Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Кафедра управління інформаційною безпекою

«Допущено до захисту»
Начальник кафедри УІБ
д.т.н. доц. Ткачук Р.Л.
_____
“____” _____2022 року

БАКАЛАВРСЬКА

КВАЛІФІКАЦІЙНА РОБОТА

на тему

Методи та засоби забезпечення захисту інформації при проектуванні web-додатка університету

Виконала:
студентка IV курсу, групи КБ-41,
спеціальності (освітньої-професійної програми)
125 “Кібербезпека”_____
(Управління інформаційною безпекою)_____
(шифр і назва спеціальності (освітньої-професійної програми)
Пожичкевич Катерина Романівна
(прізвище, ім’я, по батькові)

Керівник_____Ящук В.І.
(прізвище та ініціали)

Рецензент
(прізвище та ініціали)

Львів – 2022

АНОТАЦІЯ

Пожичкевич Катерина Романівна «**Методи та засоби забезпечення захисту інформації при проектуванні web-додатка університету»**
(П.І.Б.) (тема кваліфікаційної роботи)

Кваліфікаційна робота на здобуття вищої освіти ступеня “бакалавр” за освітньо-професійною програмою Управління інформаційною безпекою зі спеціальності 125 - Кібербезпека. – Львівський державний університет безпеки життєдіяльності. Львів. 2022.

У роботі розглянуто теоретичні, науково-методичні та організаційно-функціональні основи захисту інформації та аналіз інформаційної безпеки. Окреслено інструментарій наукового пізнання інформаційної безпеки та процесу її забезпечення. Узагальнено класифікаційні ознаки загроз інформаційної безпеки. Визначено сучасні підходи до захисту інформаційної безпеки на прикладі додатку. Наведено методичні підходи до формування концепції та структури автоматизованої системи управління захистом інформаційної безпеки. Проаналізовано стандарти, рекомендації, етапи щодо попередження загроз інформаційної безпеки. Запропоновано модель захисту веб-додатку від хакерських атак та наведено методику взлому платформи. Розроблено та візуалізовано веб-додаток для ЛДУБЖД.

Ключові слова: інформаційна безпека, захист інформаційної безпеки, загрози,проектування веб-додатка.

ANNOTATION

Pozhychkevych Kateryna Rovanivna "Methods and means of ensuring the protection of information in the design of web-application of the university"

(Name) (topic of qualification work)

Qualification work for obtaining a bachelor's degree in higher education according to the educational and professional program of the Information Security Department in the specialty 125 - Cybersecurity. - Lviv State University of Life Safety. Lviv. 2022

Theoretical, scientific-methodical and organizational-functional bases of information protection and information security analysis are considered in the work. The tools of scientific knowledge of information security and the process of its provision are outlined. The classification features of information security threats are generalized. Modern approaches to information security protection are identified on the example of the application. Methodical approaches to the formation of the concept and structure of the automated information security management system are presented. Standards, recommendations, stages of prevention of information security threats are analyzed. The model of protection of the web application against hacker attacks is offered and the technique of hacking of a platform is resulted. Developed and visualized web application for LDUBZD.

Keywords: information security, information security protection, threats, web application design.

ЗМІСТ

ВИСНОВКИ

У кваліфікаційній роботі розкриваються аспекти створення веб-додатка та забезпечення його захисту. Описано основні способи захисту інформації. Розглянуто особливості створення додатку, проаналізовано та описано запропоновані способи збереження інформації.

Також було визначено, що взлом інформації означає протиправне оволодіння інформацією, що не має бути поширена, незалежно від того, яким шляхом її отримано. Політика безпеки (ПБ) являє собою сукупність принципів, правил, процедур і практичних рішень, які захищають інформацію. ПБ повинна враховувати сучасний стан та найближчі перспективи розвитку інформаційних технологій. Програмно-технічний рівень протидії загрозам ІБ передбачає такі механізми безпеки як аутентифікація користувача, протоколювання ,криптографію, екранування каналів зв'язку.

До атак, які загрожують додаткам відносять сукупність умов і факторів, що створюють небезпеку. Загроза інформації розглядається як порушення конфіденційності, цілісності або доступності даних, а також втрату або знищення даних. Класифікація загроз здійснюється за багатьма ознакам, що дозволяє добирати та застосовувати ефективні методи та засоби захисту.Витік інформації означає незаконне отримання даних, що не мають бути поширені.

