Силабус освітнього компонента
Програма навчальної дисципліни

Комплексний тренінг «Безпека веб-застосунків»

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Професійна підготовка, Вибіркова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна, заочна

Семестр
2

Мова викладання
Українська, англійська

Викладачі, розробники

КОРОЛЬ Ольга Григорівна
olha.korol@khpi.edu.ua
кандидат технічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 175, з яких 19 навчальних посібників, 74 статті у закордонних виданнях та фахових виданнях України, 18 патентів на корисну модель, 9 у наукометричній базі Scopus, гарант освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Національна безпека держави» , «Інформаційна безпека держави», «Комплексний тренінг «Безпека веб-застосунків»», у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Комплексний тренінг «Безпека веб-застосунків»" є вибірковою навчальною дисципліною. Складність розроблюваних веб-застосунків зростає з кожним роком, що, в свою чергу, робить важкоздійсненним забезпечення їхньої безпеки. Саме тому, доцільно приділяти особливу увагу критичним проблемам захисту програмного забезпечення. Вміння оцінювати ризики та запобігати вразливостям ще на етапі проектування продукту є вкрай важливою задачею, котра знижує потенційні складності при експлуатації застосунку.

Мета та цілі дисципліни

Формування практичних навичок щодо виявлення та протидії сучасним загрозам в кіберпросторі на основі відпрацювання практичних завдань.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

Компетентності

КЗ1. Здатність застосовувати знання у практичних ситуаціях.
КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 16 год., лабораторні роботи – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Основи програмування, Архітектура та захист сучасних операційних систем, Комплексні системи захисту інформації, Основи кібербезпеки.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Впровадження коду. Виявлення ін'єкцій, таких як SQL, NoSQL, ОС та ін'єкція LDAP, які виникають, коли ненадійні дані надсилаються інтерпретатору як частина команди чи запиту. **Тема 2. Некоректна автентифікація і управління сесією.** Виявлення функцій іплікації, які пов'язані з автентифікацією та керуванням сеансом, що дозволяє зловмисникам компрометувати паролі, ключі або скельні маркери або використовувати інші недоліки впровадження, щоб тимчасово або назавжди припустити особистість інших користувачів.	2
Тема 3. Міжсайтовий скриптинг (XSS). Виявлення веб-додатків та API, які не захищені належним чином. Зловмисники можуть вкрасти або змінити такі слабко захищені дані, щоб вчинити шахрайство з кредитною карткою, крадіжку особи або інші злочини.	2
Тема 4. Небезпечні прямі посилання на об'єкти. Аналіз старих або погано налаштованих процесорів XML оцінюють посилання зовнішніх об'єктів у документах XML. Зовнішні об'єкти можуть використовуватися для розкриття внутрішніх файлів за допомогою обробника URI файлів, обміну внутрішніми файлами, сканування внутрішніх портів, віддаленого виконання коду та відмови в атаці служби. **Тема 5. Небезпечна конфігурація.**	2

Аналіз обмеження щодо дозволених користувачів, які дозволено робити, часто не виконуються належним чином. Зловмисники можуть використовувати ці недоліки для доступу до несанкціонованих функціональних можливостей та / або даних, таких як доступ до облікових записів інших користувачів, перегляд конфіденційних файлів, зміна даних інших користувачів, зміна прав доступу тощо.	
Тема 6. Витік чутливих даних – оцінка конфігурації безпеки. Зазвичай це результат небезпечних конфігурацій за замовчуванням, неповних або спеціальних конфігурацій, відкритого хмарного сховища, неправильно налаштованих заголовків HTTP та багатослівних повідомлень про помилки, що містять конфіденційну інформацію. Не тільки всі операційні системи, рамки, бібліотеки та додатки повинні бути надійно налаштовані, але вони повинні бути виправлені / модернізовані своєчасно.	2
Тема 7. Відсутність контролю доступу до функціонального рівня. Визначення недоліків XSS, які виникають щоразу, коли програма включає недовірені дані на новій веб-сторінці без належної валідації або не відкриття, або оновлює наявну веб-сторінку за допомогою наданих користувачем даних за допомогою API браузера, який може створювати HTML або JavaScript. XSS дозволяє зловмисникам виконувати скрипти в браузері жертви, які можуть захоплювати сеанси користувачів, знищувати веб-сайти або перенаправляти користувача на шкідливі сайти.	2
Тема 8. Підробка міжсайтових запитів (CSRF). Оцінка небезпечної десеріалізації, яка часто призводить до віддаленого виконання коду. Навіть якщо дефери дезаріалізації не призводять до віддаленого виконання коду, їх можна використовувати для виконання атак, включаючи атаки відтворення, атаки ін'єкції та напади ескалації привілеїв.	2
Тема 9. Використання компонентів з відомими уразливостями. Аналіз компонент, таких як бібліотеки, рамки та інші програмні модулі, які працюють із тими ж привілеями, що і додаток. Якщо використовується вразливий компонент, така атака може полегшити серйозні втрати даних або захоплення сервера. Програми та API, що використовують компоненти з відомою вразливістю, можуть підірвати захисні програми та включити різні атаки та впливи.	2
Тема 10. Невалідовані редіректи. Виявлення недостатнього обліку та моніторингу у поєднанні з відсутньою або неефективною інтеграцією з реакцією на інцидент дозволяє зловмисникам надалі атакувати системи, підтримувати стійкість, перетворювати на більші кількості систем, а також підробляти, витягувати або знищувати дані. Більшість досліджень щодо порушення виявляють час виявлення порушення понад 200 днів, як правило, виявляються зовнішніми сторонами, а не внутрішніми процесами чи моніторингом.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Впровадження коду. Розгляд ризиків, пов'язаних із некоректною або небезпечної	4	0,1

