CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

DOI 10.20535/2411-1031.2022.10.1.261176
УДК 004.056(53+57)

АРТЕМ ЖИЛІН,
ОЛЬГА ШЕВЧУК

МЕТОД АНАЛІЗУ ФІШИНГОВИХ ПОВІДОМЛЕНЬ

Розвиток та широке впровадження мережі Інтернет в повсякденне життя трансформувало як економічні, так і суспільні відносини. Представлення цих відносин в цифровому вигляді створило цифрову економіку, що характеризується активним обміном інформацією, швидким доступом до інформаційних ресурсів, перенесення платежів у цифровий вимір. Соціальні ж відносини в цифровому світі представлені соціальними мережами, месенджерами, які також надають економічні послуги. В той же час цифровий вимір, трансформована економіка й соціальні відносини породжують нові загрози. Самі користувачі активно виставляють у відкритий доступ інформацію про себе та своїх близьких, фотографії з відпочинку та місце розташування. Окрім спілкування в соціальних мережах, перегляду розважального контенту та онлайн ігор популярними є банківські розрахункові операції. Популяризація інтернет-банкінгу призводить до збільшеного інтересу викрадення даних з боку зловмисників. Результатом цього є зростання кількості шахраїв, які мають на меті отримання конфіденційної інформації користувачів. Крім того, з початком російського вторгнення в Україну збільшилась кількість кібератак на органи державної влади, об'єкти критичної інформаційної інфраструктури та на організації, які містять критично важливу інформацію. Одним з відомих методів викрадення такої інформації є фішингові атаки. Водночас, користувачі здебільшого недооцінюють серйозність даних атак і не приділяють достатньої уваги системам захисту. Це в свою чергу призводить до більш масштабних наслідків. Тому основною задачею, яка вирішувалась, є представлення методу аналізу фішингових повідомлень, який можливо використовувати для зменшення ймовірності досягнення мети фішингової атаки. Разом з цим, відомо, що зловмисники вдосконалюють та модифікують методи реалізації атак, а отже проведення класифікації фішингових атак для підвищення обізнаності користувачів становить нагальну задачу. Результатом роботи є запропонована класифікація фішингових атак та представлений метод аналізу фішингових повідомлень.

Ключові слова: фішинг, кібершахрайство, фішингове повідомлення, класифікація фішингових атак, метод аналізу.

Постановка проблеми. З кожним роком рівень кіберзлочинності зростає. На протидію побудові та впровадженню різного роду комплексів захисту, зловмисники ще більше просуваються в удосконаленні технік та методів атак. З початком російського вторгнення в Україну кількість кібератак збільшилась. Однак, окрім атак на урядові структури жертвами зламів та викрадення даних стають і пересічні громадяни [1]. Як і в реальному житті, так і в мережі Інтернет більш розповсюдженим видом злочинності є шахрайство, а саме викрадення даних банківських карт та приватної інформації. За даними Кіберполіції [2] лише у 2021 році було припинено діяльність 422 онлайн-шахраїв. У випадку з шахрайством в мережі Інтернет найчастішим способом викрадення інформації, який використовує зловмисник, є фішинг. В цьому випадку жертва являється найслабшим місцем, адже сама добровільно надає конфіденційну інформацію, яку в подальшому використовують зловмисники.

Сучасні антивірусні програми пропонують сервіси захисту, які призначені для запобігання фішинговим атакам. Однак статистика за 2021 рік представлена у [3] доводить інше:

– у сфері криптовалюти кількість фішингових атак зросла в 10 разів у порівнянні з початком 2021 року:

– з січня по червень 2021 року кількість атак у соціальних мережах зросла майже на 50%;

– 51% крадіжки облікових даних було націлено на корпоративні облікові дані;

– атаки, спрямовані на системи єдиного входу (SSO), зросли на 40% в порівнянні з першим кварталом 2021 року.

Окрім наведеної статистики, яка доводить, що фішингові атаки досі являються популярними, у [4] показано, що велика кількість користувачів, які стали жертвою фішингу, не поспішають захищати себе від таких атак, оскільки не знають жодного способу захисту від них. До того ж, більшість жертв не звертаються за допомогою до спеціальних органів.

Методи здійснення фішингових атак вдосконалюються. Інструментом здійснення таких атак зазвичай виступає електронна пошта, а самі фішингові повідомлення містять посилання на зловмисний сайт чи зловмисне вкладення, які можуть змінюватись. При чому для захисту від атак такого класу необхідно постійне слідування тенденціям їх розвитку. Тому універсального способу боротьби з фішингом не існує, але аналіз фішингових атак показує наявність деякого шаблону їх проведення. Підсумовуючи викладене, можна зазначити що актуальним є дослідження і класифікації фішингу, а також розроблення методу аналізу фішингових.

Аналіз останніх досліджень і публікацій. Дослідженню фішингових атак присвячено досить велика кількість статей, публікацій та посібників. Автори по своєму дають визначення фішингу та методам захисту від нього. До наукових досліджень проблеми фішингових атак можна віднести [8], [12] - [17]. В кожній з даних публікацій є визначення фішингу. У [8] визначаються основні дії фішерів, [12] описує основні аспекти протидії фішингу. В дослідженнях [13] - [16] викладено основні способи захисту від фішингу, програмне забезпечення, яке можна використовувати для запобігання фішингу. Низка Інтернет публікацій [18] - [20] також описують фішинг та методи захисту від нього. У [17], [21] наведено класифікацію фішингових атак відповідно. Але у зв'язку з тим, що атаки вдосконалюються, спосіб їх розповсюдження доповнюється, постає питання уточнення та оновлення класифікації фішингових атак. Однак, у жодній з проаналізованих наукових публікацій не запропоновано методу аналізу фішингових повідомлень.

