Інформаційний пакет освітніх компонент навчального плану
освітньо-професійної програми «ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА БЕЗПЕКА»
(назва)

Освітнього рівня **магістр**

Спеціальності **125 «Кібербезпека»**

Галузь знань **12 «Інформаційні технології»**

1. Назва освітньої компоненти «Технології виявлення уразливостей та забезпечення безпеки Web-ресурсів»
(назва дисципліни)

2. Тип вибіркова

3. Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінар	Практичних занять	Лабораторних занять	Самостійна підготовка
	6	72	36		18	18	108

4. Взаємозв'язок у структурно-логічній схемі	
Освітні компоненти, які передують вивченню	1. Політики безпеки. 2. Програмні комплекси захисту автиматизованих систем від несанкціонованого доступу. 3. Системи технічного захисту інформації. 4. Безпека безпроводових та хмарних технологій. 5. Безпека Web-ресурсів.
Освітні компоненти для яких є базовою	1. Організація проведення наукових досліджень. 2. Технології виявлення уразливостей мережевих ресурсів. 3. Магістерська робота.

5. Компетенції відповідно до ОПП та вимог роботодавців:	
Компетенції відповідно до ООП	
Знати	**Вміти**
1. Здатність до аналізу існуючих та проектування перспективних технологій виявлення шкідливого програмного забезпечення, а також уразливостей мережевих та Web-ресурсів та застосовування їх на практиці.	1. Уміти проектувати перспективні технології виявлення шкідливого програмного забезпечення, а також уразливостей мережевих та Web-ресурсів й застосовувати їх на практиці.
Компетенції відповідно до вимог роботодавців	
1. Знати міжнародні та державні стандарти по забезпеченню безпеки Web-ресурсів.	1. Проводити оцінку наявності уразливостей та пошук уразливостей у Web-додатках (SQL-ін'єкції, XSS, buffer overflow, тощо).
2. Знати існуючі Web-загрози (XSS, SQL(i), CSRF, (R)LFI, Code injections, Session hijacking, Path traversal, Parameter tampering, etc.).	2. Проводити аудит процесів інформаційної безпеки щодо захисту Web-ресурсів від сучасних загроз.

3. Знати основи методів адміністрування сучасних інструментів дослідження уразливостей Web-ресурсів.	3. Проводити моніторинг та контроль вторгнень за допомогою інструментів тестування з розширеними функціями і сучасними інфраструктурами.

6. Результати навчання відповідно до ОПП

1. ПРН18. Уміти розробляти та проектувати нові, вдосконалювати існуючі комплексні системи інформаційної та кібернетичної безпеки, підтримувати їх в стані, що необхідний для вирішення завдань захисту інформації.

2. ПРН19. Уміти проектувати перспективні технології виявлення шкідливого програмного забезпечення, а також уразливостей мережевих та Web-ресурсів й застосовувати їх на практиці.

7. План вивчення освітньої компоненти

Змістовний розділ	Вид заняття	Тема	Знати	Вміти	План заняття	Лекція, методична розробка
Розділ 1. Сучасні аспекти технологій виявлення уразливостей та забезпечення безпеки Web-ресурсів.						
	Лекція 1	Тема: Інформаційні ресурси гетерогенної корпоративної мережі (ГКМ). Технічні вимоги за критеріями ТЗІ. Основні поняття щодо Web-ресурсів та Web-додатків.	1. Основні поняття, види мереж, особливості функціонування. 2. Перелік номенклатури засобів ТЗІ щодо сучасної нормативно-правової бази. 3. Функціональні профілі. 4. Характеристики Web-ресурсів. 5. Основні поняття щодо безпеки Web-ресурсів.		http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лекція 2	Тема: Мережеве обладнання та середовища передачі інформації в corporate system. Вимоги та механізми ЗІ Web-систем від НСД.	1. Аналіз актуальних проблем та нормативної бази щодо ЗІ Web-систем. 2. Технічні вимоги за критеріями ТЗІ відповідно до функціонального профілю з рівнем гарантій Г-2. 3. Механізми ЗІ управління доступом до ресурсів ГКМ.		http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лекція 3	Тема: Уразливості та дестабілізуючі чинники інформаційного простору. Технології виявлення vulnerability Web-ресурсів.	1. Уразливості та загрози Web-ресурсів. 2. Класифікація vulnerability відповідно до WASC. 3. Класифікація сучасних attacks на Web-додатки.		http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507

