Силлабус дисципліни

Назва дисципліни, обсяг у кредитах ЄКТС	Захист інформації в мережах ІНТЕРНЕТ (5 кредитів ЄКТС)
Загальна інформація про викладача	Заєць Олексій Петрович, ст. викладач кафедри “Електронні обчислювальні машини”
Семестр, у якому можливе (планується) вивчення дисципліни	Магістратура 2-ий семестр
Факультети/ННЦ, студентам яких пропонується	Факультет “Комп'ютерних технологій і систем”
Перелік компетентностей та результатів навчання, що забезпечує дисципліна	**Компетентності:** 1. Знання типових вразливостей Інтернет додатків, статистики їх виникнення та потенційні ризики та загрози від їх експлуатації. 2. Знати методики виявлення та експлуатації вразливостей web-додатків. 3. Здатність розробляти алгоритмічне та програмне забезпечення, інтернет додатків з використанням сучасних методів і мов програмування, а також засобів і систем автоматизації проектування тощо Здатність проектувати системи та їхні компоненти з урахуванням усіх аспектів їх життєвого циклу та поставленої задачі, включаючи створення, налаштування, експлуатацію, технічне обслуговування та утилізацію. **Результати навчання:** 1. Вміти оцінювати ризики виникнення та експлуатації вразливостей у Інтернет додатках. 2. Вміти виконувати тестування та аналіз web-додатків на вразливості, проводити аудит інфраструктури web-систем. 3. Вміти інтегрувати та розробляти системи захисту web-додатків і проектувати захищені інформаційні системи в мережі

	Інтернет. 4. Вміти оцінювати отримані результати та аргументовано захищати прийняті рішення.
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. Елисеев Н.А., Федоров С.А., Антонов О.Д. ОБЗОР УГРОЗ БЕЗОПАСНОСТИ WEB-ПРИЛОЖЕНИЙ // Вопросы технических наук в свете современных исследований: сб. ст. по матер. V-VI междунар. науч.-практ. конф. № 1(4). – Новосибирск: СибАК, 2018. – С. 18-23. 2. Sunny Wear. Burp Suite Cookbook: Practical recipes to help you master web penetration testing with Burp Suite – USA.: Packt Publishing, 2018 – 358 с.