УДК 004.056.53

ДАВИДЮК Андрій Вікторович
ЖИЛІН Артем Вікторович
ХУДИНЦЕВ Микола Миколайович

МОДЕЛЬ СИСТЕМИ З КОМПЛЕКСНОЇ ПРОТИДІЇ ФІШИНГУ

Постановка проблеми. Забезпечення кібербезпеки є важливим завданням, що визначене Указом Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"», законами України «Про основні засади забезпечення кібербезпеки України», «Про критичну інфраструктуру» тощо. Значна роль кібербезпеці відводиться і в Законі України «Про національну безпеку України», що підтверджує залежність захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу й інших національних інтересів України від реальних і потенційних кіберзагроз. Під час війни в умовах підвищених ризиків інформаційної та кібербезпеки з метою підвищення рівня кібербезпеки держави невідкладним є вирішення завдання з розроблення нових методів і засобів кіберзахисту.

Слід зазначити, що в Україні з початком російського вторгнення у 2014 році зросла кількість кібератак на критичну інфраструктуру. Особливо активними були хакери російських спецслужб і хактивісти у 2022 році. Основними видами їхніх атак є таргетовані кібератаки (далі – APT) [1]. Це все відбувається на фоні зростання загальної кількості кібератак [2]. З огляду на зазначене для ефективної протидії таким кібератакам необхідним є проведення їх детального аналізу. Для такого аналізу американська корпорація «Lockheed Martin» розробила модель «Cyber Kill Chain» (див. рис. 1) [3].

Першим етапом кібератаки за цією моделлю є етап розвідки (Reconnaissance). Цей етап передбачає збирання інформації про ціль із використанням як технічних засобів для збирання інформації з відкритих джерел (OSINT) [4], так і засобів соціальної інженерії [5–8] та HUMINT [9]. У межах цих дій може бути зібрано досить багато інформації, що дасть можливість зловмиснику отримати доступ до системи для здійснення подальших деструктивних дій.

Водночас у разі дефіциту інформації, зібраної з відкритих джерел, використовуються такі додаткові засоби отримання доступу до цілі як фішинг [10]. За допомогою фішингу зловмисник здійснює спробу змусити користувача перейти за зловмисним посиланням або завантажити та відкрити файл, який містить шкідливе програмне забезпечення (далі – ШПЗ). Фішинг може

одночасно служити як засобом розвідки цілей, так засобом доставки (Delivery) ШПЗ [3; 11].

Рисунок 1 – Модель «Cyber Kill Chain» [3]

Слід зазначити, що метою фішингу може бути викрадення персональних даних, грошей громадян, організація кібератак на ІТ-інфраструктуру взагалі та на критичну інфраструктуру України зокрема. Інформаційний привід є ключовим в організації фішингу. Наразі активно використовуються в нинішніх реаліях такі теми, як: «Збір для ЗСУ», «Графіки відключень електроенергії», «Соціальні виплати», «Нова пошта» тощо. Вони є дуже популярними й цікавлять багатьох наших громадян, що зумовлює підвищену небезпеку.

Виходячи із зазначеного, необхідною умовою для забезпечення певного рівня кіберзахисту є розроблення відповідних засобів протидії розвідці противника, зокрема фішингу.

Аналіз останніх досліджень і публікацій. Існуючі рішення, такі як «OpenPhish» [12], «Phishing Army» [13], «PhishTank» [14], «Thinkbeforeyoulink» [15], «WOT» [16], Total Webshield [17] та повідомлення до CERT-UA [18]

тощо, мають низьку ефективність протидії фішингу, що підтверджується частотою його використання для кібератак (див. рис. 2) [19].