			4. Призначення систем оцінки наявності vulnerability в Web-додатках.			
	Лекція 4	Тема: Основні напрями ІБ Web-ресурсів. Базові поняття щодо інформаційної та кібербезпеки ОІД.	1. Визначення основних vulnerability Web-систем. 2. Уразливості та загрози Web-ресурсів SQL-ін'єкції, XSS, CSRF, (R)LFI, Session hijacking, Path traversal, Parameter tampering, CSRF. 3. Технології HTTP, SSL/TLS, JavaScript/AJAX/DOM, HTML/CSS. 4. Defence in depth concept.		http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лекція 5	Тема: Безпека рівня мережевої інфраструктури. Захист Web-додатків і сучасні напрями розвитку інформаційної та кібербезпеки.	1. Сучасні методи тестування Web-ресурсів від руйнівних кіберзагроз. 2. Security vulnerability testing для Web services. 3. Основні уразливості мережевих Web-додатків. 4. Методи усунення vulnerability.		http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лекція 6	Тема: Методи та технології забезпечення ІБ у Web-додатках. Authentication, authorization and Identification сесії Web-додатків.	1. Методи authentication web-додатків. 2. Уразливості authentication. 3. Передбачуване значення ідентифікатора session. 4. Недостатня authorization.		http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лекція 7	Тема: Мультикористу-вальницькі рішення для забезпечення безпеки Web-додатків що реалізовані в AST systems. Сканер уразливостей AppScan Standart.	1. Основні підходи та принципи роботи. 2. Базові функції та напрями реалізації AppScan Standart. 3. Black-box scanning, white-box scanning, glass box scanning. 4. Особливості тестування Web-додатків.		http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Практичне	Тема: Аналіз української		1. Вміння застосовувати	http://dl.dut	http://dl.dut

	заняття 1	нормативно-правої бази та міжнародних стандартів в напряму забезпечення безпеки Web-ресурсів.		законодавчу, нормативно-правову базу в виявленні, прогнозуванні, оцінюванні загроз Web-ресурсіві. 2. Оперування понятійним апаратом щодо ТВУЗБ Web-ресурсів.	.edu.ua/course/view.php?id=1507	.edu.ua/course/view.php?id=1507
	Практичне заняття 2	Тема: Концептуальні положення міжнародних стандартів та інформаційних джерел щодо безпеки Web-ресурсів.		1. Опанувати класифікацію vulnerability Web-додатків. 2. Знати ID класів vulnerability. 3. Проводити аналіз attacks (WASC TC v 2.0). 4. Проводити оцінку засобів Continuous Application Security Testing.	http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Практичне заняття 3	Тема: Середа тестування захищеності Web-додатків сканерами класу AST systems.		1. Методи оцінки vulnerability на основі the Ten Most Critical Web Application Security Risks. 2. Найбільш актуальні методи і ЗЗІ від загроз Web-додатків.	http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лабораторне заняття 1	Тема: Виявлення vulnerability Web-додатків сканером уразливостей AppScan Standart.		1. Принципи, що реалізовані в vulnerability scanners. 2. Основні функції та напрями реалізації AppScan Standart. 3. Склад, призначення та функції components.	http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лабораторне заняття 2	Тема: Установка та розгортання vulnerability scanner AppScan Standart. Ознайомлення з системою налаштування.		1. Можливості сканування vulnerability, що реалізовані в AppScan Standart. 2. Механізм виявлення в сесії. 3. Methods entrance та виявлення session.	http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лабораторне заняття 3	Тема: Політика тестування та налаштування сканування vulnerability AppScan Standart. Вибір методів сканування.		1. Використання можливостей the scanner setup wizard. 2. Проводити вибір та застосовувати analysis systems DAST, SAST scanning. 3. Створення expansive reports.	http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507

