ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра інженерії програмного забезпечення та кібербезпеки

ЗАТВЕРДЖЕНО
вченою радою ДТЕУ
(пост. п. 7-9 від «24» 02 2023 р.)
Ректор
_____ Анатолій МАЗАРАКІ

ТЕХНОЛОГІЇ БЕЗПЕКИ ПРОГРАМНИХ ПРОДУКТІВ
SECURITY TECHNOLOGIES OF SOFTWARE PRODUCTS

ПРОГРАМА /
COURSE SUMMARY

Київ 2023

Автори: Н.О. КОТЕНКО, кандидат педагогічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Т.О. ЖИРОВА, кандидат педагогічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Ю.В. КОСТЮК, PhD, старший викладач кафедри інженерії програмного забезпечення та кібербезпеки
Л.І. КОВАЛЬОВА, спеціаліст кафедри інженерії програмного забезпечення та кібербезпеки

Програму розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки «30» травня 2023 р., протокол №36 .

Рецензенти: Л.О. ВЛАСЕНКО, к.т.н., доцент кафедри інженерії програмного забезпечення та кібербезпеки;
О.О. РУДЕНКО, SFCC Front-End Team Lead, Raccoon LLC

ТЕХНОЛОГІЇ БЕЗПЕКИ ПРОГРАМНИХ ПРОДУКТІВ /
SECURITY TECHNOLOGIES OF SOFTWARE PRODUCTS

ПРОГРАМА /
COURSE SUMMARY

ВСТУП

Програма дисципліни «Технології безпеки програмних продуктів» призначена для студентів освітнього ступеня «магістр» галузі знань 12 «Інформаційні технології» спеціальності 121 «Інженерії програмного забезпечення», освітньо-професійної програми «Управління проєктами програмних продуктів»

Програму підготовлено відповідно до Стандарту вищої освіти України за даною спеціальністю та відповідної освітньо-професійної програми підготовки магістрів.

Програма складається з таких розділів:

1 Мета, завдання та предмет дисципліни.

2 Передумови вивчення дисципліни як вибіркової компоненти освітньо-професійної програми.

3 Результати вивчення дисципліни.

4 Зміст дисципліни.

5 Список рекомендованих джерел.

1. МЕТА, ЗАВДАННЯ ТА ПРЕДМЕТ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни «Технології безпеки програмних продуктів» є формування у майбутніх спеціалістів умінь та компетностей для оцінювання та забезпечення необхідного рівня захищеності програмних продуктів, оволодіння практичними методами захисту програмних продуктів від різних типів загроз.

Завданням дисципліни є формування теоретичних знань та практичних навичок з питань захисту програмних продуктів, зокрема вебзастосунків та мобільних застосунків, починаючи з етапів розвідки та пошуку вразливостей, типових вразливостей серверної та клієнтської частини застосунків, а також формування навичок пошуку та виправлення проблем кодування в додатку.

Предметом вивчення дисципліни є сукупність теоретичних і практичних проблем, які пов’язані із захистом програмних продуктів на етапах їх розробки та експлуатації.

2. ПЕРЕДУМОВИ ВИВЧЕННЯ ДИСЦИПЛІНИ ЯК ВИБІРКОВОЇ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ

знання: основ кібербезпеки, ООП, веб програмування;

вміння: працювати з офісними додатками Microsoft, хмарними сервісами Office 365, пошуковою системою Google.

3. РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ

Дисципліна «Технології безпеки програмних продуктів», як обов'язкова компонента освітньої програми, забезпечує оволодіння студентами загальними та фаховими компетентностями і досягнення ними програмних результатів навчання за відповідною освітньо-професійною програмою:

Управління проєктами програмних продуктів (ОС магістр)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компе-тентності
Загальні компетентності за освітньою програмою		
ЗК01	Здатність до абстрактного мислення, аналізу та синтезу	1-15
ЗК02	Здатність спілкуватися іноземною мовою як усно, так і письмово.	2-11
ЗК03	Здатність проводити дослідження на відповідному рівні.	2-11
Фахові компетентності за освітньою програмою		
СК04	Здатність розвивати і реалізовувати нові конкурентоспроможні ідеї в інженерії програмного забезпечення.	1-12
СК07	Здатність критично осмислювати проблеми у галузі інформаційних технологій та на межі галузей знань, інтегрувати відповідні знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах	1-12
СК10	Здатність використовувати підходи до управління проєктами програмних продуктів та їх захисту, які застосовуватимуться протягом проєкту.	1-12
Програмні результати навчання за освітньою програмою		
РН07	Аналізувати, оцінювати і застосовувати на системному рівні сучасні програмні та апаратні платформи для розв'язання складних задач інженерії програмного забезпечення	3-12