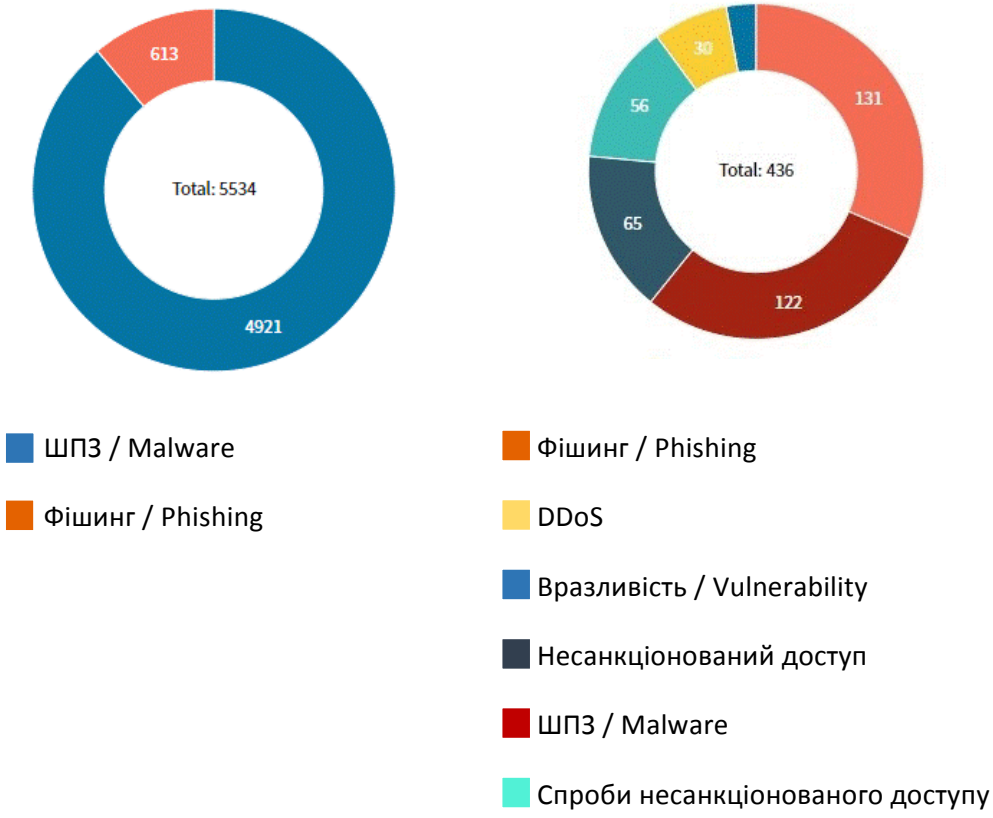

Рисунок 2 – Статистика CERT-UA з фішингу [19]

Водночас розробники антивірусного програмного забезпечення (ESET, AVAST, AVIRA тощо) інтегрують функції з фільтрації фішингу в основі функції статичного та динамічного аналізу ресурсів [20; 21]. Дослідженню явищу фішингу присвячено також низку оглядових та аналітичних праць [22; 23]. У них зазначається, що факторами зниження результативності фішингу є наявність технічних та організаційних засобів протидії. Однак у проаналізованих джерелах не висвітлюються процеси збирання, оброблення та поширення даних про фішинг, не запропонована концепція, модель середовища, яке б оброблювало дані про фішинг із різних джерел і автоматизувало процес протидії фішингу, зменшуючи при цьому час реагування на нього.

Метою статті є розроблення моделі системи збирання, оброблення та поширення даних про фішингові атаки з метою їхнього оперативного блокування. Наявність такого середовища може значно вплинути на час існування та обсяги поширення фішингу.

Виклад основного матеріалу. За результатами проведеного аналізу існуючих рішень у протидії фішингу та шляхів поширення інформації засобами інформаційних технологій були вироблені вимоги до системи з комплексної протидії фішингу (далі – Система).

Такими вимогами є надання можливості користувачу оперативно перевірити посилання на вебресурс, адресу електронної пошти, посилання на групу чи телеграм-канал, номер мобільного телефону, номер банківської карти (далі – об'єкти перевірки), створення автоматизованих перевірок вебресурсу та швидке поширення інформації про фішинг серед користувачів системи з можливістю блокування джерел фішингу.

Було розроблено модель Системи (див. рис. 3), згідно з якою користувачі з використанням програмного забезпечення (вебсайту, мобільного застосунку, телеграм-бота, розширення для веббраузера (плагіну)) надають інформацію про електронні ресурси (URL-адреси вебсайтів, сторінок у соціальних мережах, груп (каналів) у месенджерах, номери телефонів, номери банківських карток) із власного обладнання під управлінням операційної системи (комп'ютера, смартфона, планшета), що використовується для доступу до мережі Інтернет, і отримують за результатами обробки наданої інформації на сервері застосунків зі встановленим спеціалізованим програмним забезпеченням відомості щодо використання цих електронних ресурсів для зловмисних цілей. Результати перевірки електронних ресурсів, щодо яких користувачу не рекомендовано використовувати ці ресурси із-за їх високоймовірного застосування для зловмисних цілей, зберігаються до бази даних, що функціонує на сервері бази даних. Наповнення бази даних здійснюється автоматично та вручну (з довірених (верифікованих) джерел даних). Перевірка наданих відомостей здійснюється як із використанням власних розроблених алгоритмів, так і з використанням алгоритмів сторонніх сервісів і програмних застосунків, що є доступними для використання. Функція перевірки містить множину критеріїв, які мають різні залежно від їхнього значення оцінки (бали). Інформація щодо високоймовірного використання електронних ресурсів для зловмисних цілей генерується на сервері застосунків і передається до програмного забезпечення користувача, яке він використав для запиту через інтерфейс програмування застосунків (API – Application Programming Interface). Списки електронних ресурсів (URL-адреси вебсайтів, сторінок у соціальних мережах, груп (каналів) у месенджерах) синхронізуються зі списками ресурсів для блокування на сервері доменних імен (DNS-сервері). Користувач не зможе отримати доступ до потенційно зловмисного електронного ресурсу через зазначений DNS-сервер (див. рис. 4).

