**СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

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

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="3">Борсуковський Юрій Володимирович, кандидат технічних наук, доцент</td><td colspan="2">Контактна інформація лектора (e-mail), сторінка курсу в Moodle</td><td>e-mail: ikbdut@gmail.com; сторінка курсу в Moodle – http://dl.dut.edu.ua/course/view.php?id=1083</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="3">12 «Інформаційні технології»</td><td colspan="2">Рівень вищої освіти</td><td>Доктор філософії</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="3">Кібербезпека</td><td colspan="2">Семестр</td><td>1</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="3">Доктор філософії кібербезпеки</td><td colspan="2">Тип дисципліни</td><td>Професійної та практичної підготовки</td></tr>
<tr><td rowspan="2">Обсяг:</td><td rowspan="2">Кредитів ECTS</td><td rowspan="2">Годин</td><td colspan="6">За видами занять:</td></tr>
<tr><td>Лекцій</td><td>Семінарських занять</td><td>Практичних занять</td><td>Лабораторних занять</td><td>Самостійна підготовка</td></tr>
<tr><td></td><td>3</td><td>90</td><td>18</td><td>-</td><td>18</td><td>18</td><td>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">1. Основи наукових досліджень та організація науки<br>2. Методологія наукових досліджень у кібербезпеці</td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="6">Кваліфікаційна робота</td></tr>
<tr><td>Мета курсу:</td><td colspan="8">Формування знань та вмінь застосування методів та засобів виявлення уразливостей WEB-ресурсів інформаційної системи організації, виявлення недоліків та протиріч для проведення наукових досліджень</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"></td><td colspan="5">ФК-1. Інтегративна компетентність<br>ФК-3. Організаційно-комунікативна компетентність<br>ФК-4. Професійна компетентність<br>ФК-5. Загальнонаукова компетентність<br>ФК-6. Політехнічна компетентність<br>ФК-7. Інженерна компетентність</td></tr>
<tr><td colspan="9">Програмні результати навчання (ПРН)</td></tr>
<tr><td colspan="9">ПРН-18. Уміти аналізувати існуючі технології, методи і засоби застосування шкідливого програмного забезпечення, нівелювання уразливостей мережевих та Web-ресурсів.<br>ПРН-19. Уміти проектувати перспективні технології виявлення шкідливого програмного забезпечення, а також вразливостей мережевих та Web-ресурсів й застосовувати їх на практиці.<br>ПРН-20. Уміти визначати і вирішувати етичні питання при проведенні досліджень та пошуку відмінностей у шкідливому програмного забезпечення, вразливостях мережевих та Web-ресурсів.<br>ПРН-26. Уміти використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об’єктів інформаційної діяльності, а також наукових досліджень вищих рівнів.</td></tr>
</table>

| |
|---|
| ПРН-27. Бути здатним оволодіти спеціалізованими програмними пакетами, протоколами передачі даних, спеціальною мікропроцесорною технікою, сучасними інформаційними та безпековими технологіями. |