Було досліджено та створено чіткий структурований підхід до проектування користувацьких інтерфейсів, які забезпечують винятковий досвід роботи з додатками для мобільних телефонів, враховуючи потреби та бажання користувачів. Це було зроблено, дотримуючись принципів і процесів User Experience (UX) та User Interface (UI).

По-перше, був проведений аналіз конкурентів. Метою аналізу було оцінити різні стратегії взаємодії з користувачем, прийняті конкурентами, визначити їх сильні та слабкі сторони.

По-друге, дослідження користувачів було розпочато проводячи інтерв'ю та опитування, щоб зрозуміти, чи має визначена ціль однакові чи різні потреби

та проблеми, які були висунуті на етапі концепції. Крім того, були створені ідеальні профілі користувачів, які називаються персонами користувачів, щоб мати змогу ідентифікувати наших ідеальних користувачів, їхні потреби, розчарування та очікування. Потім було проаналізовано досвід користувачів, створюючи шляхи користувачів та зосереджуючи увагу на діях, цілях, думках та емоціях користувачів. Ці елементи були ключем до розробки рішень можливих проблем, з якими могли зіткнутися користувачі. Відповідно до цього ми створили каркаси. В результаті, пройшовши всі ці кроки, ми змогли краще зрозуміти як існуючих, так і майбутніх потенційних користувачів нашої програми. Це також допомогло в процесі проектування, оскільки дозволяло використовувати різноманітні типи користувачів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. А.Кичма, О.Полотай Загрози безпеки Wi-Fi мереж та основні протоколи захисту. "Інформаційна безпека та інформаційні технології": Збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів учених, студентів і курсантів. – Львів, 2021. – С. 49-51.

2. Бабаєв В.М. Електронне урядування: текст лекцій / В.М. Бабаєв, М.М. Новікова, С.О. Гайдученко. – Х.: ХНУМГ, 2014. – 127 с

3. Балацька В.С. Використання сканерів вразливостей для захисту комп'ютерної мережі навчального закладу // В. Балацька, В. Ящук, О. Полотай / матеріали VI Міжнародної науково-практичної конференції «Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи»

4. Балацька В.С., Ящук В.І., Полотай О.І. Вразливість комп'ютерної мережі як проблема закладів вищої освіти. Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи: збірник тез доповідей VI Міжнародній науково-практичній конференції (м. Київ - м. Львів, 4-5 листопада 2021 р.). Львів: ЛДУ БЖД, 2021. С. 66–68.

5. Виявлення та розслідування злочинів, що вичиняються у сфері інформаційних технологій: Наук.-практ.посіб./ За заг.ред.проф. Я.Ю.Кондратьєва. – К., 2004.]

6. Галицкий А. В. Защита информации в сети – анализ технологий и синтез решений / А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин. – М. : ДМК Пресс, 2004. – 616 с.]

7. Драб Ю. Основні підходи до побудови системи управління інформаційною безпекою / Ю. Драб, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.29-32).

8. Захист інформації [Електронний ресурс] – Режим доступу до ресурсу:: https://uk.wikipedia.org/wiki/

9. Інформаційна безпека[Електронний ресурс] – Режим доступу до ресурсу:: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0

10. Карачка А.Ф. ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ. Електронне урядування: текст лекцій. [Електронний ресурс] – Режим доступу до ресурсу:http://dspace.wunu.edu.ua/bitstream/316497/26564/1/lekzii.pdf

11. Кленик О., Ткачук Р. Особливості побудови захищеної мережі підприємства. Зб. тез доповідей V Всеукр. наук.-практ конф. молодих учених, студентів і курсантів “Інформаційна безпека та інформаційні технології” (м. Львів, 26 листопада 2021 р.). Львів : ЛДУБЖД, 2021. С. 52–54.

12. Колядич І., Ткачук Р. Системи автоматичного керування програмним забезпеченням. Зб. тез доповідей V Всеукр. наук.-практ конф. молодих учених, студентів і курсантів “Інформаційна безпека та інформаційні технології” (м. Львів, 26 листопада 2021 р.). Львів : ЛДУБЖД, 2021. С. 55–57.

13. Криптографія[Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F]

14. Купріков М. Методи тестування системи на проникнення для забезпечення кібернетичної безпеки / Н. Купріков, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.80-83).