Система може бути використана також для раннього виявлення масових розсилок. Таке виявлення базується на оцінці кількості переходів з однієї мережі за одним посиланням в одиницю часу [24; 25]. Також із використанням

математичної формалізації системи глобальної маршрутизації мережі Інтернет у вигляді топологічного простору можливим є виявлення закономірностей у точках витоку таких розсилок [26].

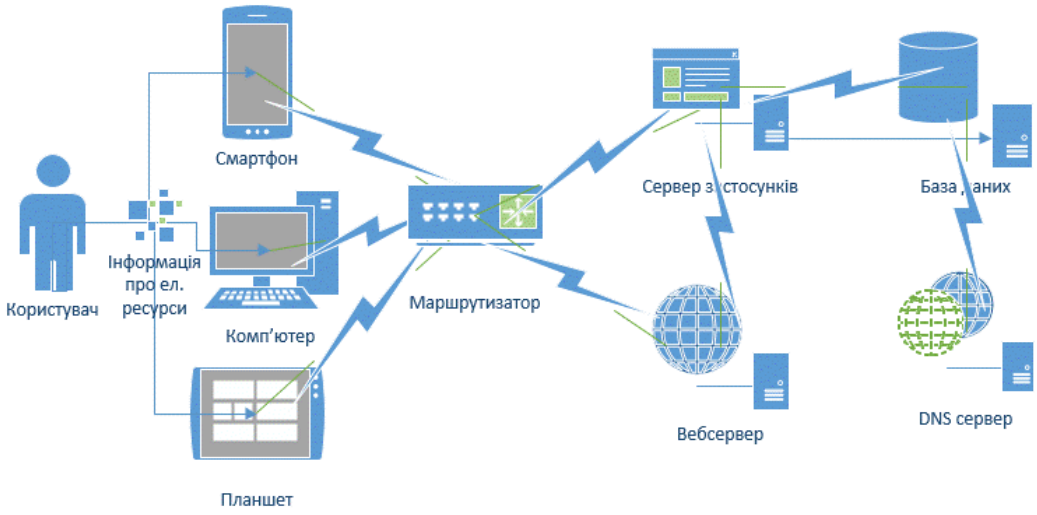

Рисунок 3 – Фізична схема моделі системи з комплексної протидії фішингу

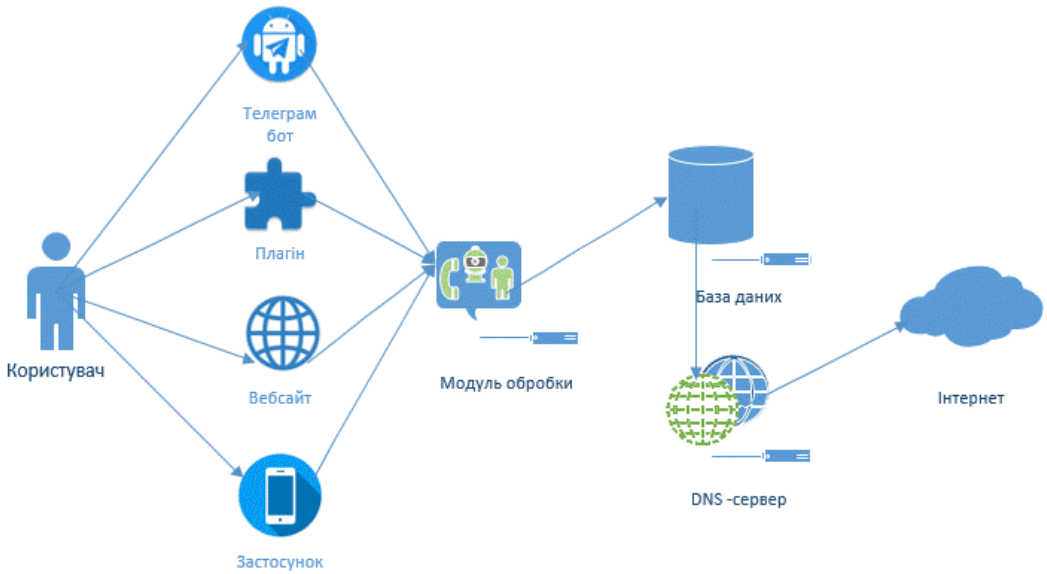

Рисунок 4 – Логічна схема моделі системи з комплексної протидії фішингу

Використання даних системи сприятиме безпеці користувачів, підвищенню ефективності роботи CERT-UA, Кіберполіції, Національного банку України, Національного координаційного центру кібербезпеки в межах процесу їхньої оперативної взаємодії.

