DOI 10.15276/imms.v12.no3.226
УДК 004.056

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 3, pp. 226-235

ЗАХИСТ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В КОНТЕКСТІ СУЧАСНИХ ГІБРИДНИХ ВІЙН

О.М. Симонова, І.І.Бобок

Національний університет «Одеська політехніка»,
просп. Шевченка, 1, Одеса, 65044,Україна; e-mail: simonova.a.m@ukr.net

Фішинг використовується для розповсюдження шкідливого програмного забезпечення і зараження мереж критичної інфраструктури. Починаючи з 2000 років фішинг набуває популярності у кіберзлочинців. Одну з перших великих, спроб було зроблено 2001 року, коли в хаосі після терактів 11 вересня зловмисники відправили своїм жертвам електронні листи нібито для перевірки їхньої особистості. Отримані дані було використано для крадіжки банківських даних. Електронна пошта стала одним із надійних засобів зв'язку в реальному часі, за допомогою якого величезна кількість людей і організацій обмінюються своїми повідомленнями та даними. Зі значним збільшенням кількості користувачів електронної пошти зловмисники використовують електронну пошту різними способами, щоб спонукати користувачів розкривати свої облікові дані. Прикладом використання електронної пошти для фішингової атаки є розповсюдження вірусу Petya та NotPety у 2017 році, який брав свій початок з української державної енергокомпанії та вважається частиною російсько-української гібридної війни. Питання протидії фішинговим атакам в Україні та у всьому світі загалом залишається гострим. Користувачі Інтернету постійно стикаються зі спробами заволодіння їх даними. Жертвами можуть стати також великі компанії, що, може поставити під загрозу безпеку держави, якщо фішингова атака є частиною кібервійни. У роботі був удосконалений алгоритм виявлення небезпечний електронних листів, який відрізняється від існуючих комплексним підходом аналізу з використанням раніше не застосованим у цьому напрямку методі, що дозволило підвищити ефективність аналізу з коротким часом обчислень. Результати даної роботи можуть бути використані для захисту інформаційно-телекомунікаційних мереж від розповсюдження шкідливого програмного забезпечення та/або витоку даних.

Ключові слова: фішинг, електрона пошта, кіберзбезпека, інформаційна безпека

Вступ

Вид ворожих дій, при якому атакуюча сторона не вдається до класичного військового вторгнення , а пригнічує супротивника, використовуючи комбінацію таємних операцій, диверсій, кібервійни, а також надаючи підтримку. повстанцям, які діяли на території ворога називається гібридною війною. При цьому військові дії можуть взагалі не вестися, і, з формальної точки зору, гібридна війна може відбуватися в мирний час.

Одною з високоефективних форм кіберзлочинності сьогодні є фішинг [2]. Фішинг – це різновид соціальної інженерії, який полягає в наступному: зловмисник-шахрай надсилає електронною поштою повідомлення, призначене для змушення людини розкрити конфіденційну інформацію зловмисникові [1] або розгорнути шкідливе програмне забезпечення в інфраструктурі жертви, поширеним прикладом чого є програми-вимагачі.

Відповідно з Radicati Group [3], загальна кількість користувачів електронної пошти на початку 2021 року становила приблизно 4,1 мільярда, і, за прогнозами, зросте до 4,5 мільярдів до кінця 2025 року, що робить питання боротьби з ним одним з найактуальніших сучасних питань кібербезпеки.

Зловмисники використовують повідомлення електронної пошти з переконливим вмістом як приманку для викрадення особистої інформації користувачів; електронний лист направляє користувача через гіперпосилання на веб-сайт, що належить злочинцям, який візуально копіює офіційний (законний) веб-сайт, де користувачеві пропонують ввести особисту та/або фінансову інформацію. Це дозволяє злочинцям отримати доступ до цієї цінної інформації, яку вони потім використовують для вчинення шахрайства або продажу. Кіберзлочинці також можуть обманом змусити користувачів завантажити шкідливі коди або зловмисне програмне забезпечення шляхом натиснення на посилання, вбудоване в електронний лист.

Актуальність теми роботи полягає у тому, що, незважаючи на існування багатьох методів та підходів для захисту користувачів від фішинг-атак [4-7], ця проблема не є вирішеною повною мірою, а питання захисту у цьому напрямку залишається доволі гострим, зокрема для нашої країни: за даними Національного координаційного центру кібербезпеки у 2021 році в Україні зафіксовано понад 400 тис. випадків фішингових атак [8]

Для боротьби з фішингом поштові клієнти використовують спам-фільтри, які відправляють підозрілі листи в карантин (папки спаму), а не в основну поштову скриньку користувача. Однак ці фільтри не завжди ефективні: з понад 555 000 фішингових листів, проаналізованих компанією хмарної безпеки Avanan в рамках свого Global Phish Report 2019 [9], 25% оминули заходи безпеки Office 365, в результаті чого потрапили до поштових скриньок потенційних жертв.