Метою статті є дослідження фішингових атак для їх класифікації, а також побудова методу аналізу фішингових повідомлень.

Виклад основного матеріалу дослідження. Визначення терміну "фішинг" існує велика кількість. Деякі джерела визначають це поняття як спробу вкрасти інформацію про людину, використовуючи електронну пошту [5]. Інші під фішингом розуміють вебсторінку, яка без дозволу заявляє, що діє від імені третьої сторони з метою отримання конфіденційної інформації користувачів [6]. У [7] фішинг описується як кримінальний механізм, який використовує як соціальну інженерію, так і технічні прийоми для крадіжки особистих даних користувачів і облікових даних фінансових рахунків. Проводячи аналіз даних визначень можна зробити висновок, що "фішинг" можна розглядати по різному, однак основна мета його проведення залишається незмінною – викрадення даних.

Згідно з [8], під фішингом розуміють процес введення в оману чи соціального примусу жертви до передачі конфіденційної інформації для зловмисного використання. Надалі під "фішингом" будемо мати на увазі саме це визначення.

Під конфіденційною інформацією користувачів в розрізі фішингової атаки розуміють [9]:

– логін та пароль для входу в мобільні застосунки;

– номер, термін дії, CVV2/CVC2, ПІН платіжної картки;

- одноразові паролі підтвердження операцій;
- адреса електронної пошти;
- фінансовий номер телефону;
- слово – пароль до картки, відповіді на секретні питання.

На даний час існує достатньо велика кількість методів реалізації фішингу. Слід відмітити, що самі методи фішингу можуть бути комбіновані, тим самим створюючи нові. В даній статі запропонована наступна класифікація фішингових повідомлень (рис. 1):

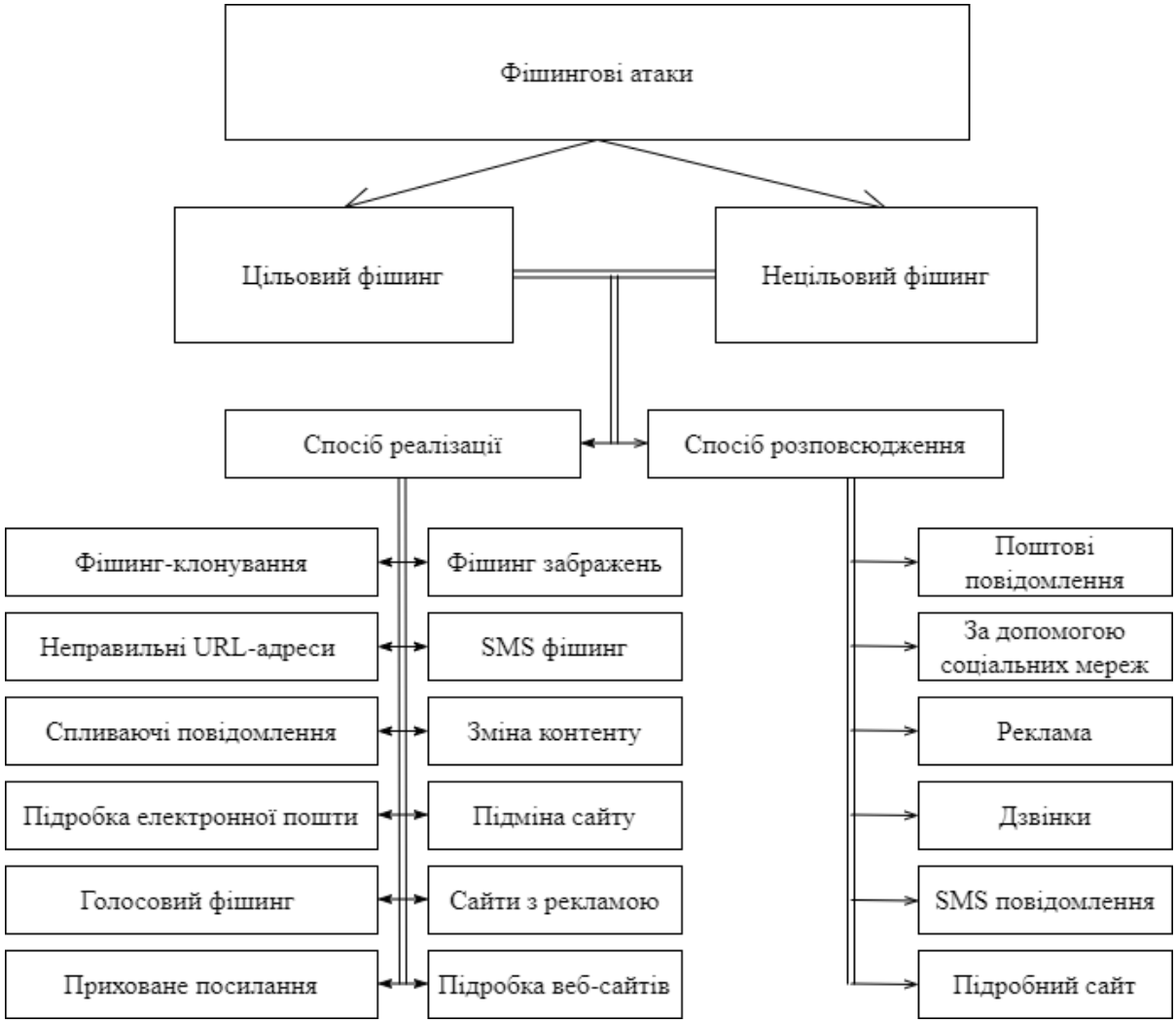

Рисунок 1 – Класифікація фішингових атак

Першочергова класифікація фішингових повідомлень передбачає визначення того, чи була обрана зловмисником жертва. Тобто чи являється даний фішинг цільовим, чи він несе випадковий характер.