Висновки. У процесі дослідження проаналізовано проблеми фішингу та застосування засобів протидії. Представлені в межах такого аналізу технічні рішення та наукові підходи є частковими рішеннями, що не вирішують комплексну проблему. Основними недоліками наявних технічних та організаційних рішень є недостатня ефективність процесів збирання, оброблення та поширення інформації про фішинг. З урахуванням цих проблем запропоновано впровадження системи з комплексної протидії фішингу як комплексу засобів автоматизації вказаних вище процесів. Такий підхід значно зменшить час оброблення та здійснення заходів із перевірки та блокування фішингових ресурсів, що відповідно значно зменшить ефективність фішингу.

Додатково впровадження такої системи значно покращить процеси кібергігієни, так як окрім теоретичної складової (лекції, тренінги, публікації) суспільство отримає практичні інструменти для повсякденного використання при прийнятті рішень щодо безпечного користування електронними ресурсами в мережі Інтернет.

Таке рішення розглядається як альтернатива блокуванню та має на меті підтримання принципів демократичного суспільства щодо доступу до інформації.

Перспективами подальших досліджень є інтеграція в розроблену інфраструктуру нейронних мереж із методами штучного інтелекту (модель BERT) [27] для покращання алгоритмів визначення шкідливих ресурсів.

Розвиток інфраструктури також передбачає створення API та його подальше використання в сервісах обміну повідомленнями (месенджери, вебресурси з функцією обміну повідомлень).

Список використаних джерел

1. Таргетовані кібератаки залишаються однією з основних кіберзагроз від хакерів із фсб – звіт. URL: https://cip.gov.ua/ua/news/targetovani-kiberataki-zalishayutsya-odniyeyu-z-osnovnikh-kiberzagroz-vid-khakeriv-iz-fsb-zvit (дата звернення: 25.10.2022).

2. У 2022 році кількість зареєстрованих кіберінцидентів виросла майже втричі – звіт. URL: https://cip.gov.ua/ua/news/u-2022-roci-kilkist-zareyestrovanikh-kiberincidentiv-virosla-maizhe-vtrichi-zvit (дата звернення: 25.10.2022).

3. The cyber kill chain. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (дата звернення: 25.10.2022).

4. OSINT framework. URL: https://osintframework.com/ (дата звернення: 25.10.2022).

5. Давидюк А. Соціальна інженерія як складова складної кібернетичної атаки.

Соціальна інженерія в контексті кібернетичної безпеки України (сучасні технології та шляхи захисту) : навчальний посібник / ред. В. М. Петрик. Київ, 2017. С. 27–39.

6. Петрик В., Давидюк А. Соціальна інженерія як засіб отримання таємної інформації. *Військова освіта і наука: сьогодення та майбутнє* : тези доповідей XIII Міжнародної науково-практичної конференції, (Київ, 24 листоп. 2017 р.). Київ, 2017. С. 230–232.

7. Давидюк А. Соціальна інженерія як складова складної кібернетичної атаки. *Соціальна інженерія* : навчальний посібник. Київ, 2019. С. 50–57.

8. Овчаров О., Давидюк А. Взаємозв'язок тролінгу та соціальної інженерії при їх застосуванні у кіберпросторі. *Безпека інформації в інформаційно-телекомунікаційних системах* : матеріали міжнародної науково-практичної конференції, (Київ, 25–26 трав. 2017 р.). Київ, 2017. С. 156–157.

9. HUMINT: конкурентна розвідка, соціальна інженерія. URL: https://www.molfar.global/humint (дата звернення: 25.10.2022).

10. Увага! Зафіксовано розсилання електронних листів із небезпечним вкладенням: зловмисники використовують тему іранських дронів-камікадзе Shahed-136. URL: https://cip.gov.ua/ua/news/uvaga-zafiksovano-rozsilannya-elektronnikh-listiv-iz-nebezpechnim-vkladennyam-zlovmisniki-vikoristovuyut-temu-iranskikh-droniv-kamikadze-shahed-136 (дата звернення: 25.10.2022).

