УДК 004.056.5

ФІШИНГ, DDOS-АТАКИ ТА ІНШІ КІБЕРАТАКИ – ЯК ЗАХИСТИТИСЯ

Наталія Чернящук, Андрій Дудко

PHISHING, DDOS ATTACKS AND OTHER CYBERATTACKS - HOW TO PROTECT YOURSELF

Nataliia Cherniashchuk, Andriy Dudko

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

Abstract. *The paper analyzes scientific research and practice of implementing methods and tools to counter phishing, DDoS attacks and other types of cyberattacks. The features of cybersecurity are considered, including the classification of threats, methods for their detection and means of protection. The subject area of cyberdefense is analyzed, the main essences of attacks, their properties and potential consequences for computer systems are determined. The functional requirements for protective software are studied and methods for detecting threats based on their characteristics are considered.*

Захист від кібератак, таких як фішинг, DDoS-атаки та інші види кіберзагроз, є важливою частиною забезпечення безпеки інформаційних систем. З кожним роком зловмисники використовують нові методи для атак на комп'ютерні системи, тому необхідно постійно оновлювати і вдосконалювати стратегії захисту. Для цього існує багато методів і технологій, але вибір правильного залежить від конкретної ситуації, потреб і рівня ризику.

Мета полягає у дослідженні методів і засобів класифікації кібератак, таких як фішинг і DDoS-атаки, а також заходів захисту від них, представлених у текстовому вигляді, з використанням стандартизованих характеристик безпеки для підвищення ефективності захисту інформаційних систем.

Визначення характеристик та ознак якості, а також формалізоване представлення моделей якості є важливими для ефективного управління безпекою та захистом комп'ютерних систем від кібератак. Це дозволяє створювати ефективні стратегії для запобігання потенційним загрозам та реагувати на атаки в реальному часі. Оскільки сучасні загрози, такі як фішинг та DDoS-атаки, можуть впливати на системи з різних аспектів, вивчення їхніх характеристик та впровадження відповідних моделей є критичним для захисту даних і підтримки належного рівня безпеки в інформаційних системах.

Фішинг – це метод шахрайства, при якому зловмисники намагаються отримати конфіденційну інформацію (логіни, паролі, дані карток) через підроблені веб-сайти або електронні листи, що виглядають як офіційні повідомлення від надійних організацій. Це може призвести до значних фінансових втрат або крадіжки особистих даних користувачів, що робить важливим виявлення і блокування таких атак на ранніх етапах [3].

DDoS-атака (Distributed Denial of Service) – це тип кібератаки, коли мережа з комп'ютерів, заражених шкідливим програмним забезпеченням, одночасно надсилає величезну кількість запитів на сервер, що призводить до його перевантаження та недоступності для легітимних користувачів. Такі атаки можуть викликати значні простій у роботі компаній і серйозно впливати на репутацію та фінансові результати [4].

Основні ознаки якості захисту від кіберзагроз:

Продуктивність: ефективність виявлення та нейтралізації атак, швидкість реагування на загрози. Наприклад, час виявлення DDoS-атаки та швидкість блокування шкідливого

трафіку можуть бути критичними для запобігання повного відключення сервісів. Висока продуктивність також дозволяє знизити навантаження на сервери та системи [3].

Ефективність: використання ресурсів для виявлення та протидії фішинговим атакам та іншим загрозам. Ефективність визначається здатністю системи швидко і точно ідентифікувати та блокувати підозрілі дії, мінімізуючи витрати часу та ресурсів на обробку запитів. Наприклад, час витрачений на обробку вхідних запитів і фільтрацію шкідливих повідомлень є важливими показниками [4].

Сумісність: взаємодія з іншими програмними і апаратними системами, що використовуються для захисту від кіберзагроз. Це важливо для забезпечення комплексного підходу до захисту і забезпечення того, щоб різні технології безпеки могли ефективно працювати разом. Приклад метрики: рівень сумісності з різними програмами безпеки, кількість несумісностей з іншими системами захисту [4].

Безпека: механізми керування доступом та захист від фішингових атак і зловмисників. Це передбачає використання сучасних методів шифрування та верифікації, щоб захистити інформацію від несанкціонованого доступу. Приклад метрики: кількість виявлених уразливостей, час на реагування на спроби злому — це важливі показники для забезпечення безпеки [3].

Формалізоване представлення моделей безпеки: Міжнародні стандарти, такі як ISO/IEC 27001, дають можливість визначити правила і вимоги до характеристик безпеки інформаційних систем, що захищають від кібератак. Інші моделі, такі як FURPS+ та модель Боема, надають конкретні атрибути для оцінки якості систем безпеки в контексті захисту від кіберзагроз. Це дозволяє стандартизувати процеси безпеки та забезпечити більш ефективне управління ризиками [4].

Вимоги зовнішньої якості для програмних систем, що захищають від кіберзагроз, включають:

Ефективність: швидкість виявлення фішингових повідомлень або DDoS-атак. Важливо, щоб система могла миттєво реагувати на нові загрози, що знижує ризик їхнього успіху [3].

Продуктивність: використання системи для ефективного блокування атак та фільтрації трафіку. Це забезпечує швидку реакцію і мінімізацію наслідків атак [5].

Стабільність: здатність залишатися стійкою під час збоїв або кібератаки, відновлення після порушень. Це дозволяє системі продовжувати виконувати свої функції навіть в умовах екстремальних навантажень [4].

