Силабус освітнього компонента

Програма навчальної дисципліни

WEB-безпека

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
Науково-професійного спрямування, Вибіркова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна

Семестр
3

Мова викладання
Українська

Викладачі, розробники

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

ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Лауреат національної премії імені Бориса Патона.
Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статтей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: Математичні основи криптології, Комп`ютерні мережі, Основи криптографічного захисту, Методи криптоаналізу, Основи кібербезпеки, Сучасні проблеми постквантової криптографії, Основи наукових досліджень, Цифрова

криміналістика, Етичний хакінг у студентів бакалавріата та магістратури, Методологія наукової та педагогічної діяльності в науках кіберзахисту для аспірантів.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Вивчення основ веб-безпеки, зосереджуючи увагу на загрозах, вразливостях та методах захисту веб-додатків. У рамках курсу студенти ознайомляться з ключовими концепціями, інструментами та практиками, необхідними для забезпечення безпеки веб-систем. Курс включає теоретичні лекції та практичні лабораторні роботи.

Мета та цілі дисципліни

Метою курсу є надання студентам знань та навичок, необхідних для виявлення, аналізу та усунення вразливостей веб-додатків, а також розробки та реалізації стратегій захисту від кіберзагроз.

Формат занять

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

Компетентності

КЗ–1. Здатність застосовувати знання у практичних ситуаціях.
КЗ–2. Здатність проводити дослідження на відповідному рівні.
КЗ–3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ–4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
КЗ–5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
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.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань нформаційної безпеки та/або кібербезпеки.

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.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
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.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
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.
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
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.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
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.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
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)

Іноземна мова, Основні поняття про веб-безпеки.

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. Вступ до WEB-безпеки. Ознайомлення з основними поняттями, принципами та цілями веб-безпеки. Розгляд сучасних загроз у мережі, моделей безпеки та методів забезпечення захисту веб-додатків.	4
Тема 2. Вразливості веб-додатків. Огляд найпоширеніших вразливостей (SQL Injection, XSS, CSRF тощо). Аналіз основних типів вразливостей, механізмів їх виникнення та способів виявлення. Розгляд практичних прикладів атак та методів їх запобігання.	4
Тема 3. Аутентифікація та авторизація. Дослідження методів перевірки користувачів (аутентифікації) та контролю доступу до ресурсів (авторизації). Порівняння технологій OAuth, OpenID, JWT та реалізація безпечних механізмів сесій.	2
Тема 4. Шифрування та захист даних. Вивчення принципів криптографії у веб-додатках. Використання SSL/TLS для захищених з'єднань. Методи зберігання та передавання конфіденційних даних.	2
Тема 5. Інструменти для тестування безпеки. Ознайомлення з сучасними інструментами для пошуку вразливостей (Burp Suite, OWASP ZAP, Nikto). Методи автоматичного та ручного тестування безпеки веб-додатків.	2