вставкою коду в додаток (включно з вхідними даними). Аналіз практик безпечного кодування, валідації та санітизації даних на клієнтському й серверному рівнях. **Тема 2. Некоректна автентифікація і управління сесією.** Вивчення типових помилок у реалізації аутентифікації та сесій (слабкі паролі, неправильне зберігання токенів, незахищені кукі). Методи посилення: багатофакторна автентифікація, безпечні кукі, життєвий цикл сесій.		
Тема 3. Міжсайтовий скриптинг (XSS). Огляд видів XSS (stored, reflected, DOM-based), механізмів виникнення і негативних наслідків. Захисні підходи: екранування/енкодинг, Content Security Policy, належна обробка введення і виходу.	4	0,1
Тема 4. Небезпечні прямі посилання на об'єкти. Аналіз проблем типу Insecure Direct Object References (IDOR): коли користувачі отримують доступ до об'єктів шляхом зміни ідентифікаторів. Практики захисту: перевірка прав доступу на сервері, непрямі ідентифікатори, авторизаційні контролі. **Тема 5. Небезпечна конфігурація.** Виявлення і усунення помилок конфігурації (відкриті директиви, непотрібні сервіси, небезпечні права доступу). Рекомендації щодо жорстких налаштувань сервера, регулярного сканування та зменшення поверхні атак.	4	0,1
Тема 6. Витік чутливих даних — оцінка конфігурації безпеки. Оцінка ризиків витоку PII, кредитних даних, ключів; валідація шифрування у збереженні та передачі; політики обробки даних і захист конфігурацій (секрети/ключі, vault).	4	0,1
Тема 7. Відсутність контролю доступу до функціонального рівня. Розгляд ситуацій, коли API/функції доступні без належної авторизації. Принципи розмежування прав, RBAC/ABAC, валідація прав на сервері та захист внутрішніх ендпоінтів.	4	0,1
Тема 8. Підробка міжсайтових запитів (CSRF). Опис механізмів CSRF-атак і чому вони небезпечні. Методи захисту: CSRF-токени, перевірка Origin/Referer, використання SameSite кукі та безпечних методів зміни стану.	4	0,1
Тема 9. Використання компонентів з відомими уразливостями. Оцінка ризиків сторонніх бібліотек і компонентів (включно з пакетами npm, pip і т.д.). Практики управління залежностями: SCA, регулярні оновлення, білд-сканування та політики прийому залежностей.	4	0,1
Тема 10. Невалідовані редіректи. Розгляд проблем відкритих редіректів і їхніх ризиків (фішинг, обходи політик). Захист: заборона довільних редіректів, білого списку URL, валідація та попередження користувача.	4	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Аналіз уразливостей веб-застосунків. У роботі передбачено аналіз типових вразливостей веб-застосунків, моделювання можливих сценаріїв атак та розробку рекомендацій із безпечного налаштування компонентів веб-додатків. Основна увага приділяється принципам безпечного кодування, контролю доступу та управлінню сесіями.	0,1
Тема 2. Забезпечення стійкості веб-застосунків до атак. Робота спрямована на оцінку безпеки веб-застосунку з позицій виявлення вразливостей, що виникають унаслідок помилок конфігурації, неправильного керування даними чи використання небезпечних бібліотек. Особливу увагу приділено формуванню практичних навичок із тестування безпеки та впровадження захисних механізмів на рівні архітектури застосунку.	0,1
Загалом	$\sum_{i=1}^{m} b_i$=0,2