15. Ленков С. В. Методы и средства защиты информации. В 2-х томах /Ленков С. В., Перегудов Д. А., Хорошко В. А.– К.: Арий,2008]

16. Мельцов В. В., Ткачук Р. Л. Організація захисту сайту створеного за технологіями: MONGODB, ANGULAR 12, HTML5, CSS3, JAVASCRIPT, NESTJS. Збірник тез доповідей VIII Всеукраїнської заочної науково – практичної конференції “Проблеми цивільного захисту населення та безпеки життєдіяльності: сучасні реалії України” (м. Київ, 28 квітня 2022 р.). Київ, НПУ

імені М.П. Драгоманова, 2022. С. 84–85.

17. Молдовян А.А., Молдовян Н.А., Рад Б.Я. Криптографія. - СПб.: Видавництво "Лань", 2001. - 224с.

18. Остапов С.Е. Технології захисту інформації: навч. посіб. / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х.: ХНЕУ, 2013. – 476 с

19. Про електронний цифровий підпис: Закон України від 22 трав. 2003 р. № 852-IV. – Режим доступу: http://zakon4. rada.gov.ua/laws/show/852-15

20. Про затвердження Концепції технічного захисту інформації в Україні: постанова Кабінету Міністрів України від 08.10.1997 р. № 1126, із змінами. URL: zakon3.rada.gov. ua/laws/show/1126-97-п.]

21. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94- ВР, зі змінами. – Режим доступу: zakon5.rada.gov.ua/laws/ show/80/94-вр.

22. Про телекомунікації: Закон України від 18.11.2003 р. № 1280-IV, зі змінами. – Режим доступу: zakon3.rada.gov.ua/ laws/show/1280-15.

23. Сомов, С. (2015) Аналіз загроз безпеці інформації в комп'ютерних мережах, Новітні інформаційні системи та технології. Полтава: ПНТУ, (3). [Електронний ресурс] – Режим доступу до ресурсу:: http://journals.nupp.edu.ua/mist/article/view/535).]

24. Сомов, С. (2015) Аналіз загроз безпеці інформації в комп'ютерних мережах, Новітні інформаційні системи та технології. Полтава: ПНТУ, (3). Режим доступу: http://journals.nupp.edu.ua/mist/article/view/535).

25. Тарасенко Р.Б. Інформаційне право: Навчально-методичний посібник / МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. – Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2010. – 512 с.

26. Шахуб С. М., Ткачук Р. Л. Дослідження методів і засобів при запроваджені концепції BYOD на підприємстві. Збірник тез доповідей VIII Всеукраїнської заочної науково – практичної конференції "Проблеми цивільного захисту населення та безпеки життєдіяльності: сучасні реалії України" (м. Київ, 28 квітня 2022 р.). Київ, НПУ імені М.П. Драгоманова, 2022. С. 149–150.

27. Britvin A., Alrawashdeh J. H., Tkachuk R. Client-Server System for Parsing Data from Web Pages. Advances in Cyber-Physical Systems Volume 7, Number 1, 2022. P. 8–13.

28. Bugtraq [Електронний ресурс] – Режим доступу до ресурсу: https://bugtraq.securityfocus.com/archive

29. EU Cybersecurity Policy: A Model for Global Governance [Електронний ресурс] – Режим доступу до ресурсу:: www.atlantic-community. org/-/eu-cybersecurity-policy-a-model-for-global-governance

30. How to prevent XSS [Електронний ресурс] – Режим доступу: https://portswigger.net/web-security/cross-site-scripting/preventing Назва з екрану.

31. O.Polotai, O. Belej, N. Nestor. Developing a local positioning algorithm based on the identification of objects in a wireless Wi-Fi network of the mall. IEEE 16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 - Proceedings, 2020, pp. 53-58.

32. O.Polotai, O. Belej., N. Nestor, S. Panchak Developing a Model of Cloud Computing Protection System for the Internet of Things. 2020 IEEE 16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 - Proceedings, 2020, pp. 53-58.

33. O.Polotai, O.Belej, K.Kolesnyk Application of neural networks in intrusion monitoring system for wireless sensor networks. Conference on computer science and information technologies. CSIT 2020: advances in intelligent systems and computing, vol 1293, Springer, Cham. – pp.1101-1115.

34. Zachko O., Kovalchuk O., Kobylkin D., Yashchuk V.. Information technologies of HR management in safety-oriented systems. Materials of 2021 IEEE 16th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT 2021). V. 2. Lviv, 2021. (Scopus Q2).