протидія XSS-атакам. Захист від CSRF. Захист від XXE-атак. Протидія впровадженню. Протидія DoS-атакам. Захист сторонніх залежностей.
<b>Тема 9.</b> Можливості Automation Frameworks. Сканування за допомогою сценарію Selenium. Протидія DoS, XSS-атакам, захист від CSRF <b>Вміти:</b> <ol style="list-style-type: none"> <li>1. Середовище автоматизації для функціонального тестування WEB-додатків.</li> <li>2. Сканування за допомогою сценарію Selenium.</li> </ol> <b>Формування компетенцій:</b> КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7 <b>Програмні результати навчання:</b> РН-1 - РН-19, РН-20, РН-22, РН-23 <b>Рекомендовані джерела:</b> 1-24	Лабораторне заняття 9 2 год	6*	Проведення повного сканування за допомогою визначених сценаріїв.
<b>Тема 9.</b>	Самостійна робота		1. Сучасні інструменти дослідження вразливостей WEB-ресурсів.

<p>Методи та сучасні інструменти дослідження вразливостей WEB-ресурсів. Переваги та недоліки спеціалізованих сканерів вразливостей</p> <p><b>Вміти:</b></p> <p>1. Підходи та методи дослідження вразливостей WEB-ресурсів.</p> <p><b>Формування компетенцій:</b> КЗ-1-КЗ-2, КЗ-4, КЗ-6 - КЗ-10, КФ-1, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7</p> <p><b>Програмні результати навчання:</b> РН-1 - РН-19, РН-20, РН-22, РН-23</p> <p><b>Рекомендовані джерела:</b> 1-24</p>			<p>Аналіз переваг та недоліків спеціалізованих сканерів вразливостей.</p>
---	--	--	---

### МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

<p>Лабораторія 420 (Кіберполігон):</p> <ol style="list-style-type: none"> <li>1. Проектор ViewSonicPJD 7720 HD – 1 шт.</li> <li>2. Сервери - 3шт.</li> <li>3. Робочі станції - 14 шт.;</li> <li>4. Маршрутизатор - 1 шт.</li> <li>5. Комутатор - 1шт.</li> <li>6. Спеціалізоване ПЗ: Ubuntu server, MatLab, WEB Application Scanner, VirtualBox, ESET Security Management, VMware, Kali Linux та ін.,</li> <li>7. ПЗ: IBM QRadar SIEM, IBM QRadar Community Edition, IBM i2 Analyst's Notebook,</li> <li>8. ПЗ: Tenable Nessus.</li> <li>9. Мережа Інтернет ауд. 420.</li> </ol>
--

### ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

<p>Рекомендовані джерела та інші навчальні ресурси: вказати підручники, навчальні посібники не пізніше 2010 року видання, які є у нас у бібліотеці на державній мові; електронні ресурси, посилання, електронна бібліотека ДУТ, іншомовні джерела.</p>
<p>1. ДСТУ ISO-IEC TR 13335-1 Інформаційні технології. Настанови з керування безпекою ІТ. Ч 1. Концепції й моделі безпеки ІТ.</p>
<p>2. Bertino E., Martino L.D., Paci F., Squicciarini A.C. Security for WEB Services and Service Oriented Architectures Springer, 2010. – 231 p. – ISBN 978-3-540-87741-7.</p>
<p>3. Andrew Hoffman. Web Application Security Exploitation and Countermeasures for Modern Web Applications. 2020. ISBN 9781492053118</p>
<p>4. Drapkin S. Application Security in .NET Succinctly Syncfusion, 2017. – 103 p.</p>
<p>5. Gunasundaram Rajesh. ASP.NET WEB API Security Essentials Packt Publishing, 2015. – 152 p. – ISBN 978-1-78588-221-0.</p>
<p>6. Lakshmiraghavan B. Pro ASP.NET WEB API Security: Securing ASP.NET WEB API Apress, 2013. – 403 Pages.</p>
<p>7. Park Foreman. Vulnerability Management. Second Edition. CRC Press Taylor &amp; Francis Group, 2019. 330 p.</p>
<p>8. Technical Guide to Information Security Testing and Assessment. Recommendations of the National Institute of Standards and Technology. Karen Scarfone. Murugiah Souppaya. Amanda Cody. Angela Orebaugh. NIST Special Publication 800-115. (Sep. 2008). 80 p. <a href="https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf">https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf</a>.</p>
<p>9. Tom Palmaers. Implementing a vulnerability management process. SANS Institute. Accepted: 03/23/2013. 24 p. <a href="https://www.sans.org/reading-room/whitepapers/threats/implementing-vulnerability-management-process-34180">https://www.sans.org/reading-room/whitepapers/threats/implementing-vulnerability-management-process-34180</a>.</p>

