Силабус освітнього компонента

Програма навчальної дисципліни

Веббезпека

Шифр та назва спеціальності
К4 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320

Спеціалізація
-

Кафедра
Кібербезпеки (328)

Освітня програма
Управління інформаційною безпекою

Тип дисципліни
Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
7

Мова викладання
Українська

Викладачі, розробники

ТКАЧОВ Андрій Михайлович

andrii.tkachov@khpi.edu.ua
Кандидат технічних наук, старший науковий співробітник кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: більше 60 публікацій, 25 статей у закордонних виданнях та фахових виданнях України, 6 патентів на корисну модель, гарант освітньо-професійної програми "Національна безпека у сфері кіберзахисту" першого (бакалаврського) рівня вищої освіти.
Детальніше про викладача на сайті кафедри

ДУНАЄВ Сергій Владиславович

Serhii.Dunaiev@cs.khpi.edu.ua
Асистент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: 5, з них 3 статті, що реферуються у науково метричних базах Scopus. Лектор з дисциплін: "Веб-програмування" та інших у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Зараз безпека веб-рішень набуває великого значення тому, що від надійної та продуктивної роботи веб-ресурсів та сервісів будь-якого підприємства залежить ефективність виконання бізнес процесів та безпосередньо рішення завдань просування продукції чи послуг на ринку країни та зарубіжжя. У дисципліні пропонується комплексний погляд з оцінки та побудови контуру безпеки, починаючи з окремого веб-серверу, до взаємодії розподілених сервісів у корпоративній мережі.

Мета та цілі дисципліни

Отримання студентами загальних відомостей про принципи побудови комплексних систем захисту інформації для формування контуру безпеки в інформаційно-комунікаційних системах; придбання навичок з нейтралізації типових загроз, використання протоколів захисту від шкідливого програмного забезпечення та трафіку за допомогою веб-технологій та застосунків.

Формат занять

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

Компетентності

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
СК1. Здатність використовувати безпекові режими під час виконання службових обов'язків.
СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
СК11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

РН3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.
РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки
РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
РН8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
РН9. Вміти використовувати безпекові режими під час виконання службових обов'язків.
РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
РН11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.
РН12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

РН16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
РН17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
РН19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
РН20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
РН22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 150 год. (5 кредитів ECTS): лекції – 32 год., лабораторні роботи – 32 год., самостійна робота – 86 год.

Передумови вивчення дисципліни (пререквізити)

Розробка веб-додатків, Безпека інтернет-речей.

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. Особливості побудови WWW. Архітектура WWW: клієнт–серверна модель. Протоколи передачі даних (HTTP, HTTPS). Основні компоненти веб-середовища (сервери, браузери, проксі). Особливості роботи веб-серверів (Apache, Nginx, IIS).	4
Тема 2. Особливості побудови веб-додатків. Архітектурні стилі веб-додатків (моноліт, клієнт–сервер, мікросервіси). Веб-технології: HTML, CSS, JavaScript, AJAX. Використання баз даних у веб-додатках. Поширені вразливості архітектури веб-додатків.	4
Тема 3. Модель загроз у WWW. Основні категорії загроз (конфіденційність, цілісність, доступність). Класифікація атак: активні та пасивні. Загрози користувачу (фішинг, соціальна інженерія). Загрози веб-додатку та серверу.	4
Тема 4. Засоби збору даних у WWW. Інструменти збору інформації (WHOIS, Shodan, Maltego). Технології веб-скрейпінгу. Роль пошукових систем у зборі даних. Методи OSINT для аналізу веб-ресурсів.	4

Тема 5. Засоби інформаційного аналізу у WWW. Аналіз мережевого трафіку (Wireshark, tcpdump). Журнали веб-серверів і їх інтерпретація. Інструменти тестування безпеки веб-додатків (Burp Suite, OWASP ZAP). Методи аналізу вразливостей.	4
Тема 6. Засоби забезпечення безпеки у WWW. Аутентифікація та авторизація. Використання SSL/TLS та сертифікатів. Веб-фільтрація та WAF (Web Application Firewall). Системи багатофакторної автентифікації.	4
Тема 7. Моделі атак у WWW. Атаки на клієнтську частину (XSS, CSRF). Атаки на серверну частину (SQL Injection, Command Injection). Атаки на сесію (Session Hijacking, Cookie Poisoning). DDoS-атаки на веб-сервіси.	4
Тема 8. Засоби захисту від шкідливого впливу у WWW. Програмні засоби моніторингу та захисту. Системи IDS/IPS у контексті веб-безпеки. Використання проксі-серверів та VPN. Організаційні заходи захисту та політики безпеки.	4
Загальна кількість годин	**32**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Дослідження особливостей побудови WWW. Архітектура клієнт–серверної моделі. Роль протоколів HTTP/HTTPS. DNS та IP-адресація у WWW. Аналіз структури веб-ресурсів.	4	0,1
Тема 2. Дослідження особливостей побудови веб-додатків. Трирівнева архітектура (клієнт, сервер, БД). Використання HTML, CSS, JavaScript. Серверні мови програмування (PHP, Python, Node.js). Особливості інтеграції з базами даних.	4	0,1
Тема 3. Дослідження моделі загроз у WWW. Класифікація загроз (пасивні, активні). Атаки на клієнта (XSS, CSRF). Атаки на сервер (SQL Injection, DoS/DDoS). Витік конфіденційних даних.	4	0,1
Тема 4. Дослідження засобів збору даних у WWW. Використання cookies та сесій. Веб-трекінг і аналітика. Методи web-scraping (автоматизований збір даних). Інструменти збору даних (Wireshark, Burp Suite).	4	0,1
Тема 5. С Дослідження засобів інформаційного аналізу у WWW. Методи аналізу логів веб-серверів. Інструменти OSINT у вебсередовищі. Аналіз трафіку мережі. Виявлення аномалій у поведінці користувачів.	4	0,1
Тема 6. Дослідження засобів забезпечення безпеки у WWW. Шифрування передавання даних (SSL/TLS). Використання VPN для доступу до ресурсів. Засоби автентифікації (однофакторна, двофакторна). Веб-брандмауери (WAF).	4	0,1

