Дисципліна
«Технології безпеки Web-ресурсів»

Лектор, науковий ступінь, вчене звання, посада	Сашньова М.В., доцент, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки.
Результати навчання	Формування теоретичних знань та практичних навичок з питань захисту вебзастосунків, починаючи з етапів розвідки та пошуку вразливостей, типових вразливостей серверної та клієнтської частини вебзастосунку, а також формування навичок пошуку та виправлення проблем кодування вебзастосунку.
Зміст	Основи конфігурації безпеки Інтернету: протокол передачі гіпертексту; HTTPS (протокол передачі гіпертексту через захищені сокети); протокол SSL (Secure Sockets Layer); симетричне та асиметричне шифрування; використання протоколу простого доступу до об'єктів (SOAP); протокол SMTP (Simple Mail Transfer Protocol); протокол поштового відділення (POP3); протокол доступу до Інтернету (IMAP). Огляд технологій вебавтентифікації. Брандмауери вебдодатків. Огляд топ-10 списку OWASP. Розвідка і уразливості веб-додатків: відкриття веб-сторінки/структури програми; збір інформації в вебзастосунках; Сканування вразливостей веб-додатків. Безпека серверної частини вебдодатків: введення в server-side-уразливості, SQL-ін'єкція, автентифікація та авторизація вебдодатків, XXE-ін'єкція, SSRF–підробка запитів на стороні сервера, вразливості бізнес-логіки, та ін. Безпека клієнтської частини веб-додатків: міжсайтові сценарії (XSS), підробка міжсайтових запитів (CSRF), перехресне спільне використання ресурсів (CORS), вразливості на основі DOM, та ін. Інші вразливості клієнтської частини веб-додатків: небезпечна десеріалізація, отруєння вебкешем, атаки заголовків хостів HTTP, автентифікація OAuth, безпека XML.