Більшість користувачів плутають спам-повідомлення з нецільовим фішингом. Варто зазначити, що ці поняття мають відмінну мету при навіть схожій реалізації. За визначенням наданим в [10], спам – це небажані повідомлення у будь-якій формі, які надсилаються у великій кількості. Найчастіше спам націлений на велику кількість адрес у формі комерційних електронних листів, а також через миттєві та текстові повідомлення (англ. Short Message Service, SMS), соціальні медіа або навіть голосову пошту. Спам має на меті привернути увагу отримувача до певного товару або послуги, спонукає його перейти на реальний сайт. Найчастіше використовується в маркетингу для просування того чи іншого товару. В той час як нецільовий фішинг, хоч і не має явної жертви, все одно має на меті отримання вигоди, шляхом обману жертви та крадіжки важливої інформації.

Цільовий фішинг використовує складніші схеми, ніж нецільовий. Найчастіше він більш технологічний, а заподіяна ним можлива шкода вагоміша. Зловмисники вивчають своїх жертв та їх профілі в соціальних мережах, збирають інформацію про їх звички, використовувані сервіси, контакти та багато іншого. Якщо використовувати ці дані при складанні листа, він виглядатиме переконливим і правдоподібним. І на відміну від нецільового фішингу ймовірність жертви "потрапити на гачок" зростає.

В наведеній класифікації (рис. 1) окремо визначено способи розповсюдження фішингових повідомлень. Спосіб, який найчастіше використовується в фішингових атаках – це поштові повідомлення. За допомогою пошти легко проводити як цільовий, так і нецільовий фішинг. Більшість сервісів та інтернет-банкінг досі використовують електрону пошту, як спосіб комунікації з користувачами. Тим самим підроблення поштових повідомлень досі є актуальною проблемою. Ще одним способом розповсюдження фішингових повідомлень є соціальні мережі. Кількість користувачів соціальних мереж зростає з кожним днем. Відповідно цільова аудиторія зловмисника може швидко розширюватися. До того ж проведення фішингових атак через соціальні мережі для зловмисника несе свої переваги. За допомогою соціальних мереж можна збирати додаткову уточнюючу інформацію про жертву, якщо зловмисника цікавить цільовий фішинг.

Використання дзвінків та SMS повідомлень актуальне для голосового та SMS фішингу відповідно. Фішинг рекламних повідомлень може бути реалізоване двома способами. По-перше, на підробленому сайті розміщується реклами-приманками, для подальшого розповсюдження шкідливого контенту або обдурювання користувача при фіктивній авторизації чи реєстрації на сайті. По-друге, рекламування фішингового сайту для подальшого проведення атаки.

За способом реалізації визначені наступні види:

– *фішинг-клонування* – атаки клонів полягає в тому, щоб скористатися легітимними повідомленнями, які жертва, можливо, вже отримувала, і створити її шкідливу версію. Атака створює віртуальну копію законного повідомлення і відправляє повідомлення з адреси електронної пошти, яка виглядає законною. Посилання або вкладення у вихідному листі замінюються на шкідливі;

– *підробка електронної пошти* – характеризується отриманням даних від користувачів без їхнього відома, шляхом:

- відправлення поштових листів через знайоме ім'я користувача;
- відправлення поштових листів, через керівника або начальника, запитуючи важливі конфіденційні дані про користувача або про організацію;
- видавання себе за легітимну організацію, в якій працює користувач, з метою запиту внутрішньої інформації;
- використання неправильних URL-адрес – характеризується використанням URL-адреси фішинг-сторінки для зараження цілі. Зловмисник використовує домени, схожі на популярні веб-сайти та створює відповідні ідентичні сайти, де просить жертву ввести свої персональні дані у визначенні поля авторизації;
- використання прихованого посилання – відрізняються наявність фрази "Натисніть тут" і схожих на неї. Перехід на приховане посилання призводить до переходу на сторінку зловмисника;
- використання реклами – фішери підроблюють сайти з "ексклюзивними пропозиціями" в якості приманки. Прикладом даної атаки є рекламна вкладка в пошуковому браузері, де фактично коштовні послуги або додатки визначаються як ексклюзивно безкоштовні протягом певного проміжку часу, що заманює жертву з більшою можливістю скористатись пропозицією;

– *підробка веб-сайтів* – зловмисник публікує веб-сайт, копіюючи дизайн і вміст легітимного сайту. Для зменшення ймовірності виявлення підробки використовують інструменти для скорочення URL-адрес. За допомогою даних інструментів підробна URL-адреса виглядає більш правдоподібно та викликає менше сумнівів у користувача;

– *фішинг-зображень* – фішери використовують зображення або інші мультимедійні формати для доставки шкідливого програмного забезпечення. Способами доставки таких зображень є автоматичне завантаження при переході на фішинговий сайт або використання закодованих зображень;

– *голосовий фішинг* – зловмисник використовує телефонні дзвінки в якості отримання конфіденційної інформації;

– *SMS фішинг* – фішинг з використанням SMS повідомлень, який спонукає жертву на розкриття особистої інформації шляхом переходу по зловмисним посиланням;

– *використання спливаючих повідомлень* – дозволяють зловмиснику отримувати реєстраційні дані, надсилаючи спливаючі повідомлення;

– *зміна контенту* – зловмисник змінює частину інформації на легітимному сайті з метою введення в оману жертву і переправлення її за зловмисними посиланнями;

– *підміна сайту* – метод, в якому шкідливий сайт видає себе за легітимний шляхом проведення атаки типу міжсайтовий скрипт чи підміною сайту.