Тема 7. Дослідження моделей атак у WWW. SQL Injection: принцип та реалізація. XSS: вбудовані сценарії та наслідки. CSRF: підробка запитів від користувача. DDoS: методи організації та захисту.	4	0,1
Тема 8. Дослідження засобів захисту від шкідливого впливу у WWW. Використання антивірусних рішень та IDS/IPS. Захист від атак ін'єкцій. Технології захисту cookies та сесій. Контроль доступу до веб-додатків.	4	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

За наявності

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Аналіз архітектури та загроз у WWW. Архітектура WWW та веб-додатків. Класифікація загроз та моделей атак. Методи збору та аналізу інформації про веб-ресурси. Приклади реальних кіберзагроз у веб-середовищі.	0,1
Тема 2. Методи та засоби захисту веб-додатків. Засоби аутентифікації та авторизації користувачів. Захист від атак (XSS, SQL Injection, CSRF тощо). Використання WAF, IDS/IPS у веб-безпеці. Криптографічні протоколи та сертифікати у WWW.	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 самостійного вивчення	Кількість годин
Тема 1. Історія розвитку WWW та сучасні тенденції вебтехнологій. Витоки створення WWW: Тім Бернерс-Лі та перші протоколи. Еволюція браузерів і вебсерверів. Перехід від статичних до динамічних вебсторінок. Сучасні тенденції розвитку: Web 2.0, Web 3.0, децентралізований Інтернет.	11
Тема 2. Протоколи прикладного рівня (HTTP, HTTPS, FTP) та їх уразливості. Основи протоколу HTTP та його недоліки. Використання HTTPS та сертифікатів SSL/TLS. Протокол FTP і його вразливості. Типові атаки на протоколи прикладного рівня (MITM, перехоплення трафіку).	11
Тема 3. Методи шифрування вебтрафіку (SSL/TLS, HTTPS). Принципи роботи SSL/TLS. Система цифрових сертифікатів та центри сертифікації. Слабкі місця SSL/TLS та способи їх уникнення. Практичне використання HTTPS у захисті вебдодатків.	11
Тема 4. Системи автентифікації користувачів (OAuth, OpenID, JWT). Основи автентифікації та авторизації. Принципи роботи OAuth 2.0. OpenID Connect як розширення OAuth. Використання JSON Web Token (JWT) для	11

безпечного доступу.	
Тема 5. Основи веб-криптографії: хешування, електронний підпис, сертифікати. Хеш-функції та їх властивості. Використання хешування у вебсистемах (захист паролів, цілісність даних). Електронний підпис та його застосування у вебсередовищі. Роль цифрових сертифікатів у захисті інформації.	11
Тема 6. Вебсервери (Apache, Nginx, IIS): особливості конфігурації та захисту. Архітектура та принципи роботи вебсерверів. Конфігурація безпеки Apache. Захист вебсерверів Nginx та IIS. Типові атаки на вебсервери та методи протидії.	11
Тема 7. Хмарні вебсервіси та особливості їх захисту. Поняття хмарних обчислень (SaaS, PaaS, IaaS). Загрози безпеці у хмарних середовищах. Інструменти захисту даних у хмарі (шифрування, контроль доступу). Міжнародні стандарти безпеки для хмарних сервісів.	10
Тема 8. Міжнародні стандарти та рекомендації щодо веббезпеки (OWASP, ISO/IEC 27001, NIST). Основні положення OWASP Top 10. ISO/IEC 27001: система управління інформаційною безпекою. Рекомендації NIST щодо вебзахисту. Практичне застосування міжнародних стандартів у веброзробці.	10
Загальна кількість годин	**86**

Тематика індивідуальних завдань

Курсовий проєкт передбачає виконання індивідуального звіту, розкривати обрану тематику, демонструвати вміння аналізувати інформацію та оформлювати текстові документи відповідно до мети навчальної дисципліни. Здобувач обирає конкретну тему в межах загальної тематики за погодженням з викладачем. Обсяг роботи: 30–40 сторінок основного тексту. Звіт має бути оформлений відповідно до вимог, наведених у літературному джерелі [2]. Завдання виконується протягом навчальних тижнів і подається на перевірку до екзамену.

