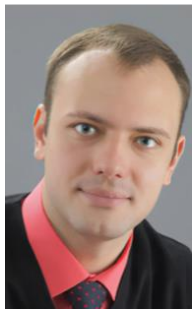


## Навчальна дисципліна

### Засоби тестування на проникнення (пентестингу, білого хакингу)

**Галузі знань:** 10 «Природничі науки», 11 «Математика та статистика»,  
12 «Інформаційні технології», 16 «Хімічна інженерія та біоінженерія»,  
17 «Електроніка, автоматизація та електронні комунікації», 19 «Архітектура та  
будівництво», 27 «Транспорт» (спеціальність 272 *Авіаційний транспорт*)

<b>Рівень вищої освіти</b>	другий (магістерський)		
<b>Статус дисципліни</b>	вибіркова (Дисципліна індивідуального вибору 3)		
<b>Обсяг дисципліни</b>	150 годин/ 5 кредитів ЄКТС		
<b>Мова викладання</b>	українська		
<b>Анотація</b>	<p>Курс «Засоби тестування на проникнення» дозволяє отримати практичні навички роботи з інструментальними засобами тестування на проникнення. 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 Web-серверів та персональних комп'ютерів, також розглядаються атаки у дротових та бездротових мережах. Освоєння курсу дозволить отримати знання щодо можливостей інструментальних засобів із виявлення вразливостей та проведення атак для різних об'єктів.</p> <p><b>Мета</b> викладання навчальної дисципліни – засвоєння необхідних знань, навичок ефективного використання інструментальних засобів тестування на проникнення при тестуванні безпеки компонентів інфраструктури.</p> <p><b>Завдання</b> дисципліни – підготовка висококваліфікованих фахівців, які вміють застосовувати отримані навички при проведенні процедур оцінювання безпеки компонентів інфраструктури.</p> <p>У результаті вивчення навчальної дисципліни студент повинен:</p> <p><b>знати:</b></p> <ul style="list-style-type: none"> <li>– етапи життєвого циклу вразливості;</li> <li>– сфери застосування інструментальних засобів тестування безпеки;</li> <li>– функціональні можливості поширених інструментальних засобів тестування безпеки;</li> </ul> <p><b>вміти:</b></p> <ul style="list-style-type: none"> <li>– складати план тестування для різних об'єктів;</li> <li>– обирати відповідні інструментальні засоби для окремих задач тестування;</li> <li>– користуватися поширеними інструментальними засобами тестування безпеки</li> </ul>		
<b>Організація навчання</b>	<p>Види занять: лекції, лабораторні заняття.          Форми здобуття освіти: денна, заочна.          Форми контролю: модульний контроль, іспит</p>		
<b>Кафедра</b>	Кафедра комп'ютерних систем, мереж і кібербезпеки		
<b>Факультет</b>	Факультет радіоелектроніки, комп'ютерних систем та інфокомунікацій		
<b>Викладач</b>		<b>ПІБ</b>	<b>Тецький Артем Григорович</b>
<b>Посада</b>		старший викладач	
<b>Вчене звання</b>			
<b>Науковий ступінь</b>		кандидат технічних наук	
<b>e-mail</b>			
<b>Посилання на електронні матеріали курсу</b>	<a href="https://mentor.khai.edu/course/view.php?id=8275">https://mentor.khai.edu/course/view.php?id=8275</a>		
<b>Посилання на робочу програму (силабус)</b>	<a href="https://khai.edu/assets/files/silabusi/dp3/503_rp_m_zasobi-testuvannya-na-proniknennya-pentestingu-bilogo-hakingu.pdf">https://khai.edu/assets/files/silabusi/dp3/503_rp_m_zasobi-testuvannya-na-proniknennya-pentestingu-bilogo-hakingu.pdf</a>		