| **ОРГАНІЗАЦІЯ НАВЧАННЯ** | | | |
|---|---|---|---|
| **Тема, опис теми** | **Вид заняття** | **Оцінювання за тему** | **Форми і методи навчання/питання до самостійної роботи** |
| **Змістовий модуль 1. Сучасні аспекти технологій виявлення вразливостей та забезпечення безпеки WEB-ресурсів** | | | |
| **Тема 1.**<br>Інформаційні ресурси гетерогенної корпоративної мережі (ГКМ). Основні поняття щодо безпеки WEB-ресурсів та WEB-додатків<br>***Знати***:<br>1. Основні поняття, види мереж, особливості функціонування.<br>2. Перелік номенклатури засобів ТЗІ щодо сучасної нормативно-правової бази.<br>3. Функціональні профілі.<br>4. Характеристики WEB-ресурсів.<br>5. Основні поняття щодо безпеки WEB-ресурсів.<br>6. Розвідка веб-додатків.<br>***Вміти:***<br>1. Оперувати поняттями процесу управління вразливостями - стандарт NIST SP 800.<br>2. Оперування понятійним апаратом щодо ТВУЗБ WEB-ресурсів.<br>3. Застосовувати законодавчу, нормативно-правову базу щодо виявлення загроз WEB-ресурсів.<br>***Формування компетенцій:*** ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7<br>***Програмні результати навчання:*** ПРН-18 - ПРН-19, ПРН-20<br>***Рекомендовані джерела:*** 1-19 | Лекція 1<br>2 год | 2* | Лекція-візуалізація |
| | Практичне заняття 1<br>2 год | | Нормативно-правова база, міжнародні документи в напряму забезпечення безпеки WEB-ресурсів.<br>Методи збору інформації.<br>Карта веб-додатка. |
| **Тема 2.**<br>Мережеве обладнання та середовища передачі інформації в корпоративних системах.<br>Вимоги та механізми ЗІ WEB-систем від НСД<br>***Знати***:<br>1. Аналіз актуальних проблем та нормативної бази щодо ЗІ WEB-систем. | Лекція 2<br>2 год | 2* | Лекція-візуалізація |
| | Практичне заняття 2<br>2 год | | Аналіз української нормативно-правої бази та міжнародних стандартів в напряму забезпечення безпеки WEB-ресурсів.<br>Основні версії додатків.<br>REST API.<br>Формат JSON. |

| | | | |
|---|---|---|---|
| 2. Технічні вимоги за критеріями ТЗІ відповідно до функціонального профілю з рівнем гарантій Г-2.<br>3. Механізми ЗІ управління доступом до ресурсів ГКМ.<br>4. Структура сучасних веб-додатків.<br>***Вміти***:<br>1. Проводити оцінку ризиків ІБ щодо забезпечення безпеки WEB-ресурсів.<br>2. Застосовувати законодавчу, нормативно-правову базу в виявленні, прогнозуванні, оцінюванні загроз WEB-ресурсів.<br>***Формування компетенцій:*** ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7<br>***Програмні результати навчання:*** ПРН-18 - ПРН-19, ПРН-20, ПРН-20,<br>***Рекомендовані джерела:*** 1–19 | | | |
| **Тема 3.**<br>Уразливості та дестабілізуючі чинники інформаційного простору. Технології виявлення вразливостей WEB-ресурсів<br>***Знати***:<br>1. Основні поняття, види мереж, особливості функціонування.<br>2. Перелік номенклатури засобів ТЗІ щодо сучасної нормативно-правової бази.<br>3. Функціональні профілі.<br>4. Характеристики WEB-ресурсів.<br>5. Основні поняття щодо безпеки WEB-ресурсів.<br>6. Структура сучасних веб-додатків.<br>***Вміти:***<br>1. Впроваджувати законодавчу, НПБ щодо виявлення, прогнозування, оцінювання загроз WEB-ресурсів до вибору раціональних технологій безпеки WEB-ресурсів.<br>***Формування компетенцій:*** ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7<br>***Програмні результати навчання:*** ПРН-18 - ПРН-20, ПРН-26, ПРН-27<br>***Рекомендовані джерела:*** 1-19 | Лекція 3<br>2 год | 6* | Лекція-візуалізація |
| | Практичне заняття 3<br>2 год | | Аналіз української нормативно-правої бази та міжнародних стандартів в напряму забезпечення безпеки WEB-ресурсів.<br>Змінні javascript і їх область видимості.<br>Функції javascript.<br>Контекст javascript.<br>Прототипне спадкування javascript.<br>Асинхронне виконання коду javascript.<br>Фреймворки для SPA.<br>Системи аутентифікації і авторизації.<br>Веб-сервери.<br>Бази даних на стороні сервера.<br>Зберігання даних на стороні клієнта. |
| **Тема 3.**<br>Уразливості та дестабілізуючі чинники інформаційного простору. Технології виявлення вразливостей WEB-ресурсів | Самостійна робота | | Аналіз технологій виявлення вразливостей WEB-ресурсів.<br>Структура сучасних веб-додатків. |
| **Тема 4.** | Лекція 4<br>2 год | 6* | Лекція-візуалізація |

