

Технології захисту хмарних та вебсистем



Спеціальності: E2 Екологія, E4 Науки про Землю, F2 Інженерія програмного забезпечення, F3 Комп'ютерні науки, F4 Системний аналіз та наука про дані, F5 Кібербезпека та захист інформації, F6 Інформаційні системи і технології, F7 Комп'ютерна інженерія, G5 Електроніка, електронні комунікації, приладобудування та радіотехніка, G6 Інформаційно-вимірювальні технології, G7 Автоматизація, комп'ютерно-інтегровані технології та робототехніка, G18 Геодезія та землеустрій, G22 Біомедична інженерія, J6 Авіаційний транспорт

Рівень вищої освіти	другий (магістерський)
Статус дисципліни	вибіркова (Дисципліна індивідуального вибору 3)
Обсяг дисципліни	150 годин/ 5 кредитів ЄКТС
Мова викладання	українська
Анотація	Курс «Технології захисту хмарних та вебсистем» дозволяє отримати знання стосовно способів атак та захисту від атак хмарних та вебсистем, отримати практичні навички роботи з інструментальними засобами тестування на проникнення вебсистем. Розглядаються інструментальні засоби спеціалізованої операційної системи Kali Linux для оцінювання безпеки комп'ютерних систем або мереж засобами моделювання атаки зловмисника. Об'єктами атак є вразливості програмного забезпечення (зокрема вебзастосунків), також розглядаються атаки у дротових та бездротових мережах. Освоєння курсу дозволить отримати знання щодо можливостей інструментальних засобів із виявлення вразливостей, проведення атак для різних об'єктів та забезпечення їх захисту. Мета викладання навчальної дисципліни «Технології захисту хмарних та вебсистем» –засвоєння необхідних знань і отримання навичок ефективного використання інструментальних засобів тестування на проникнення при тестуванні безпеки компонентів інфраструктури. Завдання дисципліни – підготовка висококваліфікованих фахівців, які вміють застосовувати отримані навички при проведенні процедур оцінювання безпеки компонентів інфраструктури. У результаті вивчення навчальної дисципліни студент повинен: знати: – етапи життєвого циклу вразливості; – природу походження поширених вразливостей; – сфери застосування інструментальних засобів тестування безпеки; – функціональні можливості поширених інструментальних засобів тестування безпеки; вміти: – складати план тестування для різних об'єктів; – обирати відповідні інструментальні засоби для окремих задач тестування; – користуватися популярними методологіями пошуку проблем безпеки; – користуватися поширеними інструментальними засобами тестування безпеки. Розроблено і викладається фахівцем, який має науковий досвід (дисертація на здобуття наукового ступеня кандидата технічних наук за тематикою дисципліни) та практичний досвід (адміністрування та налагодження мереж, адміністрування Linux-систем, розроблення та тестування безпеки вебзастосунків, експертиза та усунення наслідків атак вебзастосунків)
Організація навчання	Види занять: лекції, лабораторні заняття. Форми здобуття освіти: денна, заочна. Форми контролю: модульний контроль, іспит
Кафедра	Кафедра комп'ютерних систем, мереж і кібербезпеки
Факультет	Факультет радіоелектроніки, комп'ютерних систем та інфокомунікацій

Викладач		ПІБ	Тецький Артем Григорович
		Посада	старший викладач
		Вчене звання	
		Науковий ступінь	кандидат технічних наук
		e-mail	
Посилання на електронні матеріали курсу	https://mentor.khai.edu/course/view.php?id=9583		
Посилання на силабус			