10. Tenable Scan Strategy Tenable Professional Services. Last Revised: May 07, 2021. 22 p. <a href="https://docs.tenable.com/other/nessus/Tenable_ProServ_Scan_Strategy_Guide.pdf">https://docs.tenable.com/other/nessus/Tenable_ProServ_Scan_Strategy_Guide.pdf</a> .
11. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В. Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний Н.В. Лукова-Чуйко/ – К. : ДУТ – КНУ, 2016. – 178 с.
12. ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements
13. ISO/IEC 27035:2011«Information technology. Security techniques. Information security incident management
14. Application Security Verification Standard 4:0 <a href="https://www.owasp.org/images/d/d4/OWASP_Application_Security_Verification_Standard_4.0-en.pdf">https://www.owasp.org/images/d/d4/OWASP_Application_Security_Verification_Standard_4.0-en.pdf</a>
15. MITRE Common Weakness Enumeration: <a href="https://cwe.mitre.org/">https://cwe.mitre.org/</a>
16. MITRE Common Weakness Enumeration: <a href="http://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html">http://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html</a>
17. National Institute of Standards and Technology: <a href="https://nvd.nist.gov/vuln-metrics/cvss">https://nvd.nist.gov/vuln-metrics/cvss</a>
18. Open WEB Application Security Project: <a href="https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project">https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project</a>
19. MITRE ATT&CK: <a href="https://cve.mitre.org/index.html">https://cve.mitre.org/index.html</a>
20. Стандарт NIST SP 800 <a href="https://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf">csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf</a>
21. CSDL   IEEE Computer Society: <a href="https://www.computer.org/csdl/proceedings/2008/hicss/12OmNy3iFtz">Building a Test Suite for Web Application Scanners</a> <a href="https://www.computer.org/csdl/proceedings/2008/hicss/12OmNy3iFtz">https://www.computer.org/csdl/proceedings/2008/hicss/12OmNy3iFtz</a>
22. Qualys Web Application Scanning: <a href="https://www.qualys.com/apps/web-app-scanning/">https://www.qualys.com/apps/web-app-scanning/</a>
23. Tenable.io vulnerability management: <a href="https://www.tenable.com/products/tenable-io">https://www.tenable.com/products/tenable-io</a>
24. IBM AppScan Enterprise scanner: <a href="https://www.ibm.com/docs/en/dsm?topic=guide-appscan-enterprise-scanner-overview">https://www.ibm.com/docs/en/dsm?topic=guide-appscan-enterprise-scanner-overview</a>

#### 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 практичних 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 студент/аспірант 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 студент/аспірант повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату студент/аспірант отримує за завдання 0 балів.
- Студент/аспірант, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- За використання телефонів і комп'ютерних засобів без дозволу викладача, порушення дисципліни студент/аспірант видаляється з заняття, за заняття отримує 0 балів.

#### \* КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є набрання студентом/аспірантом 30 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
<b>ПОТОЧНИЙ КОНТРОЛЬ</b>	<i>Робота на заняттях, у т.ч.:</i>	
	<ul style="list-style-type: none"> <li>• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)</li> </ul>	за кожне відвідування 0,5 бала

	• звіт про виконання практичного завдання	за кожен звіт максимум 1 бал
<b>Додаткова оцінка</b>	Участь у наукових конференціях, підготовка наукових публікацій, отримання міжнародного сертифікату за напрямом.	Звільняється від екзамену
<b>ПІДСУМКОВЕ ОЦІНЮВАННЯ екзамен</b>	Метою екзамену є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. Екзамен проходить у письмовій та усній формі.	40 балів

### ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	Критерії оцінювання	Рівень компетентності	Оцінка /зачис в екзаменаційній відомості
90-100	Студент/аспірант 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 стосуються дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або аспірант проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	<b>Високий</b> Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції аспіранта в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивченні інших дисциплін, а також знання, набуті при самостійному поглибленому вивченні питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (А)
82-89	Студент/аспірант 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.	<b>Достатній</b> Забезпечує аспіранту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивченні дисципліни	Добре / Зараховано (В)
75-81	Студент/аспірант 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	<b>Достатній</b> Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість	Добре / Зараховано (С)

	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.	використання теоретичних положень для практичного використання викликають утруднення.	
64-74	Студент/аспірант 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 розглядалися з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.	<b>Середній</b> Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-63	Студент/аспірант 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, аспірант 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.	<b>Середній</b> Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	Студент/аспірант може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни аспірант виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у аспіранта відсутні.	<b>Низький</b> Не забезпечує практичної реалізації задач, що формуються при вивченні дисципліни	Незадовільно з можливістю повторного складання / Не зараховано (FX) <i>В залікову книжку не представляється</i>
1-34	Студент/аспірант повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент/аспірант не допущений до здачі заліку.	<b>Незадовільний</b> Студент/аспірант не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) <i>В залікову книжку не представляється</i>