Глобіна Анастасія,
здобувачка другого (магістерського) рівня вищої освіти
факультет інформаційно-комп'ютерних технологій
Науковий керівник: ***Вакалюк Тетяна,***
доктор педагогічних наук, професор,
завідувач кафедри інженерії програмного забезпечення,
Державний університет «Житомирська політехніка»,
м. Житомир, Україна

СИМБІОЗ ПРОГРАМУВАННЯ ТА КІБЕРБЕЗПЕКИ: ШЛЯХ ДО СТІЙКОГО ТА БЕЗПЕЧНОГО ЦИФРОВОГО СВІТУ

В сучасному цифровому світі, де технології постійно змінюються, та залучення до кіберпростору ширшого загалу користувачів стає все більш актуальним, питання кібербезпеки виникає на першому плані [2]. Технології стають неодмінною складовою нашого повсякденного життя, тому справедливо стверджувати, що програмування та кібербезпека взаємопов'язані поняття, які визначають наш шлях до стійкого та безпечного цифрового світу.

Інтенсивний розвиток програмного забезпечення та програмування, з одного боку, пропонує безліч переваг для суспільства , таких як: автоматизація, ефективність, зручність та доступність технологічний прогрес та інновації, а з іншого — вносить нові виклики та загрози, які потребують уваги та експертизи з боку спеціалістів з кібербезпеки, а саме: проблеми приватності та захисту даних, загрози інформаційної безпеки, залежність від технологій та багато інших.. Цей симбіоз відіграє критичну роль у забезпеченні безпеки даних, цифрових систем та мереж, з якими ми взаємодіємо щодня [1].

Взаємодія програмування та кібербезпеки стає ще більш важливою в контексті розширення сфери впливу технологій на всі аспекти нашого життя [7]. Зростаюча кількість підключених до Інтернету пристроїв, розширення хмарних технологій та розвиток Інтернету речей підкреслюють необхідність забезпечення високого рівня кібербезпеки для забезпечення захисту приватності та безпеки користувачів.

В той час як програми стають все більш складними та великими, їх вразливість стає предметом зацікавлення для кіберзлочинців, які шукають шляхи для несанкціонованого доступу, втручання чи знищення даних [10]. Це ставить перед програмістами та інженерами завдання не лише створення функціонального програмного забезпечення, а й забезпечення його стійкості та захищеності від кібератак [8].

Передові програмісти розуміють, що включення принципів кібербезпеки у кожен етап процесу програмування допомагає уникнути вразливостей та захистити програмне забезпечення від потенційних загроз [6]. Розробка безпечного програмного забезпечення вимагає врахування основних принципів, таких як аутентифікація, авторизація, шифрування та ін. [5]. Розуміння цих

понять допомагає програмістам створювати програмне забезпечення, яке відповідає найвищим стандартам безпеки та захищає дані користувачів від потенційних загроз. Це створює надійний фундамент для програм, забезпечуючи їх захищеність від кібератак та несанкціонованого доступу [11].

Ключовою складовою взаємодії між програмуванням та кібербезпекою є освіта та навчання. Навчання професійних програмістів та експертів з кібербезпеки повинно охоплювати найновіші технології та методики для ефективного впровадження найкращих практик у сфері кібербезпеки в розробці програмного забезпечення.

Додатково знання кібербезпеки може забезпечити програмісту можливість виявлення та виправлення вразливостей в коді до того, як вони стануть об'єктом атаки. Це передбачає включення засобів перевірки безпеки, аудиту та тестування на етапах розробки програмного продукту [4].

Успішні компанії, які створюють програмне забезпечення, також розуміють важливість впровадження комплексних заходів з кібербезпеки. Вони вкладають значні ресурси у підвищення кваліфікації своїх розробників, проведення аудитів безпеки та вдосконалення своїх методів реагування на потенційні кібератаки [12]. Бо саме ключовою складовою взаємодії між програмуванням та кібербезпекою є неперервне навчання. Навчання професійних програмістів та експертів з кібербезпеки повинно охоплювати найновіші технології та методики для ефективного впровадження найкращих практик у сфері кібербезпеки в розробку програмного забезпечення [3].

Однією з головних загроз кібербезпеці є хакерські атаки, такі як віруси, черви, троянські програми та зловмисний код, які можуть завдати серйозної шкоди даним та інформаційним системам. Відсутність адекватного захисту може призвести до витоку конфіденційної інформації, фінансових збитків та пошкодження репутації. Крім того, інші загрози, такі як фішинг, соціальний інжиніринг та DDoS-атаки (атаки з відмовою в обслуговуванні), також становлять серйозну загрозу кібербезпеці.

Забезпечення безпеки в цифровому світі потребує постійної уваги та удосконалення. Нові технології, такі як штучний інтелект, аналітика даних та блокчейн, можуть бути використані для створення нових методів захисту та виявлення кіберзагроз [11].

Загалом, в сучасному світі програмування та кібербезпека стають нерозривними складовими для створення та підтримки безпечного та стійкого програмного забезпечення. Розуміння цих двох аспектів допомагає забезпечити, що сучасні технології не тільки інноваційні, але й безпечні для користувачів у всіх аспектах їх використання.

Список використаних джерел та літератури

1. "The Art of Deception: Controlling the Human Element of Security" by Kevin D. Mitnick.

2. "Hacking: The Art of Exploitation" by Jon Erickson.

3. "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard, Marcus Pinto.

4. "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" by Michael Sikorski, Andrew Honig.

5. "Cybersecurity and Cyberwar: What Everyone Needs to Know" by P.W. Singer, Allan Friedman.

6. "Security Engineering: A Guide to Building Dependable Distributed Systems" by Ross J. Anderson.

7. "Clean Code: A Handbook of Agile Software Craftsmanship" by Robert C. Martin.

8. "Code Complete: A Practical Handbook of Software Construction" by Steve McConnell.

9. "The Pragmatic Programmer: Your Journey to Mastery" by David Thomas, Andrew Hunt.

10. "Structure and Interpretation of Computer Programs" by Harold Abelson, Gerald Jay Sussman, Julie Sussman.

11. "Introduction to the Theory of Computation" by Michael Sipser.

12. "Design Patterns: Elements of Reusable Object-Oriented Software" by Erich Gamma, Richard Helm, Ralph Johnson, John Vlissides.

13. Krebs on Security. URL: https://krebsonsecurity.com/.

14. Schneier on Security. URL: https://www.schneier.com/.

15. Dark Reading. URL: www.darkreading.com/.

16. The Hacker News. URL: https://thehackernews.com/.