	Лабораторне заняття 4	Тема: Методи та засоби адміністрування інструментів сканера AppScan Standart.		1. Використання можливостей сканування та політик AppScan Standart. 2. Характеризувати та розкривати основні можливості аналізу Glass box scanning. 3. Проведення оцінки результатів сканування.	http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
Розділ 2. Технології щодо забезпечення виявлення уразливостей та забезпечення безпеки Web-ресурсів						
	Лекція 8	Тема: Призначення та функціональні можливості сучасних AST system. Характеристика Vulnerability Management Software (VMS).	1. Основи застосування та можливості. 2. Принципи роботи, функції та можливості Vulnerability Scanner Software (VSS). 3. Особливості тестування VSS.		http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лекція 9	Тема: Основні напрями інформаційної та кібербезпеки Web-ресурсів. Перспективні напрями розвитку Open Source Web Security Scanner to Find Vulnerabilities.	1. Можливості VMS. 2. Представники та лідери на ринку Open Source Web Security Scanners. 3. Переваги та недоліки. 4. Напрями розвитку.		http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лекція 10	Тема: Методи та сучасні інструменти дослідження уразливостей Web-ресурсів. Переваги та недоліки спеціалізованих vulnerability scanners.	1. Застосування WAS, WASS, WAVS system. 2. Інтеграція з ЦОД. 3. Функціональні можливості. 4. Планування установки у своєму середовищі. 5. Механізми захисту Web-ресурсів. 6. Основні напрями реалізації.		http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Практичне заняття 4	Тема: XSS Attack: Problem & Solution directions.		1. XSS attack: проведення оцінки результатів сканування. 2. Уразливості, що призводять до code execution. 3. Напрями вибору стратегії рішень. 4. Приклади використання	http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507

				правильно кодованого виводу бібліотек Anti-XSS, encoding module OAPASP ESAPI і Apache Wicket.		
	Практичне заняття 5	Тема: Picking the right Appsec to get the desired results.		Планувати ефективний моніторинг контролю вторгнень за допомогою advanced testing tools with advanced features.	http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лабораторне заняття 5	Тема: Тестування сканером класу AST systems на рівнях методів користувача, несанкціонованого доступу та введення коду.		1. Підтримка базового рівня захищеності від: SQL-injection, XSS, buffer overflow, Session hijacking. 2. Integrated tool сканування Web-сервісів.	http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лабораторне заняття 6	Тема: SQLi: Problem & Solution directions.		1. Проведення оцінки результатів сканування. 2. Базові методи боротьби з вразливістю SQL injection. 3. Проведення аналізу та вибір напряму стратегії рішень.	http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лабораторне заняття 7	Тема: Інтегровані засоби сканування Web-сервісів. Vulnerability Testing та Web Applications Analisis		1. Основні функції of the direct implementation Kali Linux for testing penetration Web-додатків. 2. Базові інструменти Vulnerability Testing та Web Applications Analisis.	http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лабораторне заняття 8	Тема: Додаткові механізми захисту Web-додатків. Testing Tools.		1. Методи та vulnerability research tools Web-ресурсів. 2. Приклади реалізації Firewall Systems для ЗІ Web-додатків. 3. Переваги та недоліки.	http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507

8. Мова вивчення освітньої компоненти

(*українська*, англійська, розділи, що викладаються *англійською* мовою)

Українська, англійська

9. Інформаційне забезпечення освітньої компоненти

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. 3. 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.
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. https://cve.mitre.org/index.html
10. Методи оцінювання, підсумкові звітності за освітньою компонентою
(заліки, екзамени, курсові проекти, тестування)
залік
11. Матеріально-технічне забезпечення освітньої компоненти
Лабораторія 419, 420. ПК.

Виконано ст. викладачем Хмелевським Р.М.