РН12	Приймати ефективні організаційно-управлінські рішення в умовах невизначеності та зміни вимог, порівнювати альтернативи, оцінювати ризики	1-12
РН16	Планувати, організовувати та здійснювати тестування, верифікацію та валідацію програмного забезпечення.	1-12
РН19	*Вміти вибирати й автоматизовано налаштовувати технологію управління програмними продуктами згідно з життєвим циклом програмного продукту та їх захист.*	1-12

4. ЗМІСТ ДИСЦИПЛІНИ

Тема 1. Основні принципи безпеки програмних продуктів

Вступ. Мета та завдання дисципліни. Огляд загальних принципів безпеки (визначення основних термінів та понять у галузі безпеки програмного забезпечення). Загрози та атаки на програмне забезпечення. Класифікація загроз та атак, які можуть бути спрямовані на програми; аналіз ризиків із зазначенням потенційних наслідків.

Список рекомендованих джерел

Основний: 4 [с. 4-56]
Додатковий: 9 [с. 5-72]
Інтернет-джерела: 10, 11, 12, 13, 19

Тема 2. Системний аналіз безпеки програмного забезпечення

Системний аналіз безпеки програмного забезпечення.
Інтеграція безпеки в архітектуру програмних систем.
Використання сучасних платформ для забезпечення безпеки.
Вплив апаратного забезпечення на безпеку програмного забезпечення.

Список рекомендованих джерел

Основний: 2 [с. 18-56]
Додатковий: 6 [с. 34-48], 7 [с. 14-31], 8 [с. 6-55]
Інтернет-джерела: 10, 11, 12, 13, 19

Тема 3. Архітектура безпеки програмного забезпечення.

Архітектура безпеки програмного забезпечення.
Розробка та оцінка безпечних архітектурних рішень.
Моделювання загроз у архітектурі програмного забезпечення.
Стратегії безпечного дизайну програмних систем.
Оцінка ефективності архітектурних рішень у розрізі безпеки.

Список рекомендованих джерел

Основний: 3 [с. 14 - 167]
Додатковий: 6 [с. 48 - 110]
Інтернет-джерела: 10, 14, 15, 19

Тема 4. Організаційні аспекти безпеки програмного забезпечення.

Організаційні аспекти безпеки програмного забезпечення.

Управлінські рішення у сфері безпеки інформації.
Порівняння альтернатив для безпеки на рівні організації.
Оцінка ризиків та управління ними в умовах невизначеності.
Впровадження політик та стандартів безпеки.

Список рекомендованих джерел

Основний:3 [с. 168-220], 4 [с. 24-127], 5 [с. 143-159]
Додатковий: 6 [с. 216-234], 9 [с. 118-160]
Інтернет-джерела: 10, 15, 16

Тема 5. Методи тестування безпеки програмного забезпечення.

Методи тестування безпеки програмного забезпечення.
Розробка тестових сценаріїв для перевірки безпеки.
Автоматизоване тестування на наявність вразливостей у ПЗ.
Використання інструментів для аналізу безпеки.
Тестування захисту від атак в реальному середовищі.

Список рекомендованих джерел

Основний: 4 [с. 128-157]
Додатковий: 6 [235-284]
Інтернет-джерела: 10, 15, 16

Тема 6. Верифікація та валідація безпеки програмного забезпечення.

Верифікація та валідація безпеки програмного забезпечення.
Методи верифікації безпеки.
Валідація функціональних вимог з точки зору безпеки.
Валідація відповідності стандартам безпеки.
Інструменти для підтримки верифікації та валідації.

Список рекомендованих джерел

Основний: 4 [с. 160-204]
Додатковий: 6 [с. 285-312]
Інтернет-джерела: 10, 15, 16

Тема 7. Управління безпекою в життєвому циклі програмного продукту.

Управління безпекою в життєвому циклі програмного продукту.

Вибір технологій для управління безпекою.
Автоматизація процесів управління безпекою.
Інтеграція безпеки у життєвий цикл розробки ПЗ.
Управління змінами в контексті безпеки.

Список рекомендованих джерел

Основний: 3 [с. 220-243]
Додатковий: 6 [с. 320-375]
Інтернет-джерела: 10, 15, 16

Тема 8. Аудит безпеки програмного забезпечення.