| | | | |
|---|---|---|---|
| Інформаційні ресурси гетерогенної корпоративної мережі (ГКМ). Основні поняття щодо безпеки WEB-ресурсів та WEB-додатків<br>***Знати***:<br>1. Основні поняття, види мереж, особливості функціонування.<br>2. Перелік номенклатури засобів ТЗІ щодо сучасної нормативно-правової бази.<br>3. Функціональні профілі.<br>4. Характеристики WEB-ресурсів.<br>5. Основні поняття щодо безпеки WEB-ресурсів.<br>6. Аналіз API.<br>***Вміти:***<br>1. Методи оцінки вразливостей на основі the Ten Most Critical WEB Application Security Risks.<br>2. Найбільш актуальні методи і ЗЗІ від загроз WEB-додатків.<br>***Формування компетенцій:*** ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7<br>***Програмні результати навчання:*** ПРН-18, ПРН-20, ПРН-26<br>***Рекомендовані джерела:*** 1-19 | Практичне заняття 4<br>2 год | | Середа тестування захищеності WEB-додатків сканерами класу AST systems. WEB-сканери вразливостей провідних виробників.<br>Аналіз API.<br>Виявлення кінцевої точки- механізми аутентифікації.<br>Різновиди кінцевих точок- базові різновиди.<br>Різновиди кінцевих точок- спеціалізовані різновиди. |
| **Тема 4.**<br>Інформаційні ресурси гетерогенної корпоративної мережі (ГКМ). Основні поняття щодо безпеки WEB-ресурсів та WEB-додатків | Самостійна робота | | Аналіз технологій забезпечення безпеки WEB-ресурсів та WEB-додатків.<br>Аналіз API. |
| **Тема 5.**<br>Безпека рівня мережевої інфраструктури. Захист WEB-додатків і сучасні напрями розвитку інформаційної та кібербезпеки<br>***Знати***:<br>1. Сучасні методи тестування WEB-ресурсів від руйнівних кіберзагроз.<br>2. Security vulnerability testing для WEB services.<br>3. Основні уразливості мережевих WEB-додатків.<br>4. Методи усунення вразливостей.<br>***Вміти:***<br>1. Загальні принципи, що реалізовані в сканерах вразливостей.<br>2. Класифікація вразливостей відповідно до WASC, небезпечні атаки на WEB-ресурси.<br>3. Принципи роботи WEB Application Scanning.<br>4. Виявлення сторонніх залежностей.<br>***Формування компетенцій:*** ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7 | Лекція 5<br>2 год | 6* | Лекція-візуалізація |
| | Практичне заняття 5<br>2 год | | Тестування захищеності WEB-додатків AST systems. WEB-сканер вразливостей - WEB Application Scanning.<br>Клієнтські фреймворки- фреймворки для односторінкових додатків.<br>Клієнтські фреймворки- бібліотеки JavaScript.<br>Клієнтські фреймворки- бібліотеки CSS.<br>Фреймворки на стороні сервера- заголовки.<br>Фреймворки на стороні сервера- стандартні повідомлення про помилку і сторінки 404.<br>Фреймворки на стороні сервера- бази даних. |