Відповідно до сказано раніше, зловмисники можуть комбінувати дані способи, створювати свій власний метод проведення фішингу та вдосконалювати його. Однак, розуміння реалізації кожного з цих методів окремо зменшує ймовірність стати жертвою фішингових атак.

Після проведення аналізу літератури [13] - [16] можна сформулювати низку правил, які допоможуть не стати жертвою Інтернет-шахраїв:

– не відкривайте сумнівні електронні листи, які не мають конкретного логічного вмісту;

– натискайте на посилання всередині листа або повідомлення лише, якщо ви впевнені в адресаті;

– натискайте на посилання всередині листа або повідомлення, якщо ви впевнені в тому на який сайт веде це посилання;

– уважно переглядайте URL-адресу. Вона може бути змінена або модифікована;

– перед тим, як переходити за посиланням подивіться, чи захищене ваше з'єднання;

– звертайте уваги на будь-які деталі листа: помилки, неправильні посилання;

– якщо на сайті з'явилось спливаюче вікно, з запитом на завантаження будь-якого файлу або документу – не підтверджуйте автоматичне завантаження контенту. Це може бути ознакою шахрайства;

– перевіряйте наповненість вебсторінки. Якщо є підозра в неправдивості логотипів чи контенту – перевірте законність сайту відвідавши його напряму виконуючи пошук за назвою сервісу або організації;

– не розголошуйте інформацію про себе даремно. Якщо вебсторінка вимагає обов'язкового заповнення поля реєстрації чи будь-яких контактних даних – зверніть на це увагу. Це може бути ознакою шахрайства;

– звертайте увагу на листи від невідомих адресатів;

– встановіть антивірусне програмне забезпечення;

– якщо маєте сумнів в безпечності додатків що завантажуються – відкривайте їх в віртуальному безпечному середовищі;

– встановіть штатні засоби захисту від фішингових атак на поштовому сервері, в розширеннях браузеру та на робочій станції.

На сьогодні існує достатня кількість антивірусного програмного забезпечення, які пропонують різні рівні захисту для попередження фішинговим атакам. Однак, ці інструменти не мають гарантованої результативності своєї роботи. Фішингові повідомлення все одно потрапляють до жертви. Зазвичай ці захисні рішення лише блокують фішингові сайти при спробі перейти за шкідливим посиланням або просто відправляють лист до категорії "спам", але це також відбувається далеко не завжди. Тому постає задача розробки методу аналізу фішингових повідомлень, за допомогою якого, користувачі зможуть класифікувати повідомлення на основі певних ознак.

Існує декілька підходів до розпізнавання фішингових атак: навчання користувачів і використання програмних засобів відокремлення фішингових листів [11]. Перший підхід має на меті покращити розуміння користувачів в галузі розповсюдження фішингових атак. Навчання збільшить ймовірність коректного розпізнавання та виявлення фішингових листів, вкладень та сайтів. Другий підхід спрямований на більш точну класифікацію фішингових листів, вкладень та сайтів та зменшення ймовірності неправильного розпізнавання фішингових атак.

Пропонується розглянути варіант розпізнавання фішингових повідомлень, який націлений саме на дії користувача. На рис. 2 представлено структурну схему реалізації методу аналізу фішингових повідомлень, який передбачає використання людського мислення та програмних засобів, для аналізу на кожному з запропонованих етапів. Запропонований метод складається з низки етапів, які включають в себе аналіз складових електронного листа, зокрема, трьох частин – заголовка, основної частини (тіла) та вкладення.

Перший етап аналізу – аналіз заголовку. У заголовку представлено маршрутну інформацію повідомлення. Він може містити й інші відомості – тип контенту, дані відправника та адресата, дату отримання, абсолютну адресу відправника, адресу поштового сервера та реальну адресу електронної пошти, з якої або на яку було надіслано повідомлення.

До важливих заголовків відносяться:

Return-Path. Адреса електронного листа Return-Path містить інформацію про статус доставки. Поштовий сервер читає вміст заголовка Return-Path для обробки недоставлених або повернутих відправнику листів. Сервер одержувача використовує це поле для ідентифікації підроблених листів: запитує всі дозволені IP-адреси, пов’язані з доменом відправника, і зіставляє їх з IP-адресою автора повідомлення. Якщо збігів немає, електронний лист надсилається до спаму.

Received. Це поле відображає інформацію про всі сервери, через які пройшов електронний лист. Останній запис – початкова адреса відправника.

Reply-To. Адреса електронної пошти в цьому полі використовується для надсилання повідомлення у відповідь. У підроблених листах він може відрізнятись від адреси відправника.