Мета роботи

Метою роботи є розробка алгоритму захисту пошти від фішингових атак, який може бути імплантовано у сучасний браузер.

Основна частина

Електронний лист складається з двох частин: заголовків та вмісту. У роботі пропонується алгоритм, який би враховував в аналізі на наявність фішингу обидві частини листа, використовуючи гібридний метод аналізу, та реалізація цього алгоритму шляхом створення розширення для браузера під назвою Athena logic.

Підробка електронної пошти – техніка, яка використовується під час атак зі спамом і фішингом, щоб змусити користувачів подумати, що повідомлення надійшло від особи чи організації, яку вони знають або якій можуть довіряти. Під час спуфінгу відправник підробляє заголовки електронної пошти, щоб клієнтське програмне забезпечення відображало шахрайську адресу відправника, яку більшість користувачів сприймають за чисту монету. Якщо вони не перевірять заголовок уважніше, користувачі побачать у повідомленні підробленого відправника. Якщо це ім’я, яке вони впізнають, вони, швидше за все, довірятимуть йому. Тож вони натискатимуть шкідливі посилання, відкриватимуть вкладені файли зловмисного програмного забезпечення , надсилатимуть конфіденційні дані та навіть переведуть корпоративні кошти.

У роботі пропонується проведення аналізу наступних частин заголовків електронного листа для запобігання фішингу:

— Return-Path;
— Reply-To;
— Received-SPF;
— DKIM (Domain Keys Identified Mail).

Адреса електронної пошти Return-Path містить інформацію про статус відправлення. Поштовий сервер зчитує вміст заголовка Return-Path для обробки повідомлень, які не можна доставити або повернути відправнику. Сервер-одержувач використовує це поле для ідентифікації «підроблених» електронних листів: він запитує всі дозволені IP-адреси, пов’язані з доменом відправника, і порівнює їх з IP-адресою автора повідомлення. Якщо вони не знайдуть збігів, лист відправляється в спам.

Адреса електронної пошти в полі Reply-To використовується для надсилання відповіді. У фальшивих електронних листах вона може відрізнятися від адреси відправника.

Received-SPF дозволяє одержувачу перевірити, що електронна пошта, яка нібито походить з певного домену, походить з IP-адреси, дозволеної адміністраторами цього домену. Адміністратор домену зазвичай авторизує IP-адреси, які використовують його власні вихідні MTA, включаючи будь-які проксі-сервери або смарт-хости [10].

При встановленні з'єднання протокол управління трафіком перевіряє IP-адресу відправника MTA і переконується, що віддалений хост доступний. Поштовий сервер-одержувач отримує команду HELO SMTP незабаром після встановлення з'єднання і команду Mail from: на початку кожного повідомлення. Обидва можуть включати в себе доменне ім'я. Верифікатор SPF запитує в системі доменних імен (DNS) відповідний SPF-запис, який, за наявності, ідентифікує IP-адреси, дозволені адміністратором домену. Це поле є дійсним, якщо воно має значення PASS.

DKIM перевіряє зміст повідомлень за допомогою цифрових підписів. Замість цифрових сертифікатів через DNS розповсюджуються ключі перевірки підпису. Таким чином, повідомлення асоціюється з доменним ім'ям.

Адміністратор DKIM-сумісного домену створює одну або більше пар асиметричних алгоритмів шифрування, потім відправляє закриті ключі підписуючим MTA і публікує відкриті ключі в DNS. DNS мітки структуровані у вигляді selector._domainkey.example.com, де селектор вказує пару ключів, а _domainkey - фіксоване ключове слово, за яким слідує назва підписаного домену, щоб публікація перебувала під контролем ADMD цього домену. Безпосередньо перед тим, як вставити повідомлення в транспортну систему SMTP, підписуючий MTA створює цифровий підпис, який охоплює вибрані поля заголовка і тіла (або тільки початок). Підпис повинен включати основні поля заголовка, такі як «Від кого», «Кому», «Дата» і «Тема», а потім додаватися до самого заголовка повідомлення як поле для відстеження.

Повідомлення можуть прийматися і відправлятися будь-якою кількістю ретрансляторів, і на кожному кроці підпис може бути перевірений шляхом отримання відкритого ключа з DNS [11]. Поки посередники не змінюють підписані частини повідомлення, підписи повідомлень DKIM залишаються дійсними. Це поле є дійсним, якщо воно має значення PASS.

