

Програма підвищення кваліфікації викладачів дисципліни «Безпека вебзастосунків» закладів ФПО та П(ПТ)О

1	Розробник	Глазков Роман Миколайович – викладач		
2	Найменування програми	Підвищення кваліфікації викладачів дисципліни «Безпека вебзастосунків» закладів ФПО та П(ПТ)О		
3	Мета програми	Удосконалення методичного та практичного рівнів професійної, компетентності викладачів дисципліни «Безпека вебзастосунків» закладів ФПО та П(ПТ)О, відповідно до державної політики у галузі освіти та забезпечення якості освіти		
4	Напрямок програми	Розвиток професійних компетентностей: знання навчальної дисципліни, фахових методик, технологій		
5	Зміст програми	№ з/п	Тема	Год
		1	Вступ до безпеки вебзастосунків <ul style="list-style-type: none"> • Основи інформаційної безпеки та роль безпеки вебзастосунків. • Методика викладання теми «Загрози для вебзастосунків». 	2
		2	Аутентифікація та авторизація <ul style="list-style-type: none"> • Основи аутентифікації користувачів. • Викладання принципів безпечної авторизації у вебзастосунках. 	4
		3	Захист від SQL-ін'єкцій <ul style="list-style-type: none"> • Принципи роботи SQL-ін'єкцій та їх вплив на безпеку. • Лабораторні заняття з використанням методів захисту від SQL-ін'єкцій. 	4
		4	Захист від XSS-атак <ul style="list-style-type: none"> • Типи та наслідки XSS-атак. • Використання практичних завдань для навчання захисту від XSS-атак. 	4
		5	Захист вебзастосунків від CSRF-атак <ul style="list-style-type: none"> • Механізм роботи CSRF-атак. • Викладання методів захисту вебзастосунків від CSRF-атак. 	4
		6	Управління сесіями та безпека куків <ul style="list-style-type: none"> • Основи управління сесіями у вебзастосунках. • Практичні рекомендації з безпеки куків 	4
		7	Використання протоколів HTTPS і SSL/TLS <ul style="list-style-type: none"> • Принципи роботи HTTPS і роль SSL/TLS у безпеці вебзастосунків. • Викладання налаштування HTTPS для вебзастосунків. 	4
		8	Основи тестування безпеки вебзастосунків <ul style="list-style-type: none"> • Види тестування безпеки: сканування вразливостей, пенетрацінг. • Практичні заняття з використання інструментів тестування безпеки. 	4

		Всього	30
6	Обсяг (тривалість) програми	30 годин / 1 кредит ЄКТС	
7	Форма підвищення кваліфікації	Дистанційна	
8	Вид підвищення кваліфікації	Навчання за програмою підвищення кваліфікації	
9	Перелік компетентностей, що вдосконалюватимуться / набуватимуться	Фахова, методична, аналітична, загальнопедагогічна, освітологічна та нормативно-правова	
10	Документ, що видається за результатами підвищення кваліфікації	Сертифікат про підвищення кваліфікації	
11	Розміщення на вебсайті	http://vectorua.com/	



Контрольні питання до програми

1. Що таке безпека вебзастосунків і які основні загрози існують?
2. Які основні принципи аутентифікації та авторизації у вебзастосунках?
3. Що таке SQL-ін'єкція, і як захистити вебзастосунки від цієї атаки?
4. Які типи XSS-атак існують, і як їм запобігти?
5. Як працюють CSRF-атаки, і які методи захисту можна застосувати?
6. Які принципи управління сесіями забезпечують безпеку вебзастосунків?
7. Що таке HTTPS, і як його налаштування впливає на безпеку вебзастосунків?
8. Які інструменти використовуються для тестування безпеки вебзастосунків?