Received-SPF. Метод SPF (англ. – Sender Policy Framework; укр. – рамкова політика відправника) підтверджує, що повідомлення з конкретного домену було надіслано з сервера, який контролюється власником цього домену. Якщо значення цього поля – Pass (“Перевірка пройдена”), джерело листа вважається справжнім.

DKIMC. Служба DKIM (англ. – Domain Keys Identified Mail; укр. – ідентифікована пошта з ключами домену) відзначає вихідну пошту зашифрованим підписом усередині заголовків, а поштовий сервер одержувача розшифровує її, використовуючи відкритий ключ, щоб переконатися, що повідомлення не було змінено під час пересилання.

X-Headers. Цим терміном позначаються експериментальні заголовки чи заголовки розширення. Вони зазвичай додаються постачальниками послуг електронної пошти одержувача. Для виявлення спаму використовуються поля типу X-FOSE-Spam та X-Spam-Score.

До можливих аномалій в заголовках можна віднести такі:

– зворотній шлях може не співпадати з адресою в полі: From (“Від”). Це означає що всі недостовірні листи будуть повернені по першій адресі;

– у поле Received (“Отримано”) ім’я домена, з якого відправлявся лист може не співпадати з зазначеною. При аналізі IP- адреси відповідно результати будуть такі ж;

– адреса відправника From відрізняється від адреси в полі Reply-To. Таким чином відповідь буде відправлена на іншу адресу;

значення поля DKIM – може бути none (“Ні”). Це означає що лист не підписаний.

Аналіз тіла листа.

Тіло фішингового листа – основна частина електронного повідомлення, саме його зміст покликаний ввести в оману користувача. Вміст повідомлення зазвичай адресований особисто одержувачу і виглядає настільки правдоподібним, що жертва часто потрапляє в пастку зловмисника.

