Назва дисципліни, обсяг у кредитах ЄКТС	Захист інформації в мережах ІНТЕРНЕТ (5 кредитів ЄКТС)
Загальна інформація про викладача	Заєць О. П., ст. викладач кафедри ЕОМ т. (056)373-15-89; email: zaets.evm.diit@gmail.com
Семестр, у якому можливе (планується) вивчення дисципліни	Магістрантам - 2 семестр
Факультети/ННЦ, студентам яких пропонується	Факультет “Комп'ютерних технологій і систем”
Перелік компетентностей та результатів навчання, що забезпечує дисципліна	ЗК5. Здатність до пошуку, опрацювання та аналізу інформації з різних джерел. ФК1. Здатність застосовувати практичні методи, методологічні аспекти та комп’ютерну логіку при конструюванні, побудові та схемотехніці апаратних та програмних засобів захисту комп’ютерних систем та мереж, ФК5. Здатність аналізувати, оптимізувати та моделювати складність архітектури комп’ютерних систем та мереж із застосуванням сучасних принципів побудови математичного, програмного, лінгвістичного, технічного та інформаційного забезпечення для захисту інформації. ФК8. Знання основних принципів побудови засобів захисту комп’ютерних систем та мереж, принципів побудови та функціонування їх периферійних засобів. ПРН2. Знати професійно-орієнтовані дисципліни спеціальності. ПРН6. Уміння застосовувати знання і розуміння для розв’язання задач синтезу та аналізу захисних засобів в системах, які характерні обраній спеціальності. ПРН8. Уміння виконувати експериментальні дослідження та застосовувати дослідницькі навички за професійною тематикою. ПРН10. Уміння використовувати набуті знання з спеціальності для знаходження нових, нешаблонних рішень і засобів їх здійснення при проведенні експериментальних досліджень для розв’язку поставлених задач. ПРН12. Уміння опрацьовувати отримані

	спеціальності для знаходження нових, нешаблонних рішень і засобів їх здійснення при проведенні експериментальних досліджень для розв'язку поставлених задач. ПРН12. Уміння опрацьовувати отримані результати, аналізувати та осмислювати їх, представляти результати роботи і обґрунтовувати запропоновані рішення на сучасному науково-технічному і професійному рівні ПРН19. Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення. ПРН20. Відповідально ставитись до виконуваної роботи та досягати поставленої мети з дотриманням вимог професійної етики.
Опис дисципліни	
Попередні умови, необхідні для вивчення дисципліни	Знання мережевих технологій, технологій збереження даних та сучасних мов програмування Інтернет-додатків і принципів їх проектування.
Основні теми дисципліни	1. Класифікація загроз та вразливостей web-додатків. Статистика. Проект OWASP TOP10. 2. Парольний захист web-додатків. Атаки типу brute force. 3. Засоби аутентифікації web-додатків. OAuth Protocol. 4. Міжсайтовий скриптинг. Reflected XSS, Stored XSS, DOM XSS. 5. Вразливості типу Command і File Injections. LFI, RFI. 6. Вразливості типу SQL Injections. 7. Огляд DevSecOps, як ефективного підходу для забезпечення контролю безпеки ІС у мережі Інтернет.
Мова викладання	Українська

Список основної та додаткової літератури	**Основна:** 1. Open Web Application Security Project Top-10 2017. 2. Kimberly Graves. CEH: Official Certified Ethical Hacker Review Guide. – USA: EC-Council, 2007. – 264 с. 3. Jeremiah Grossman. XSS Attacks CROSS SITE SCRIPTING EXPLOITS AND DEFENSE. – USA.: Amazon DS, 2018 – 630 с. 4. Chris Snyder. Pro PHP Security: From Application Security Principles to the Implementation of XSS Defenses – USA.: Amazon DS, 2010 – 368 с. 5. Jonathan LeBlanc. Identity and Data Security for Web Development: Best Practices – UK.: O'Reilly Media, 2016 – 204 с. 6. Certified Information Systems Security Professional Study Guide – USA.: CISSP, 2015 – 901 с. **Додаткова:** 1. Скембрейц Дж., Шема М. Безопасность Web-приложений – готовые решения – М: Издательский дом «Вильямс», 2003 – 384 с. 2. Sunny Wear. Burp Suite Cookbook: Practical recipes to help you master web penetration testing with Burp Suite – USA.: Packt Publishing, 2018 – 358 с.