| | | | |
|---|---|---|---|
| ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26<br>***Рекомендовані джерела:*** 1-19 | | | |
| **Тема 5.**<br>Безпека рівня мережевої інфраструктури. Захист WEB-додатків і сучасні напрями розвитку інформаційної та кібербезпеки | Самостійна робота | | Аналіз технологій захисту WEB-додатків.<br>Виявлення сторонніх залежностей. |
| **Тема 6.**<br>Методи та технології забезпечення ІБ у WEB-додатках. Автентифікація та ідентифікація сесій WEB-додатків. Пошук слабких місць в архітектурі додатків<br>***Знати***:<br>1. Методи автентифікації WEB-додатків.<br>2. Уразливості автентифікації.<br>3. Передбачуване значення ідентифікатора session.<br>4. Недостатня авторизація.<br>5. Пошук слабких місць в архітектурі додатків.<br>***Вміти:***<br>1. Основні функції і процедури роботи WEB Application Scanning.<br>2. WEB Application Scanning full scan, додаткові функції.<br>***Формування компетенцій:*** ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7<br>***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26<br>***Рекомендовані джерела:*** 1-19 | Лекція 6<br>2 год<br><br>Практичне заняття 6<br>2 год | 6* | Лекція-візуалізація<br><br>Нормативно-правова база, міжнародні документи в напряму забезпечення безпеки WEB-ресурсів.<br>Ознаки безпечної і небезпечної архітектури.<br>Рівні безпеки.<br>Запозичення і перекроювання. |
| **Тема 6.**<br>Методи та технології забезпечення ІБ у WEB-додатках. Автентифікація та ідентифікація сесій WEB-додатків | Самостійна робота | | Методи та технології забезпечення кібернетичної та інформаційної безпеки у WEB-додатках.<br>Аналіз методів пошуку слабких місць в архітектурі додатків. |
| **Тема 7.**<br>Мульти-користувальницькі рішення для забезпечення безпеки WEB-додатків що реалізовані в AST systems. Сканери вразливостей WEB Application Scanning<br>***Знати***:<br>1. Основні підходи та принципи роботи.<br>2. Базові функції та напрями реалізації WEB Application Scanning.<br>3. Black-box scanning, white-box scanning, glass box scanning. | Лекція 7<br>2 год<br><br>Практичне заняття 7<br>2 год | 6* | Лекція-візуалізація<br><br>Основи виявлення вразливостей WEB-додатків за допомогою WEB Application Scanning.<br>Міжсайтовий скриптинг (XSS).<br>Підробка міжсайтових запитів (CSRF).<br>Атака на зовнішні сутності XML (XXE).<br>Впровадження коду.<br>Відмова в обслуговуванні (DoS). |

| | | | |
|---|---|---|---|
| 4. Особливості тестування WEB-додатків.<br>5. Типові методи атак на веб-додатки.<br>***Вміти:***<br>1. Налаштування сканування та політики WEB Application Scanning.<br>2. Автоматичний потік операцій сканування WEB Application Scanning.<br>***Формування компетенцій:*** ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7<br>***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27<br>***Рекомендовані джерела:*** 1-19 | | | Експлуатація сторонніх залежностей. |
| **Тема 7.**<br>Мульти-користувальницькі рішення для забезпечення безпеки WEB-додатків що реалізовані в AST systems. Сканери вразливостей WEB Application Scanning | Самостійна робота | | Порівняльний аналіз сканерів вразливостей WEB Application Scanning.<br>Аналіз типових методів атак на веб-додатки. |
| **Тема 8.**<br>Виявлення вразливостей WEB-додатків за допомогою WEB Application Scanning<br>***Вміти:***<br>1. Black-box scanning.<br>2. White-box scanning<br>3. Glass box scanning Security WEB Application Scanning.<br>***Формування компетенцій:*** ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7<br>***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27<br>***Рекомендовані джерела:*** 1-19 | Практичне заняття 8<br>2 год | 5* | Виявлення вразливостей WEB-додатків за допомогою WEB Application Scanning. |
| **Тема 8.**<br>Виявлення вразливостей WEB-додатків за допомогою WEB Application Scanning | Самостійна робота | | Методи та технології виявлення вразливостей WEB-додатків за допомогою WEB Application Scanning.<br>Аналіз типових методів атак на веб-додатки. |
| **Тема 9.**<br>Політика тестування та налаштування сканування вразливостей за допомогою WEB Application Scanning<br>***Вміти:***<br>1. Основні функції та напрями реалізації WEB Application Scanning.<br>2. Використання можливостей the scanner setup wizard. | Лабораторне заняття 1<br>2 год | 5* | Визначення політика тестування та налаштування параметрів сканування вразливостей за допомогою WEB Application Scanning. |