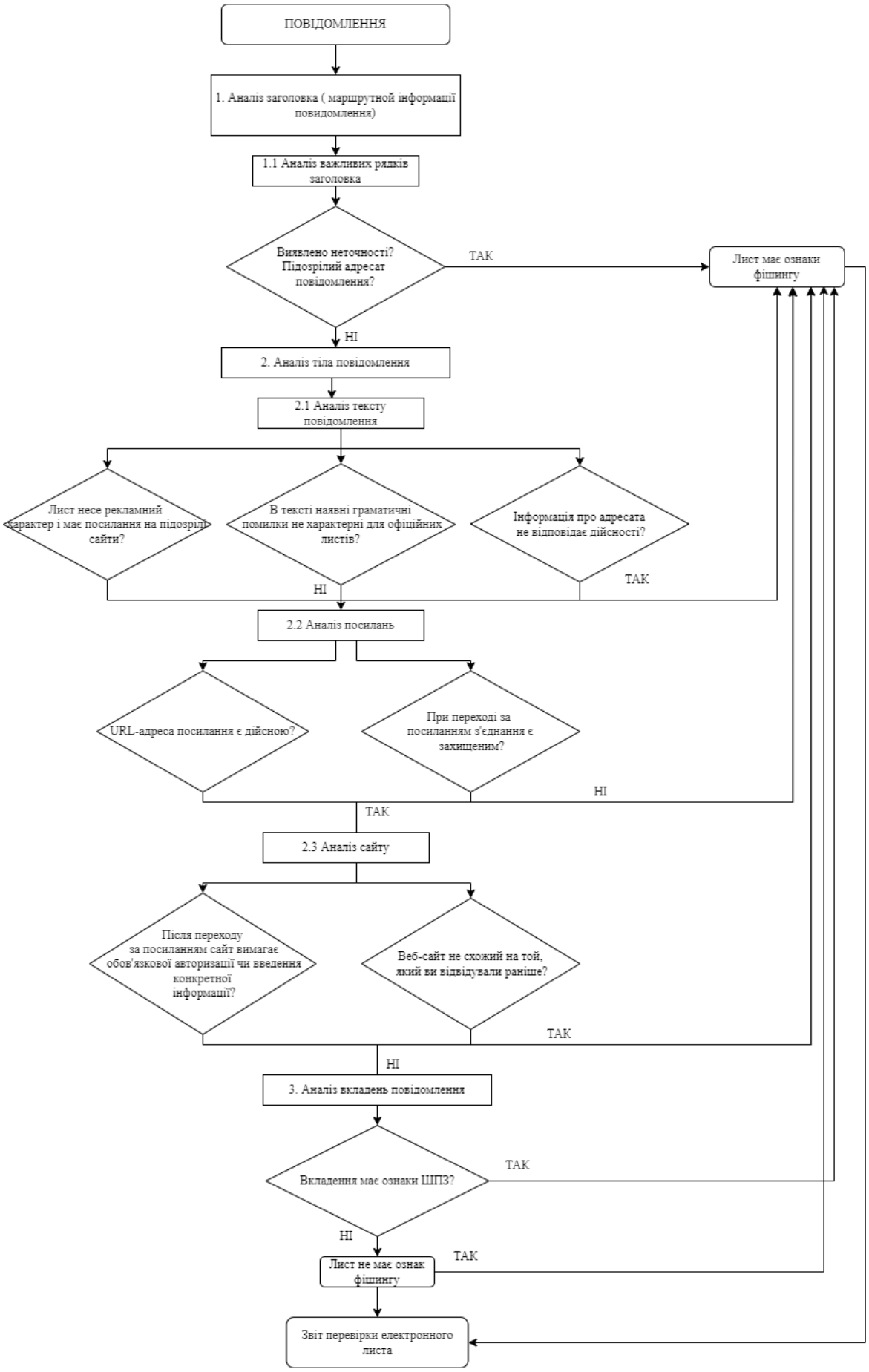

Рисунок 2 – Структурна схема реалізації методу аналізу фішингових повідомлень

Шляхом аналізу структури та змісту повідомлення в тілі листа можна зробити висновки чи має лист ознаки фішингу. Якщо повідомлення не має конкретики та має якісь посилання це наводить на те, що повідомлення належить до спаму або фішингу. При умові, що повідомлення має точні контакти адресата необхідно перевірити їх достовірність стосовно існування адресату. Якщо в повідомленні є посилання на сторінку авторизації чи посилання на інші вебсайти, то варто звернути увагу на правильність написання URL-адреси. Якщо здійснити перехід за посиланням, варто проаналізувати сторінку, адже вона може відрізнятись від легітимної (старі логотипи, старий або незвичний дизайн).

Аналіз вкладень листа.

Зазвичай вкладенням електронної пошти є тексові або виконувані файли. Ці формати часто використовуються злочинцями як інструмент для завантаження шкідливого програмного забезпечення (ШПЗ). Аналізування вкладень можна провести за допомогою наступних кроків.

Етапи аналізу вкладень:

Крок 1. Аналіз властивостей файлу. Необхідно визначити розмір файлу, його тип та автора, дату та час створення.

Крок 2. Перевірка вкладення за допомогою пісочниці. Для цього необхідно завантажити файл в ізольоване середовище перевірки файлів (пісочницю). За допомогою стандартних YARA-правил, які перевіряють вкладення на основі сигнатур, пісочниця визначить приналежність файлу до ШПЗ.

Крок 3. Визначення аналізу поведінки вкладення шляхом його відкриття у віртуальному середовищі. Аналіз запущених процесів та подій в системі.

Крок 4. Перевірка вкладення за допомогою онлайн ресурсів VirusTotal, MalwareBazaar.

Крок 5. Перевірка вмісту документу на можливі приховані вкладення за допомогою OllyDbg та hex-редактора.

Крок 6. Висновки проведеного аналізу.

Отже, запропонований метод аналізу фішингових повідомлень дозволяє користувачам виявляти фішингові повідомлення.

Висновки. Фішинг являє собою вид шахрайства, за допомогою якого методами соціальної інженерії зловмисник змушує жертву виконувати дії в своїх цілях. Наведена класифікація фішингових атак доводить, що існує велика кількість способів їх реалізації. Проблема фішингу досі є актуальною, а зловмисники – винахідливі в виборі способу реалізації фішингових атак.

Представлений метод аналізу фішингових повідомлень дозволяє зменшити ймовірність досягнення зловмисниками мети фішингової атаки. Крім того, підвищує обізнаність користувачів в області фішингових атак. В подальшому використання представленого методу можливе для удосконалення автоматизованих систем виявлення фішингових повідомлень.

Отже, ефективним методом захисту від фішингу можна вважати комплексну систему захисту з використанням різних технологій. Лише одночасне використання антивірусного програмного забезпечення, пильності користувача та правильного аналізу підозрілих повідомлень підвищить точність виявлення фішингових атак та зменшить кількість можливих збитків спричинених фішинговими атаками.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Атака на інформаційному фронті, 2022. [Електронний ресурс]. Доступно: https://cyberpolice.gov.ua/news/ataka-na-informaczijnomu-fronti---porady-kiberpolicziyi-shhodo-zaxystu-gadzhetiv-vid-vytoku-danyx-6563/. Дата звернення: Січ. 03, 2022.

[2] Кіберполіція припинила діяльність шахраїв, 2022. [Електронний ресурс]. Доступно: https://cyberpolice.gov.ua/news/u--roczi-kiberpolicziya-prypynyla-diyalnist--onlajn-shaxrayiv-6518/?fbclid=IwAR0RaghjZSzEzytXJ1RARnhVcWEq9IzPKgZIKj3ydsY8QgOaRgqSvEaifl8. Дата звернення: Січ. 03, 2022.

[3] Quarterly threat trends & intelligence report November, 2021. [Online]. Available: https://www.phishlabs.com/blog/new-quarterly-threat-trends-intelligence-report-now-available/. Accessed on: Febr. 4, 2022.