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1 Основи безпечного програмування у веб-середовищі. Ознайомлення з принципами secure coding, уникнення типових помилок розробників, що призводять до вразливостей.	8
Тема 2. OWASP Top 10 – сучасні тенденції уразливостей веб-додатків. Аналіз актуального рейтингу загроз, методи їх виявлення та рекомендації з усунення.	8
Тема 3. Безпечне керування паролями та токенами доступу. Методи зберігання, передавання й оновлення облікових даних у веб-застосунках.	7
Тема 4. Використання HTTPS і сертифікатів для захисту даних користувачів. Принципи роботи SSL/TLS, сертифікаційні центри, типові помилки налаштування HTTPS.	7
Тема 5. Веб-атаки на рівні API: загрози та методи захисту. Дослідження уразливостей REST і GraphQL API, способи контролю доступу й валідації запитів.	7
Тема 6. Захист від SQL-ін'єкцій та командного ін'єктування. Розгляд методів атак і способів їх запобігання через параметризацію запитів.	7
Тема 7. Безпека JavaScript та клієнтських застосунків. Методи захисту від XSS, підробки DOM, атаки через сторонні скрипти (supply chain attacks).	7
Тема 8. Забезпечення безпеки у контейнеризованих середовищах (Docker, Kubernetes). Вразливості контейнерів, керування секретами, сканування образів на наявність уразливостей.	7
Тема 9. Методи тестування безпеки веб-застосунків (Penetration Testing). Інструменти та етапи пентесту, використання Burp Suite, OWASP ZAP, Nikto.	7

Тема 10. Захист веб-застосунків у хмарних інфраструктурах. Особливості архітектури, розподіл відповідальності між постачальником та користувачем, механізми безпеки у AWS, Azure, GCP.	7
Загальна кількість годин	**72**

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

Рекомендовані курси, тренінги, стажування

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Kali Linux Web Penetration Testing Cookbook, Second Edition (Packt Publishing) [Електронний ресурс]. – Режим доступу : https://www.packtpub.com/product/kali-linux-web-penetration-testing-cookbook-second-edition/9781788991513.
2. Зразок звіту з тестування на проникнення [Електронний ресурс]. – Режим доступу : https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf.
3. Зразок технічного звіту з проникнення [Електронний ресурс]. – Режим доступу : https://tbgsecurity.
4. OWASP Top 10: issues in the 10 most critical security risk categories in your web applications [Електронний ресурс]. – Режим доступу : https://www.sonarqube.org/features/security/owasp/?gads_campaign=Europe-1-Generic&gads_ad_group=OWASP&gads_keyword=owasp%20top%2010&gclid=CjwKCAiAsNKQBhAPEiwAB-I5zQywzTKai6fcrilMphlAn21CRehrI0q9DEjUZNpHUoDt5V_bVpLm4RoClIkQAvD_BwE.
5. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с. [Електронний ресурс]. – Режим доступу : http://kist.ntu.edu.ua/textPhD/tzi.pdf.
6. WEB-технології [Електронний ресурс]: Навчально-довідковий посібник / С.П. Євсеєв, А.М. Ткачов, В.О. Алексієв, Ю.М. Рябуха – Харків : ХНЕУ ім. С. Кузнеця, – Львів: Видавництво «Новий Світ –2000», 2021. – 390 с. [Електронний ресурс]. – Режим доступу : https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Додаткова література

7 Встановлення Metasploitable 2 [Електронний ресурс]. – Режим доступу : https://metasploit.help.rapid7.com/docs/metasploitable-2.
8. Збірка Metasploitable 3 [Електронний ресурс]. – Режим доступу : https://github.com/rapid7/metasploitable3.
9. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. [Електронний ресурс]. – Режим доступу : https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
10. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. [Електронний ресурс]. – Режим доступу : https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

11. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p. [Електронний ресурс]. – Режим доступу : https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,8	0,2		

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, K, І,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено	30.08.2025		**Завідувач кафедри** Сергій ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Ольга КОРОЛЬ