| | | | |
|---|---|---|---|
| 3. Testing strategies.<br>***Формування компетенцій:*** ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7<br>***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27<br>***Рекомендовані джерела:*** 1-19 | | | |
| **Тема 10.**<br>Сканування захищеності WEB-ресурсів за допомогою WEB Application Scanning. Способи управління етапом аналізу<br>***Вміти:***<br>1. Операції, що виконуються під час сканування.<br>2. Способи управління етапом аналізу вручну і експорт результатів сканування.<br>***Формування компетенцій:*** ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7<br>***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27<br>***Рекомендовані джерела:*** 1-19 | Лабораторне заняття 2<br>2 год | 5* | Проведення сканування захищеності WEB-ресурсів за допомогою WEB Application Scanning. Способи управління етапом аналізу. |
| **Тема 11.**<br>Базова конфігурурація сканера для оцінки захищеності WEB-ресурсів за допомогою WEB Application Scanning<br>***Вміти:***<br>1. Сканування WEB-служб.<br>2. Configuring the scan, Running the scan, Reviewing Scan Results WEB Application Scanning.<br>***Формування компетенцій:*** ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7<br>***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27<br>***Рекомендовані джерела:*** 1-19 | Лабораторне заняття 3<br>2 год | 5* | Проведення конфігурування сканера для оцінки захищеності WEB-ресурсів за допомогою WEB Application Scanning. |
| **Тема 12.**<br>Повне сканування, налаштування сканування вразливостей WEB Application Scanning. Вибір методів сканування<br>***Вміти:***<br>1. Визначати конфігурацію сканування.<br>2. Проводити вибір та застосовувати analysis systems DAST, SAST scanning.<br>***Формування компетенцій:*** ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7<br>***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27<br>***Рекомендовані джерела:*** 1-19 | Лабораторне заняття 4<br>2 год | 5* | Проведення повного сканування, налаштування сканування вразливостей WEB Application Scanning. Вибір базових методів сканування. |

| | | | |
|---|---|---|---|
| **Тема 13.**<br>Інтегрований клієнт GSC та файл WSDL WEB-служби<br>***Вміти:***<br>1. Інтегрований клієнт GSC<br>2. Склад, призначення та функції components.<br>***Формування компетенцій:*** ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7<br>***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27<br>***Рекомендовані джерела:*** 1-19 | Лабораторне заняття 5<br>2 год | 5* | Інтегрований клієнт GSC та файл WSDL WEB-служби. |
| | | | |
| **Змістовий модуль 2. Технології щодо забезпечення виявлення вразливостей та забезпечення безпеки WEB-ресурсів** | | | |
| **Тема 13.**<br>Призначення та функціональні можливості сучасних AST system. Характеристика Vulnerability Management Software (VMS).<br>***Знати***:<br>1. Основи застосування та можливості.<br>2. Принципи роботи, функції та можливості Vulnerability Scanner Software (VSS).<br>3. Особливості тестування VSS.<br>***Вміти:***<br>4. Підходи та методи зниження ризику витоків даних і атак на WEB-додатки.<br>***Формування компетенцій:*** ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7<br>***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27<br>***Рекомендовані джерела:*** 1-19 | Лекція 8<br>2 год | 6* | Лекція-візуалізація |
| | Практичне заняття 9<br>2 год | | Зниження ризику від атак і витоків даних WEB-ресурсів та WEB-додатків перед розгортанням сайту.<br>Методи захисту веб-додатків. |
| **Тема 13.**<br>Характеристика Vulnerability Management Software (VMS) | Самостійна робота | | Порівняльні характеристики Vulnerability Management Software |
| **Тема 14.**<br>Методи та сучасні інструменти дослідження вразливостей WEB-ресурсів. Переваги та недоліки спеціалізованих сканерів вразливостей<br>***Знати***:<br>1. Класифікація загроз безпеки WEB-ресурсів - WASC Threat Classification. | Лекція 9<br>2 год | 6* | Лекція-візуалізація |
| | Практичне заняття 9<br>2 год | | Зниження ризику від атак і витоків даних WEB-ресурсів та WEB-додатків перед розгортанням сайту.<br>Безпечна архітектура додатків.<br>Перевірка безпеки коду.<br>Виявлення вразливостей. |