Теми індивідуального завдання

Тема 1. Аналіз загроз безпеці вебдодатків та методи їх запобігання. Класифікація сучасних загроз у вебсередовищі. Вплив уразливостей на цілісність, конфіденційність та доступність. Приклади поширених атак на вебдодатки. Огляд методів попередження атак. Розробка рекомендацій щодо підвищення рівня безпеки.
Тема 2. Розробка безпечної системи автентифікації користувачів для вебдодатків. Проблематика зберігання паролів у вебсистемах. Методи автентифікації: паролі, токени, багатофакторна автентифікація. Реалізація безпечного хешування та соління паролів. Використання протоколів OAuth2, OpenID Connect. Тестування безпечності реалізованої системи.
Тема 3. Застосування криптографічних методів у забезпеченні веббезпеки (SSL/TLS, HTTPS). Основи криптографії у веббезпеці. Протоколи SSL/TLS: принципи роботи та структура. Налаштування HTTPS для захисту передавання даних. Проблеми сертифікації та управління ключами. Практичне дослідження захищеності вебз'єднання.
Тема 4. Моделювання та дослідження атак типу SQL Injection та методи захисту від них. Принцип роботи SQL Injection. Види SQL Injection (Classic, Blind, Time-Based). Інструменти для виявлення уразливостей (sqlmap та ін.). Методи захисту: prepared statements, ORM. Практичне дослідження на тестовому вебдодатку.
Тема 5. Використання OWASP Top 10 для оцінки захищеності вебдодатків.

Ознайомлення з OWASP та його значенням. Характеристика OWASP Top 10 (актуальна версія). Методика тестування вебдодатків за OWASP Top 10. Приклад аналізу конкретного вебдодатку. Рекомендації з підвищення захищеності.
Тема 6. Аналіз ефективності засобів захисту від міжсайтових атак (XSS, CSRF). Принципи XSS-атак (Stored, Reflected, DOM-based). Механізм CSRF-атак. Методи виявлення уразливостей у вебдодатках. Засоби протидії XSS і CSRF (Content Security Policy, токени). Практичне тестування захисних механізмів.
Тема 7. Розробка та впровадження системи моніторингу безпеки вебресурсу. Завдання та принципи моніторингу безпеки. Інструменти для моніторингу (Splunk, ELK Stack, Wazuh). Збір і аналіз логів вебсервера. Виявлення та реагування на інциденти. Практичний кейс впровадження моніторингу.
Тема 8. Захист вебсерверів Apache/Nginx: методи конфігурації та тестування уразливостей. Загрози вебсерверам та наслідки компрометації. Безпечне налаштування Apache та Nginx. Використання SSL/TLS у вебсерверах. Тестування конфігурації (Nikto, OpenVAS). Практичні рекомендації для адміністраторів.
Тема 9. Використання міжмережевих екранів (Web Application Firewall, WAF) у захисті вебдодатків. Призначення та принципи роботи WAF. Види WAF: апаратні, програмні, хмарні. Інтеграція WAF у інфраструктуру вебдодатку. Оцінка ефективності роботи WAF. Практичне дослідження (ModSecurity, Cloudflare).
Тема 10. Дослідження безпеки хмарних вебсервісів та механізмів їх захисту. Особливості архітектури хмарних вебсервісів. Загрози та уразливості хмарних середовищ. Технології забезпечення безпеки (IAM, шифрування, резервування). Інструменти аудиту безпеки хмарних вебсервісів. Практичні рекомендації щодо підвищення безпеки.
Загальна кількість годин **86**

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. CCNA Cybersecurity Operations [Електронний ресурс]. – Режим доступу: https://www.netacad.com/ru/courses/cybersecurity/cyberops-associate.
2. Amazon Web Services (AWS) [Електронний ресурс]. – Режим доступу: https://www.checkpoint.com/solutions/amazon-aws-security/.
3. Microsoft Azure (Azure) [Електронний ресурс]. – Режим доступу: https://www.checkpoint.com/solutions/microsoft-azure-security/.
4. Google Cloud Platform (GCP) [Електронний ресурс]. – Режим доступу: https://www.checkpoint.com/solutions/google-cloud-platform-security/.
5. Kali Linux [Електронний ресурс]. – Режим доступу : https://www.kali.org/.

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.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

Додаткова література

1 Internet Security [Електронний ресурс]. – Режим доступу: https://www.tutorialspoint.com/internet_security/index.htm.
2. Computer Network Security [Електронний ресурс]. – Режим доступу: https://www.javatpoint.com/computer-network-security.
3. Веб-безпека [Електронний ресурс]. – Режим доступу: https://developer.mozilla.org/ru/docs/Learn/Server-side/First_steps/Website_security

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
0,6	0,2	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

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

цілого числа в більшу сторону.

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** Роман КОРОЛЬОВ