Взаємодія з іншими системами: інтеграція з антивірусами, фаєрволами та іншими системами для забезпечення комплексного захисту від атак. Це забезпечує ефективний захист на всіх рівнях системи безпеки [5].

Сумісність з ПЗ: забезпечення сумісності між різними антивірусними програмами та фаєрволами. Це дозволяє зберігати рівень безпеки без зниження продуктивності [4].

Захист даних: забезпечення цілісності та конфіденційності даних під час кіберзагроз. Система повинна використовувати шифрування та інші методи захисту для збереження конфіденційності інформації [3].

Керування доступом: забезпечення доступу лише авторизованим користувачам, запобігання несанкціонованому доступу до даних та систем. Це гарантує, що тільки уповноважені особи можуть взаємодіяти з системою та її ресурсами [4].

Ці вимоги мають бути адаптовані до потреб користувачів і обмежень технічної архітектури, з урахуванням постійного розвитку нових типів атак [3][4][5], зображено на рисунку 1.

Формалізація моделі кіберзахисту полягає в тому, щоб визначити, як різні елементи захисту від кіберзагроз пов'язані між собою. Це схоже на моделі інформаційної безпеки. Для кожної категорії захисту визначають важливість і залежність від інших частин системи, щоб забезпечити ефективний підхід до кіберзахисту.

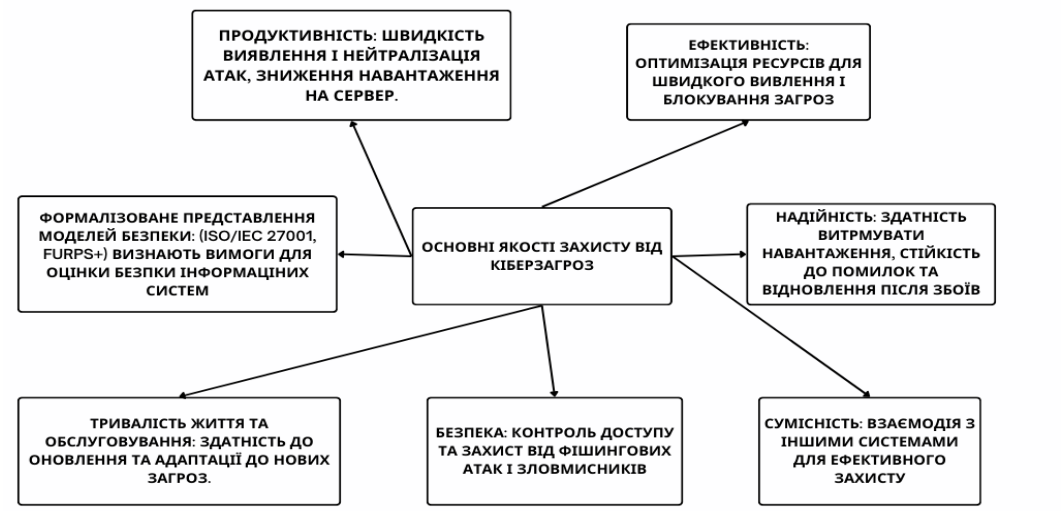

Рисунок 1 – Схема якості захисту від кіберзагроз

Проведено аналіз ефективності заходів захисту від кіберзагроз, зокрема фішингу, DDoS-атак та інших типів кіберзагроз, а також визначено основні негативні фактори, які можуть вплинути на захист комп'ютерних систем. Основні з них – невідповідність заходів безпеки реальним загрозам та недостатня адаптація до нових технік атак. Класифікація методів і інструментів захисту потребує додаткового дослідження, зокрема в контексті аналізу тексту даних для виявлення шкідливих дій. Проведено аналіз моделей безпеки для оцінки ефективності застосованих заходів щодо захисту від кіберзагроз, що дозволило обґрунтувати використання стандартів безпеки для забезпечення відповідності вимогам до захисту від фішингу, DDoS-атак і інших кіберзагроз.

Бібліографія

1. Державна служба спеціального зв'язку та захисту інформації України. *Державна служба спеціального зв'язку та захисту інформації України*. URL: https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601 (дата звернення: 23.03.2025).
2. ELARTU – Інституційний репозитарій ТНТУ імені Івана Пулюя: Методи захисту від кібератак на основі штучного інтелекту. *ELARTU – Інституційний репозитарій ТНТУ імені Івана Пулюя: Домівка*. URL: https://elartu.tntu.edu.ua/handle/lib/48319?locale=in (дата звернення: 24.03.2025).
3. How to spot and protect yourself from a phishing attack. *Cybersecurity Guide*. URL: https://cybersecurityguide.org/resources/phishing/ (date of access: 24.03.2025).
4. Guide to Understanding & Protecting Against DDoS Attacks. *Makes Email Safe For Business: Microsoft 365, Google Workspace*. URL: https://guardiandigital.com/resources/blog/ddos-attack-protection (date of access: 24.03.2025).
5. How to Spot and Avoid Phishing Attacks: Expert Tips for Online Safety | Hivenet. *Hivenet: Distributed Cloud Storage & Computing | Secure, Sustainable*. URL: https://www.hivenet.com/post/how-to-protect-yourself-from-phishing-attacks-top-tips-to-avoid-scams (date of access: 24.03.2025).