Аудит безпеки програмного забезпечення.
Методи проведення аудиту безпеки.
Оцінка ефективності існуючих заходів безпеки.
Розробка рекомендацій на основі результатів аудиту.
Документування та звітування про результати аудиту.

Список рекомендованих джерел

Основний: 3 [с. 243-306]
Додатковий: 6 [с. 375-401]
Інтернет-джерела: 10, 15, 16

Тема 9. Інтеграція безпеки в DevOps і CI/CD.

Безпека в процесах Continuous Integration/Continuous Deployment (CI/CD). Інтеграція безпеки в DevOps і CI/CD. Впровадження автоматизованих тестів безпеки в CI/CD.

Інструменти для інтеграції безпеки в CI/CD.

Оцінка ефективності автоматизованих тестів. Управління конфігурацією та секретами.

Безпечне зберігання та управління конфіденційною інформацією. Інструменти для автоматизації управління конфігураціями. Інтеграція безпеки в мікросервісну архітектуру.

Виклики безпеки в контейнеризованих середовищах.

Контейнерна безпека та управління вразливостями.

Список рекомендованих джерел

Основний: 3 [с. 306-320]
Додатковий: 8 [с. 87-124]

Інтернет-джерела: 10, 11, 15, 16

Тема 10. Безпека в багатокористувацьких системах та блокчейн-технології.

Безпека в багатокористувацьких системах та блокчейн-технології.

Протоколи консенсусу та їх вплив на безпеку.

Механізми консенсусу в блокчейн-системах.

Уразливості і атаки на протоколи консенсусу. Оцінка безпеки різних алгоритмів консенсусу.

Механізми захисту даних у блокчейн-системах.

Захист приватності в блокчейні.

Анонімність та конфіденційність транзакцій.

Управління ідентифікацією та доступом у блокчейні.

Атаки на блокчейн та захист від них.

Типи атак на блокчейн-системи.

Розробка стратегій захисту від атак.

Список рекомендованих джерел

Основний: 3 [с. 320-328]

Додатковий: 8 [с. 125-164]

Інтернет-джерела: 10, 15, 16

Тема 11. Політики та технології для забезпечення конфіденційності в програмному забезпеченні.

Політики та технології для забезпечення конфіденційності в програмному забезпеченні.

Вбудовані технології конфіденційності. Методи вбудованого захисту даних. Оцінка впливу на продуктивність систем. Виявлення типових помилок і способи їх уникнення.

Список рекомендованих джерел

Основний:5 [с.300-362]

Додатковий: 7 [с.14-153]

Інтернет-джерела: 10, 15, 16

Тема 12. Динамічне управління безпекою в умовах змінюваних загроз.

Динамічне управління безпекою в умовах змінюваних загроз.

Прогнозування і моделювання загроз.

Використання статистичних та машинних методів для моделювання загроз.

Інструменти для динамічного моніторингу загроз.

Адаптивні стратегії безпеки.

Інтеграція автоматичних реакцій на нові загрози.

Використання ML для виявлення нових загроз.

Список рекомендованих джерел

Основний:4 [с. 204-220]

Додатковий: 7 [с.154-170]

Інтернет-джерела: 17, 18, 20

5. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В.Л.Бурячок, А.О.Аносов, В.В.Семко, В.Ю.Со-колов, П.М.Складанний. –К.:КУБГ, 2019. – 218с.

2. Anoop Singhal, Theodore Winograd, Karen Scarfone. Guide to secure web services. National Institute of Standards and Technology Special Publication 800-95, 2017. - 128 Pages

3. Elie Saad, Rick Mitchell. Owasp Testing Guide v4. Open Web Application Security Project, 2020. - 453 Pages

4. Andrew Homan. Web Application Security Exploitation and Countermeasures for Modern Web Applications. United States of America, 2020. – 331 *Pages.* ISBN: 978-1-492-08796-0

5. Justin Clarke. SQL Injection Attacks and Defense. Syngress Publishin g, Inc., Elsevier, Inc., 2019 - 494 Pages. ISBN 13: 978-1-59749-424-3

Додатковий

6. Kimberly Graves. Certified Ethical Hacker Study Guide. Wiley Publishing, Inc., Indianapolis, Indiana, 2020. - 439 Pages. ISBN: 978-0-470-52520-3

7. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. /В.Л. Бурячок, С.В. Толюпа, В.В. Семко, Л.В. Бурячок, П.М. Складанний, Н.В. Лукова-Чуйко / –К.: ДУТ -КНУ, 2016. –178 с. ISBN 978–617–7092–78–9

8. Bertino E., Martino L.D., Paci F., Squicciarini A.C. Security for Web Services and Service Oriented Architectures Springer, 2020. – 231 p. –ISBN 978-3-540-87741-7.