| | | | |
|---|---|---|---|
| 2. Застосування WAS, WASS, WAVS system.<br>3. Функціональні можливості.<br>4. Планування установки у своєму середовищі.<br>5. Механізми захисту WEB-ресурсів. Основні напрями реалізації.<br>***Вміти:***<br>1. Підходи та методи зниження ризику витоків даних і атак на WEB-додатки.<br>***Формування компетенцій:*** ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7<br>***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27<br>***Рекомендовані джерела:*** 1-19 | | | Управління вразливостями.<br>Протидія XSS-атакам.<br>Захист від CSRF.<br>Захист від XXE-атак.<br>Протидія впровадженню.<br>Протидія DoS-атакам.<br>Захист сторонніх залежностей. |
| **Тема 14.**<br>Методи та сучасні інструменти дослідження вразливостей WEB-ресурсів. Переваги та недоліки спеціалізованих сканерів вразливостей | Самостійна робота | | 1. Сучасні інструменти дослідження вразливостей WEB-ресурсів.<br>2. Аналіз переваг та недоліків спеціалізованих сканерів вразливостей. |
| **Тема 15.**<br>Утиліти Power Tools. Інтегровані засоби сканування WEB-сервісів<br>***Вміти:***<br>1. Визначати конфігурацію сканування.<br>2. Проводити вибір та застосовувати analysis systems DAST, SAST scanning.<br>***Формування компетенцій:*** ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7<br>***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27<br>***Рекомендовані джерела:*** 1-19 | Лабораторне заняття 6<br>2 год | 6* | Використання інтегрованих засобів сканування WEB-сервісів. |
| **Тема 16.**<br>Створення звіту щодо захищеності WEB-ресурсів, Industry Standard and Compliance reports<br>***Вміти:***<br>1. Генерація спеціалізованих звітів для розробників, внутрішніх аудиторів та тестувальників загроз.<br>2. Створення expansive reports.<br>***Формування компетенцій:*** ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7<br>***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27<br>***Рекомендовані джерела:*** 1-19 | Лабораторне заняття 7<br>2 год | 6* | Створення типових звітів щодо захищеності WEB-ресурсів. |

| | | | |
|---|---|---|---|
| **Тема 17.**<br>Інтегровані засоби сканування WEB-сервісів. Vulnerability Testing та WEB Applications Analisis<br>***Вміти:***<br>1. Інтегровані засоби сканування WEB-сервісів.<br>2. Базові інструменти щодо Vulnerability Testing та WEB Applications Analisis.<br>***Формування компетенцій:*** ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7<br>***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27<br>***Рекомендовані джерела:*** 1-19 | Лабораторне заняття 8<br>2 год | 6* | Проведення Vulnerability Testing та WEB Applications Analisis. |
| **Тема 18.**<br>Можливості Automation Frameworks. Сканування за допомогою сценарію Selenium<br>***Вміти:***<br>1. Середовище автоматизації для функціонального тестування WEB-додатків.<br>2. Сканування за допомогою сценарію Selenium.<br>***Формування компетенцій:*** ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7<br>***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27<br>***Рекомендовані джерела:*** 1-19 | Лабораторне заняття 9<br>2 год | 6* | Проведення повного сканування за допомогою визначених сценаріїв. |
| | | | |

**МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ**

Лабораторія 420 (Кіберполігон):

1. Проектор ViewSonicPJD 7720 HD – 1 шт.
2. Сервери - 3шт.
3. Робочі станції - 14 шт.;
4. Маршрутизатор - 1 шт.
5. Комутатор - 1шт.
6. Спеціалізоване ПЗ: Ubuntu server, MatLab, WEB Application Scaner, VirtualBox, ESET Security Management, VMware, Kali Linux та ін.,
7. ПЗ: IBM QRadar SIEM, IBM QRadar Community Edition, IBM i2 Analyst’s Notebook,
8. ПЗ: Tenable Nessus.
9. Мережа Інтернет ауд. 420.

**ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ**

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.

1. 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.
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.
3. Andrew Hoffman. Web Application Security Exploitation and Countermeasures for Modern Web Applications. 2020. ISBN 9781492053118
4. Drapkin S. Application Security in .NET Succinctly Syncfusion, 2017. – 103 p.
5. Gunasundaram Rajesh. ASP.NET WEB API Security Essentials Packt Publishing, 2015. – 152 p. – ISBN 978-1-78588-221-0.
6. Lakshmiraghavan B. Pro ASP.NET WEB API Security: Securing ASP.NET WEB API Apress, 2013. – 403 Pages.
7. ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements
8. ISO/IEC 27035:2011«Information technology. Security techniques. Information security incident management
9. Application Security Verification Standard 4:.0 https://www.owasp.org/images/d/d4/OWASP_Application_Security_Verification_Standard_4.0-en.pdf
10.MITRE Common Weakness Enumeration: https://cwe.mitre.org/
11.MITRE Common Weakness Enumeration: http://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html
12. National Institute of Standards and Technology: https://nvd.nist.gov/vuln-metrics/cvss
13. Open WEB Application Security Project: https://www.owasp.org/index.php/Category: OWASP_Code_Review_Project
14. MITRE ATT&CK: https://cve.mitre.org/index.html
15. Стандарт NIST SP 800 csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
16. CSDL | IEEE Computer Society: Building a Test Suite for Web Application Scanners https://www.computer.org/csdl/proceedings/2008/hicss/12OmNy3iFtz
17. Qualys Web Application Scanning: https://www.qualys.com/apps/web-app-scanning/
18. Tenable.io vulnerability management: https://www.tenable.com/products/tenable-io
19. IBM AppScan Enterprise scanner: https://www.ibm.com/docs/en/dsm?topic=guide-appscan-enterprise-scanner-overview

**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 |
|---|---|---|
| **ПОТОЧНИЙ КОНТРОЛЬ** | ***Робота на заняттях,*** *у т.ч.:* | |
| | • присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу) | за кожне відвідування 0,5 бала |
| | • звіт про виконання практичного завдання | за кожен звіт максимум 1 бал |
| | | |
| **Додаткова оцінка** | Участь у наукових конференціях, підготовка наукових публікацій, отримання міжнародного сертифікату за напрямом. | Звільняється від екзамену |
| **ПІДСУМКОВЕ ОЦІНЮВАННЯ** ***екзамен*** | Метою екзамену є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи.<br>Екзамен проходить у письмовій та усній формі. | 30 балів |

**ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ**

| **бали** | **Критерії оцінювання** | **Рівень компетентності** | **Оцінка /*запис 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.<br>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.<br>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 аспірант проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань. | **Високий**<br>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 вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені 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.<br>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**<br>Забезпечує аспіранту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені 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 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**<br>Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення. | Добре / Зараховано (C) |
| **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 розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача. . | **Середній**<br>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. | **Середній**<br>Є мінімально допустимим у всіх складових навчальної програми з дисципліни | Задовільно / Зараховано (E) |
| **35-59** | Студент/аспірант може відтворити окремі фрагменти з курсу.<br>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. | **Низький**<br>Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни | Незадовільно з можливістю повторного складання / Не зараховано (FX)<br>*В залікову книжку не проставляється* |
| **1-34** | Студент/аспірант повністю не виконав вимог робочої програми навчальної дисципліни.<br>Його знання на підсумкових етапах навчання є фрагментарними.<br>Студент/аспірант не допущений до здачі заліку. | **Незадовільний**<br>Студент/аспірант не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни | Незадовільно з обов'язковим повторним вивченням / Не допущений (F)<br>*В залікову книжку не проставляється* |