[4] С. Думчиков, та В. Лучіков, “Статистика фішингових інцидентів в Україні за 2021 рік”, 2021. [Електронний ресурс]. Доступно: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/34523/91970.pdf?sequence=2&isAllowed=y. Дата звернення: Січ. 03, 2022.
[5] PhishTank. [Online]. Available: https://www.phishtank.com/what_is_phishing.php. Accessed on: Jan. 4, 2022.
[6] C. Whittaker, “Large-scale automatic classification of phishing pages”, 2013. [Online]. Available: https://research.google.com/pubs/archive/35580.pdf. Accessed on: Jan. 5, 2022.
[7] Phishing Activity Trends Report, 1st Quarter, 2019. [Online]. Available: http://docs.apwg.org/reports/apwg_trends_ report_q1_2019.pdf. Accessed on: Jan. 4, 2022.
[8] М. Акулич, “Фишинг и маркетинг”, 2022. [Электронный ресурс]. Доступно: https://books.google.com.ua/books?id=BLsVEAAAQBAJ&printsec=frontcover&hl=ru#v=onepage&q&f=false. Дата обращения: Янв. 03, 2022.
[9] Що таке фішинг і як від нього захиститись. [Електронний ресурс]. Доступно: https://www.fg.gov.ua/articles/50140-shcho-take-fishing-i-yak-vid-nogo-zahistitis.html. Дата звернення: Січ. 03, 2022.
[10] Що таке спам. [Електронний ресурс]. Доступно: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/spam/. Дата звернення: Лют. 03, 2022.
[11] M. Khonji, Y. Iraqi, and A. Jones, “Phishing Detection: A Literature Survey”, *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2091-2121, 2013. [Online]. Available: https://doi.org/10.1109/surv.2013.032213.00009. Accessed on: Jan. 5, 2022.
[12] І. В. Яковюк, А. Волошин, та А. Шовкун, “Правові аспекти протидії фішингу: досвід Європейського Союзу”, *Проблеми законності*, № 149, с. 16, 2020.
[13] Д. О. Давидов, “Програмне забезпечення системи формування фільтрів від фішингу в мережі Internet”. [Електронний ресурс]. Доступно: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/4088/1/ConferenceMITandCompSysS2013_p89.pdf. Дата звернення: Січ. 10, 2022.
[14] О. Боскін, та П. Чорний, “Аналіз загрози фішингу”, у *Сучасна молодь в світі інформаційних технологій*, Н. Кириченко та Г. Димова, Ред. Херсон, Україна: Херсон, 2021, с. 179-181. [Електронний ресурс]. Доступно: http://dspace.ksau.kherson.ua/bitstream/handle. Дата звернення: Січ. 10, 2022.
[15] О. Боскін, та П. Чорний, “Аналіз захисту від фішингу”, у *Сучасна молодь в світі інформаційних технологій*, Н. Кириченко та Г. Димова, Ред. Херсон, Україна: Херсон, 2021, с. 182-183. [Електронний ресурс]. Доступно: https://dspace.ksau.kherson.ua/bitstream/handle. Дата звернення: Січ. 10, 2022.
[16] A. Jain Kumar, “Phishing Detection: Analysis of Visual Similarity Based Approaches”. [Online]. Available: https: //www.researchgate.net/publication/312205924_Phishing_Detection_Analysis_of_ Visual_Similarity_Based_Approaches. Accessed on: Febr. 4, 2022.
[17] D. Gupta, “Comparison of classification algorithms to detect phishing web pages using feature selection and extraction”. [Online]. Available: https://pdfs.semanticscholar.org/fccd/8ff23734a1947d3efc14d3df9863a5efac6c.pdf. Accessed on: Jan. 4, 2022.
[18] Анатомия фишинга, 2020. [Электронный ресурс]. Доступно: https://blog.avast.com/ru/the-anatomy-of-a-phish-avast. Дата обращения: Янв. 10, 2022.
[19] Всё о фишинге. [Электронный ресурс]. Доступно: https://ru.malwarebytes.com/phishing/. Дата обращения: Янв. 10, 2022.
[20] Фишинг своими руками, 2017. [Электронный ресурс]. Доступно: https://habr.com/ru/company/aktiv-company/blog/329470/. Дата обращения: Янв. 09, 2022.
[21] T. Dakpa, “Study of Phishing Attacks and Preventions”, International Journal of Computer Applications, vol. 163, no. 2, pp. 5-8, 2017. [Online]. Available: https://www.ijcaonline.org/archives/volume163/number2/dakpa-2017-ijca-913461.pdf. Accessed on: Jan. 14, 2022.

Стаття надійшла до редакції 15.02.2022.

REFERENCE

[1] Attack on the information front, 2022. [Online]. Available: https://cyberpolice.gov.ua/news/ataka-na-informaczijnomu-fronti---porady-kiberpolicziyi-shhodo-zaxystu-gadzhetiv-vid-vytoku-danyx-6563/. Accessed on: Jan. 3, 2022.

[2] Cyberpolice has stopped the activities of fraudsters, 2022. [Online]. Available: https://cyberpolice.gov.ua/news/u--roczi-kiberpolicziya-prypynyla-diyalnist--onlajn-shaxrayiv-6518/?fbclid=IwAR0RaghjZSzEzytXJ1RARnhVcWEq9IzPKgZIKj3ydsY8QgOaRgqSvEaifl8. Accessed on: Jan. 3, 2022.

[3] Quarterly threat trends & intelligence report November, 2021. [Online]. Available: https://www.phishlabs.com/blog/new-quarterly-threat-trends-intelligence-report-now-available/. Accessed on: Febr. 4, 2022.

[4] S. Dumchikov, and V. Luchikov, "Statistics of phishing incidents in Ukraine in 2021", 2021. [Online]. Available: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/34523/91970.pdf?sequence=2&isAllowed=y. Accessed on: Jan. 3, 2022.

[5] PhishTank. [Online]. Available: https://www.phishtank.com/what_is_phishing.php. Accessed on: Jan. 4, 2022.

[6] C. Whittaker, "Large-scale automatic classification of phishing pages", 2013. [Online]. Available: https://research.google.com/pubs/archive/35580.pdf. Accessed on: Jan. 5, 2022.

[7] Phishing Activity Trends Report, 1st Quarter, 2019. [Online]. Available: http://docs.apwg.org/reports/apwg_trends_ report_q1_2019.pdf. Accessed on: Jan. 4, 2022.

