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

Освітнього рівня **бакалавр**

Спеціальності **125 «Кібербезпека»**

Галузь знань **12 «Інформаційні технології»**

1. Назва освітньої компоненти «Безпека Web-ресурсів»
(назва дисципліни)

2. Тип Дисципліни фахової спеціалізації

3. Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінар	Практичних занять	Лабораторних занять	Самостійна підготовка
	3	90	18		18	18	80
4. Взаємозв'язок у структурно-логічній схемі							
Освітні компоненти, які передують вивченню	1. Аудит систем захисту інформації 2. Захист від шкідливого програмного засобу 3. Політики безпеки. 4. Основи безпеки комп'ютерних мереж 5. Програмні комплекси захисту автоматизованих систем від несанкціонованого доступу. 6. Безпека безпроводових, мобільних та хмарних технологій.						
Освітні компоненти для яких є базовою	1. Аудит систем захисту інформації. 2. Комплексні системи захисту інформації. 3. Методи та засоби протидії кіберзлочинності. 4. Технології виявлення уразливостей мережевих ресурсів. 5. Технології виявлення уразливостей та забезпечення безпеки Web-ресурсів.						

5. Компетенції відповідно до ООП	
Знати	**Вміти**
Знання та розуміння предметної області та розуміння професії.	1. ПП 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та кібербезпеки.
Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.	2. ПП 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та

	походження.
	3. ПП 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та кібербезпеки.
	4. ПП 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та кібербезпеки.
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, CSRF, buffer overflow, тощо).
2. Знати існуючі Web-загрози відповідно до міжнародних та державних стандартів по забезпеченню безпеки Web-ресурсів.	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. ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку якості прийнятих рішень.
2. ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
3. ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
4. ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
5. ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
6. ПРН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

7. План вивчення освітньої компоненти

Змістовний розділ	Вид заняття	Тема	Знати	Вміти	План заняття	Лекція, методична розробка
	Лекція 1	Тема: Введення в безпеку Web-ресурсів. Інформаційні ресурси та технічні вимоги за критеріями захисту інформації.	1. Види мереж і особливості їх функціонування. 2. Web-ресурси. WAN. LAN. WWW. Базові поняття. 3. Нормативна база щодо забезпечення захисту Web-ресурсів.		http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507

			4. Основні поняття щодо безпеки Web-ресурсів.			
	Лекція 2	Тема: Уразливості Web-ресурсів. Статистичні дані загроз безпеки Web-додатків.	1. Уразливості та загрози Web-ресурсів. 2. Технології виявлення уразливостей Web-ресурсів. 3. Уразливості та загрози Web-ресурсів. 4. Класифікація уразливостей.		http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лекція 3	Тема: Вимоги та захист інформації Web-ресурсів від НСД.	1. Класифікація сучасних attacks на Web-додатки. 2. Перелік засобів ЗІ Web-сторінок відповідно до вітчизняної нормативної бази. 3. Вимоги щодо захисту інформації Web-ресурсів.		http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лекція 4	Тема: Основні напрями інформаційної безпеки Web-ресурсів.	1. Визначення основних уразливостей Web-систем на базі client-server. 2. Технології HTTP, SSL/TLS.		http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лекція 5	Тема: Інформаційна та кібербезпека корпоративної організації.	1. Безпека рівня мережевої інфраструктури ОІД. 2. Захист Web-додатків і сучасні напрями розвитку інформаційної та кібербезпеки.		http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лекція 6	Тема: Методи, технології забезпечення інформаційної безпеки Web-додатків.	1. Основні уразливості мережевих Web-додатків та методи їх усунення. 2. Сучасні методи тестування Web-ресурсів. 3. Security vulnerability testing для Web services.		http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лекція 7	Тема: Сканери безпеки Web-додатків в організації. Основи адміністрування сканером уразливостей	1. Базові функції та напрями реалізації AppScan Standart. 2. Основні підходи та принципи роботи.		http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507