Тема 6. Реакція на інциденти та управління ризиками. Розгляд процесів виявлення, аналізу та реагування на інциденти безпеки. Стратегії управління ризиками, планування заходів із відновлення після атак і формування політики безпеки організації.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Аналіз веб-додатка на вразливості. Проведення огляду тестового веб-додатку для ідентифікації потенційних вразливостей (структура, вхідні точки, форми, API). Формування списку ризиків, пріоритезація вразливостей та підготовка рекомендацій щодо їхнього усунення — без експлуатації у реальному середовищі.	6	0,2
Тема 2. Моделювання сценаріїв SQL-ін'єкцій (у контрольованому середовищі). Вивчення природи SQL-ін'єкцій на ізольованому стенді — демонстрація механізмів виникнення та впливу на цілісність/конфіденційність даних. Аналіз методів виявлення (логування, WAF, параметризовані запити) та реалізація захисних практик.	6	0,2
Тема 3. Дослідження XSS-вразливостей (відкритих і DOM-типів). Виявлення й класифікація XSS-проблем у тестовому застосунку, аналіз шляхів потрапляння небезпечних скриптів і їхніх наслідків. Оцінка заходів захисту: екранування/енкодинг, CSP, безпечна обробка вводу на клієнті й сервері.	5	0,1
Тема 4. Реалізація безпечної системи аутентифікації на простому веб-додатку. Проєктування та налаштування механізмів безпечної аутентифікації (строгі правила паролів, соль+хешування, робота з токенами/сесіями, MFA-ідеї) у тестовому додатку; оцінка слабких місць і рекомендації щодо покращення.	5	0,1
Тема 5. Налаштування веб-сервера для підтримки HTTPS. Розгортання тестового веб-сервера з вимкненим/включеним HTTPS, ознайомлення з сертифікатами (CA, самопідписані), налаштуванням TLS-профілів, політик безпеки (HSTS) та перевіркою конфігурації на предмет слабких шифрів і помилок, з подальшими рекомендаціями.	5	0,1
Тема 6. Моделювання сценарію інциденту безпеки та розробка плану реагування. Відтворення контрольованого інциденту (симуляція виявлених проблем у тестовому середовищі), збір і аналіз логів, визначення причини, оцінка впливу та формування детального плану реагування і відновлення (повідомлення, усунення, запобігання повторенню).	5	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 вразливостей та методи їх усунення. Теоретичне та практичне опрацювання основних типів веб-вразливостей (SQL Injection, XSS, CSRF). Студенти повинні пояснити механізми виникнення атак, запропонувати шляхи їх запобігання та навести приклади безпечного коду.	0,1
Тема 2. Механізми захисту та реагування на інциденти. Аналіз методів шифрування, аутентифікації й авторизації у веб-додатках. Розгляд сценаріїв реагування на інциденти безпеки, управління ризиками та розробка рекомендацій щодо підвищення рівня захищеності веб-системи.	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. OWASP Top 10: сучасні вразливості веб-додатків. Ознайомлення з десяткою найпоширеніших типів атак за класифікацією OWASP, їх наслідками та способами запобігання.	8
Тема 2. Безпека RESTful API та GraphQL API. Методи захисту веб-API від атак (автентифікація, контроль доступу, rate limiting, валідація запитів).	8
Тема 3. Безпечне управління сесіями та кукі-файлами. Політики зберігання даних сесій, атрибути cookie (Secure, HttpOnly, SameSite), запобігання викраденню сесій.	7
Тема 4. Політики контентної безпеки (CSP) та захист від XSS-атак. Використання CSP для контролю скриптів, стилів та джерел контенту у браузері.	7
Тема 5. Використання Web Application Firewall (WAF). Призначення, принципи роботи та типові налаштування WAF для захисту веб-додатків.	7
Тема 6. Безпека CMS-систем (WordPress, Joomla, Drupal). Аналіз основних вразливостей у популярних системах керування контентом та практики їх захисту.	7
Тема 7. Захист веб-додатків у хмарному середовищі. Особливості безпеки веб-сервісів, що розгортаються у AWS, Azure або Google Cloud.	7
Тема 8. Соціальна інженерія та фішинг у веб-середовищі. Методи виявлення, приклади атак та рекомендації щодо підвищення обізнаності користувачів.	7
Тема 9. Безпечне використання JavaScript і сторонніх бібліотек.	7

Ризики, пов'язані з використанням зовнішніх скриптів, та засоби перевірки їхньої цілісності (Subresource Integrity).	
Тема 10. Автоматизація тестування безпеки веб-додатків. Використання інструментів (OWASP ZAP, Burp Suite, Nikto тощо) для автоматизованого пошуку вразливостей у тестовому середовищі.	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. OWASP (Open Web Application Security Project) - owasp.org
2. "Web Security for Developers" by Malcolm McDonald
https://www.amazon.com/Web-Security-Developers-Malcolm-%E2%80%90McDonald/dp/1593279949
3. "The Web Application Hacker's Handbook" by Dafydd Stuttard and Marcus Pinto
https://books.google.com/books?id=jN6cDprdnd0C&printsec=frontcover&utm_source=chatgpt.com
4. "Web Application Security: A Beginner's Guide" by Bryan Sullivan and Vincent Liu
5. "The Art of Deception" by Kevin Mitnick.

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** Станіслав МІЛЕВСЬКИЙ