9. Хорошко О.В. Захист систем електронних комунікацій: навч.посіб./ В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с.

Інтернет-джерела

10. The Open Web Application Security Project® (OWASP) - foundation that works to improve the security of software. URL: https://owasp.org/

11. ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements. URL: https://www.certification.ua/wp-content/uploads/2018/03/ISO_27001_2013_%D0%9C%D0%9D%D0%A1-%D0%93%D0%A0%D0%A3%D0%9F%D0%9F.pdf

12. National Institute of Standards and Technology: URL: https://nvd.nist.gov/vuln-metrics/cvss

13. Holistic Info-Sec for Web Developers. URL: https://holisticinfosecforwebdevelopers.com/

14. Welcome to the OWASP Top 10 – 202. URL: https://owasp.org/Top10/

15. OWASP Top 10. URL: https://tryhackme.com/room/owasptop10

16. OWASP Top 10.Course. URL: https://www.cybrary.it/course/owasp/

17. Website Security. How to Secure & Protect Your Website. URL: https://sucuri.net/guides/website-security/

18. Як захистити веб-додатки: основні поради, інструменти, корисні посилання. URL: https://echo.lviv.ua/dev/6231

19. Національний інститут стандартів і технологій. URL: https://www.nist.gov/

20. Free website security check & malware scanner (дослідження загроз, база даних сигнатур шкідливих програм і статистика). URL: https://sitecheck.sucuri.net/

21. Тестування мобільних додатків. URL: https://qagroup.com.ua/publications/testuvannia-mobilnykh-dodatkiv-vid-a-do-ia/

22. Підходи до тестування мобільних додатків. URL: https://training.qatestlab.com/blog/technical-articles/approaches-to-testing-mobile-applications/

Наукові публікації відповідно до тем дисципліни:

23. Куперштейн, Л., Луцишин, Г., & Кренцін , М. (2024). ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ МОНІТОРИНГУ БЕЗПЕКИ ДАНИХ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 71–84. https://doi.org/10.28925/2663-4023.2024.23.7184

24. Скіцько, О., Складанний, П., Ширшов, Р., Гуменюк, М., & Ворохоб, М. (2023). ЗАГРОЗИ ТА РИЗИКИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 6–18. https://doi.org/10.28925/2663-4023.2023.22.618

25. Добришин, Ю., Сидоренко, С., & Ворохоб, М. (2023). АВТОМАТИЗОВАНА СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕННЯ ЩОДО ВІДНОВЛЕННЯ ПОШКОДЖЕНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВНАСЛІДОК ВПЛИВУ КІБЕРАТАК . *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *4*(20), 174–182. https://doi.org/10.28925/2663-4023.2023.20.174182

26. Авраменко, О. А. (2012). Організація тестування програмного забезпечення при оцінюванні його безпеки. *Eastern-European Journal of Enterprise Technologies*, *6*(2(54), 37–41. https://doi.org/10.15587/1729-4061.2011.1923

27. Milov, O., Hrebeniuk, A., Nalyvaiko, A., Nyemkova, E., Opirskyy, I., Pasko, I., Rzayev, K., Salii, A., Synytsina, U., & Soloviova, O. (2020). Розробка просторово-часової структури методології моделювання поведінки антагоністичних агентів системи безпеки. *Eastern-European Journal of Enterprise Technologies*, *6*(2 (108), 30–52. https://doi.org/10.15587/1729-4061.2020.218660

28. Lakhno V., Akhmetov B., Mohylnyi H., Chubaievskyi V., Kryvoruchko O., Desiatko A. Multi-criterial optimization composition of cyber security circuits based on genetic algorithm // Journal of Theoretical and Applied Information Technologythis. 2022. Vol. 100. № 7. P. 1996–2006.

29. Lakhno V., Bereke M., Adilzhanova S., Chubaievskyi V., Desiatko A., Palaguta K. Genetic algorithm for solving the problem of scaling a cloud-oriented object of informatization // Journal of Theoretical and Applied Information Technologythis link is disabled. 2022. Vol. 100. № 6. P. 1693–1705.

30/ Lakhno V., Akhmetov B., Chubaievskyi V., Desiatko A., Palaguta K., Blozva A., Chasnovskyi Y. Information security audit method based on the use of a neuro-fuzzy system // Proceedings of the 5th Computational Methods in Systems and Software 2021. Springer, Cham, 2021. P. 171–184.