		AppScan Standart.	3. Black-box scanning, white-box scanning, glass box scanning.			
	Практичне заняття 1-2	Тема: Основні положення вітчизняної нормативно-правої бази (НПБ) та міжнародних стандартів щодо забезпечення безпеки Web-ресурсів.		1. Вміння застосовувати НПБ в оцінці якості прийнятих рішень щодо виявлення і прогнозування загроз Web-ресурсів.	http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Практичне заняття 3-4	Тема: Вимоги до безпеки Web-ресурсів на основі концептуальних положень міжнародних стандартів та інформаційних джерел.		1. Класифікувати уразливості Web-додатків. 2. Знати ID класів vulnerability. 3. Проводити аналіз attacks.	http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Практичне заняття 5-6	Тема: Проведення тестування захищеності Web-додатків.		1. Методи оцінки уразливостей на основі 10 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: Основи виявлення уразливостей Web-додатків на прикладі AppScan Standart.		1. Принципи сканування vulnerability scanners. 2. Базові функції, напрями реалізації AppScan Standart.	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 сканеру уразливостей AppScan Standart.		1. Основні можливості сканування AppScan Standart. 2. Здатність виконувати повне сканування Web-додатків.	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, налаштування сканування AppScan Standart.		1. Володіти можливостями scanner setup wizard. 2. Вміти проводити вибір та застосовувати analysis systems scanning.	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 і засоби адміністрування інструментів AppScan Standart.		1. Використання політик AppScan Standart. 2. Розкривати можливості аналізу Glass box scanning.	http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507

	Лекція 8	Тема: Функціональні можливості систем сканування Web-ресурсів.	1. Принципи роботи, функції та можливості Vulnerability Scanner Software (VSS). 2. Особливості тестування, сучасні підходи до VSS.		http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лекція 9	Тема: Перспективні напрями розвитку інструментів дослідження уразливостей Web-ресурсів.	1. Принципи застосування WASS, WAVS system. 2. Функціональні можливості. Механізми захисту Web-ресурсів.		http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Практичне заняття 7-8	Тема: Атаки на Web-системи та методи протидії.		1. Знати принципи застосування XSS attack. 2. Уразливості, що призводять до code execution. 3. Використання правильно кодованого виводу бібліотек Anti-XSS.	http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лабораторне заняття 5	Тема: 4. Метод тестування на проникнення.		Володіти загальними методами на проникнення.	http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лабораторне заняття 6	Тема: Природа SQL injection та методи протидії. Переваги та недоліки методів.		1. Базові методи боротьби з вразливістю SQL injection. 2. Виконання сканування на проникнення 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: Засоби сканування Web-сервісів.		1. Kali Linux та основні функції реалізації для тестування проникнення Web-додатків. 2. Базові інструменти Kali Linux Vulnerability Testing .	http://dl.dut.edu.ua/course/view.php?id=1507	http://dl.dut.edu.ua/course/view.php?id=1507
	Лабораторне заняття 8-9	Тема: Додаткові механізми захисту Web-додатків.		1. Методи та сучасні інструменти дослідження уразливостей Web-ресурсів. 2. Приклади реалізації Fairwall systems. 3. Переваги та недоліки Fairwall systems.	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.
2. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью Учебное пособие для вузов.2-е изд., испр.Серия «Вопросы управления информационной безопасностью. Выпуск 1» 2016 г.244 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. Олифер В.Г. Безопасность компьютерных сетей / В. Г. Олифер, Н. А. Олифер. – М. : Горячая линия-Телеком, 2017. – 644 с.
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.
1. ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements
2. Application Security Verification Standard 4:.0 https://www.owasp.org/images/d/d4/OWASP_Application_Security_Verification_Standard_4.0-en.pdf
3. MITRE Common Weakness Enumeration: https://cwe.mitre.org/
4. National Institute of Standards and Technology: https://nvd.nist.gov/vuln-metrics/cvss
5. Open Web Application Security Project: https://www.owasp.org/index.php/Category: OWASP_Code_Review_Project
10. Методи оцінювання, підсумкові звітності за освітньою компонентою
(заліки, екзамени, курсові проекти, тестування)
екзамен
11. Матеріально-технічне забезпечення освітньої компоненти
Лабораторія 419, 420. ПК.