[8] M. Akulich, "Phishing and Marketing", 2022. [Online]. Available: https://books.google.com.ua/books?id=BLsVEAAAQBAJ&printsec=frontcover&hl=ru#v=onepage&q&f=false. Accessed on: Jan. 3, 2022.

[9] What is phishing and how to protect yourself from it. [Online]. Available: https://www.fg.gov.ua/articles/50140-shcho-take-fishing-i-yak-vid-nogo-zahistitis.html. Accessed on: Febr. 3, 2022.

[10] What is spam. [Online]. Available: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/spam/. Accessed on: Febr. 3, 2022.

[11] M. Khonji, Y. Iraqi, and A. Jones, "Phishing Detection: A Literature Survey", *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2091-2121, 2013. [Online]. Available: https://doi.org/10.1109/surv.2013.032213.00009. Accessed on: Jan. 5, 2022.

[12] I. Yakovyuk, A. Voloshin, and A. Shovkun, "Legal aspects of combating phishing: the experience of the European Union", *Problems of legality*, no. 149, pp. 16, 2020.

[13] D. Davydov, "Software for the system of forming filters against phishing on the Internet". [Online]. Available: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/4088/1/Conference MITandComp SysS2013_p89.pdf. Accessed on: Jan. 10, 2022.

[14] O. Boskin, and P. Chorny, "Analysis of the threat of phishing", in *Modern youth in the world of information technology*, N. Kirichenko and G. Dimova, Ed. Kherson, Ukraine: Kherson, 2021, pp. 179-181. [Online]. Available: http://dspace.ksau.kherson.ua/bitstream/handle/. Accessed on: Jan. 10, 2022.

[15] O. Boskin, and P. Chorny, "Analysis of protection against phishing", in *Modern youth in the world of information technology*, N. Kirichenko and G. Dimova, Ed. Kherson, Ukraine: Kherson, 2021, pp. 182-183. [Online]. Available: https://dspace.ksau.kherson.ua/bitstream/handle/. Accessed on: Jan. 10, 2022.

[16] A. Jain Kumar, "Phishing Detection: Analysis of Visual Similarity Based Approaches". [Online]. Available: https: //www.researchgate.net/publication/312205924_Phishing_Detection_ Analysis_of_ Visual_Similarity_Based_Approaches. Accessed on: Febr. 4, 2022.

[17] D. Gupta, "Comparison of classification algorithms to detect phishing web pages using feature selection and extraction". [Online]. Available: https://pdfs.semanticscholar.org/fccd/8ff23734a1947d3efc14d3df9863a5efac6c.pdf. Accessed on: Jan. 4, 2022.

[18] Anatomy of phishing, 2020. [Online]. Available: https://blog.avast.com/ru/the-anatomy-of-a-phish-avast. Accessed on: Jan. 10, 2022.

[19] All about phishing. [Online]. Available: https://ru.malwarebytes.com/phishing/. Accessed on: Jan. 10, 2022.
[20] Do-it-yourself Phishing, 2017. [Online]. Available: https://habr.com/ru/company/aktiv-company/blog/329470/. Accessed on: Jan. 9, 2022.
[21] T. Dakpa, "Study of Phishing Attacks and Preventions", International Journal of Computer Applications, vol. 163, no. 2, pp. 5-8, 2017. [Online]. Available: https://www.ijcaonline.org/archives/volume163/number2/dakpa-2017-ijca-913461.pdf. Accessed on: Jan.14, 2022.

ARTEM ZHYLIN,
OLHA SHEVCHUK

METHOD OF ANALYSIS FOR ANALYZING PHISHING MESSAGES

The development and widespread introduction of the Internet into everyday life has transformed both economic and social relations. The representation of these relations in digital form has created a digital economy, characterized by an active exchange of information, quick access to information resources, and the transfer of payments to the digital dimension. Social relations in the digital world are represented by social networks, instant messengers, which also provide economic services. At the same time, the new space, the transformed economy and social relations give rise to new threats. Users themselves actively expose information about themselves and their loved ones, photos of vacations and locations to the public. In addition to social networking, viewing entertainment content and online games, bank settlement transactions are popular. The popularization of Internet banking leads to an increased interest in stealing data from intruders. The result of this is an increase in the number of scammers who aim to obtain confidential user information. In addition, since the beginning of the war, the number of cyber attacks on public authorities, critical information infrastructure facilities and organizations containing critical information has increased. One of the well-known methods of stealing such information is phishing attacks. At the same time, most users underestimate the severity of these attacks and do not pay enough attention to protection systems. This, in turn, leads to wider consequences. Therefore, the problem to be solved is to present a method for analyzing phishing messages that can be used to reduce the probability of reaching the goal of a phishing attack. At the same time, it is known that attackers improve and modify the methods of implementing attacks, and therefore, classifying phishing attacks to increase user awareness is an urgent task. The result of the work is the proposed classification of phishing attacks and the presented method for analyzing phishing messages.

Keywords: phishing, cyber fraud, phishing messages, classification of phishing attacks, method of analysis.

Жилін Артем Вікторович, кандидат технічних наук, доцент, професор кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID ID 0000-0002-4959-612X, zhylinartem@gmail.com.

Шевчук Ольга Сергіївна, викладач-стажист кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID ID 0000-0002-2866-439X, olia13511@gmail.com.

Zhylin Artem, candidate of technical sciences, associate professor, professor at the cybersecurity and application of information systems and technology academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Shevchuk Olha, trainee teacher at the cybersecurity and application of information systems and technology academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.