11. Для атак на українське інформагентство російські хакери намагалися використати п'ять шкідливих програм. URL: https://cip.gov.ua/ua/news/dlya-ataka-na-ukrayinske-informagentstvo-rosiiski-khakeri-namagalisya-vikoristati-p-yat-shkidlivikh-program (дата звернення: 25.10.2022).

12. OpenPhish – phishing intelligence. *OpenPhish – Phishing Intelligence*. URL: https://openphish.com/ (дата звернення: 26.10.2022).

13. Phishing army. URL: https://phishing.army/ (дата звернення: 26.10.2022).

14. PhishTank | Join the fight against phishing. *PhishTank | Join the fight against phishing*. URL: https://phishtank.org/ (дата звернення: 26.10.2022).

15. Home – think before you link. *Think Before You Link*. URL: https://thinkbeforeyoulink.app/ (дата звернення: 26.10.2022).

16. Website safety check & phishing protection | web of trust. *Website Safety Check & Phishing Protection | Web of Trust*. URL: https://www.mywot.com/ (дата звернення: 26.10.2022).

17. Total webshield: browser antivirus protection. *Дополнения Opera*. URL: https://addons.opera.com/ru/extensions/details/total-webshield-browser-antivirus-protection/ (дата звернення: 07.11.2022).

18. Cert-ua. URL: https://cert.gov.ua/ (дата звернення: 26.10.2022).

19. Довідкова інформація з питань діяльності CERT-UA за фактами впливу на стан кібербезпеки у 2022 році. URL: https://cert.gov.ua/article/37121 (дата звернення: 07.11.2022).

20. Phishing. *Malware Protection & Internet Security | ESET*. URL: https://www.eset.com/us/anti-phishing/ (дата звернення: 07.11.2022).

21. Download phishing protection for free | avira. *Avira*. URL: https://www.avira.com/en/phishing-protection (дата звернення: 07.11.2022).

22. Aleroud A., Zhou L. Phishing environments, techniques, and countermeasures: a survey. *Computers & security*. 2017. Т. 68. С. 160–196. URL: https://doi.org/10.1016/j.cose.2017.04.006 (дата звернення: 08.11.2022).

23. Safi A., Singh S. A systematic literature review on phishing website detection techniques. *Journal of king saud university – computer and information sciences*. 2023.

URL: https://doi.org/10.1016/j.jksuci.2023.01.004 (дата звернення: 27.10.2023).

24. Serheiev S., Davydiuk A., Onyskova A. Development detection cyberatacs methods in the critical infrastructure objects information systems overview and prospects. *Information technology and security*. 2021. Vol. 9. No. 1. P. 91–99. URL: https://doi.org/10.20535/2411-1031.2021.9.1.249821 (дата звернення: 19.10.2022).

25. Яковів І., Давидюк А., Куликівський І. Засоби аналізу складних кібератак. *Безпека інформації в інформаційно-телекомунікаційних системах* : матеріали міжнародної науково-практичної конференції, (Київ, 25–26 трав. 2017 р.). Київ, 2017. С. 113.

26. Зубок В., Давидюк А. Математична формалізація системи глобальної маршрутизації мережі Інтернет у вигляді топологічного простору. *Інформаційні технології та безпека (ІТБ-2021)* : XXI Міжнародна науково-практична конференція. Київ, 2021. С. 170–177.

27. Getting started with the built-in BERT algorithm | AI Platform Training | Google Cloud. *Google Cloud*. URL: https://cloud.google.com/ai-platform/training/docs/algorithms/bert-start (дата звернення: 07.11.2022).

Рецензенти:
доктор технічних наук, доцент
В. Шестаков,
доктор технічних наук, доцент
А. Вавіленкова

Анотація. Стаття присвячена розробці рішень із протидії фішингу. Проведено дослідження існуючих механізмів захисту від кіберзагроз фішингу, за результатами запропоновано модель технічного рішення для комплексної протидії фішингу. Ця модель включає набір інструментів для підтримки прийняття рішень користувача при використанні ним електронних ресурсів у мережі Інтернет. Використання таких інструментів повинно сприяти існуючим процесам кібергігієни та стати її практичною складовою.

Ключові слова: кібербезпека, фішинг, кіберризик.

Abstract. The article is devoted to the development of anti-phishing solutions. Within the framework of the article, a study of the existing mechanisms of protection against phishing cyber threats was carried out. According to the results of these studies, a model of a technical solution for optimizing existing processes is proposed. This model includes a set of tools to support the user's decision-making when using electronic resources on the Internet. The use of these tools should contribute to existing processes of cyber hygiene and become a practical component of it..

Key words: cyber security, phishing, cyber risk.