Для аналізу вмісту листа у роботі використовується семантичний аналіз для порівняння слів та словосполучень. Порівняння здійснюється за допомогою двох словників: спаму та тональності (настроїв), аналізуючи слова, вирази та символи, як видимі, так і приховані для людського ока, за допомогою різних методів.

У роботі використовується словник OOPSpam та український тональний словник [12], який містить 3442 слова української мови, які мають не нейтральну тональність.

Мета аналізу настроїв полягає в аналізі певної кількості даних, щоб визначити різні почуття, виражені в них. Отримані почуття потім можуть бути предметом статистичних даних щодо загального відчуття спільноти. Прикладом

використання тональності тексту є робота Мангурі та ін. [13], які проводили аналіз настроїв записів користувачів у Twitter щодо спалахів COVID-19 у всьому світі.

Сентимент-аналіз дозволяє аналізувати листи «вимагачі», «жебраки» або «благодійні», які можуть бути надіслані з реальних адрес та не містити жодного посилання. У цьому разі фішери використовують як зброю слова, щоб викликати у жертви конкретні емоції та відчуття. Зазвичай виділяють два види емоцій: позитивні та негативні, виконуючи класифікацію за двома класами, для якої в роботі використовується лексичний аналіз.

Підхід, заснований на лексичному аналізі, полягає у виведенні емоцій, які викликає речення, за допомогою семантичного аналізу слів. Цей підхід включає класифікацію речення за допомогою вже існуючих екземплярів речень, для яких емоції ідентифіковано, для чого використовується словник. Кожне слово тексту зіставляється зі словником; якщо знайдене співпадіння, то тональність тексту зростає.

Словник спаму містить у собі слова та словосполучення з типовою лексикою спаму.

Зміст листа може містити посилання. У цьому випадку метою зловмисника є перенаправлення жертви на певний веб-ресурс, куди зловмисник намагається впровадити шкідливе програмне забезпечення, використовуючи вразливості в самій сторінці або при переході в браузері.

URL-фішинг – це шахрайська практика заманювання людей на фальшиві сайти з переконливим змістом, де вони завантажують шкідливе програмне забезпечення або розкривають конфіденційну інформацію, таку як імена користувачів, паролі та банківські реквізити. Один з найпоширеніших прикладів такої атаки, коли шахраї імітують компанію та надсилають електронного листа з наступним повідомленням: «Ваш обліковий запис заблоковано. Відновити його можна за посиланням». Ошуканий користувач переходить за посиланням і несвідомо завантажує шкідливе програмне забезпечення або переходить на підроблений веб-сайт, який виглядає легітимно. Після переходу за посиланням користувач може стати жертвою різного роду XSS-атак. Суть цих атак полягає у виконанні скрипту в браузері та його подальшій взаємодії з сервером зловмисника. Ці операції відкривають доступ до даних браузера і дозволяють ввести в нього експлойтів, а також викрадати файли cookie, дані авторизації або, наприклад, здійснювати HTTP-запити від імені користувача.

За даними Звіту про розслідування порушень даних [14] близько 91% порушень безпеки починаються з фішингової атаки, і багато з них включають шкідливі посиланням на підроблені сайти.

У роботі URL-адреса аналізується за наступними критеріями:

- наявність символу «@»;
- довжина URL-адреси;
- кількість скісних рисок.

Зловмисники часто використовують подвійні скісні риски, щоб приховати шахрайську частину URL-адреси. Якщо URL-адреса містить забагато символів «/», вона є фішинговою, в іншому випадку - легітимною.

Підрахунок кількості символів в URL-адресі є важливою характеристикою для виявлення шахрайських джерел. Зловмисники використовують довгі URL-адреси, щоб приховати шахрайську частину адреси в адресному рядку. Таким чином, видима частина адресного рядка містить легітимну URL-адресу, яка може вводити в оману. Якщо довжина URL-адреси перевищує 35-символьний ліміт, джерело вважається підозрілим, в іншому випадку джерело легітимне [15].

Символ равлика «@» використовується для перенаправлення трафіку на інший, як правило шахрайський, сайт, доменне ім'я якого одразу супроводжується символом @. Наприклад, http://op.edu.ua@download.file.com перенаправить користувача на download.file.com замість op.edu.ua. Усе, що стоїть перед равликом, відкидається. Як правило, цей синтаксис сьогодні практично не використовується. Так, якщо в адресному рядку з'являється символ "@", то URL-адреса вважається підозрілою, в іншому випадку - легальною.

З урахуванням вищенаведеного пропонується наступний алгоритм захисту електронної пошти від фішингових атак, блок-схема якого наведена на рис. 1.

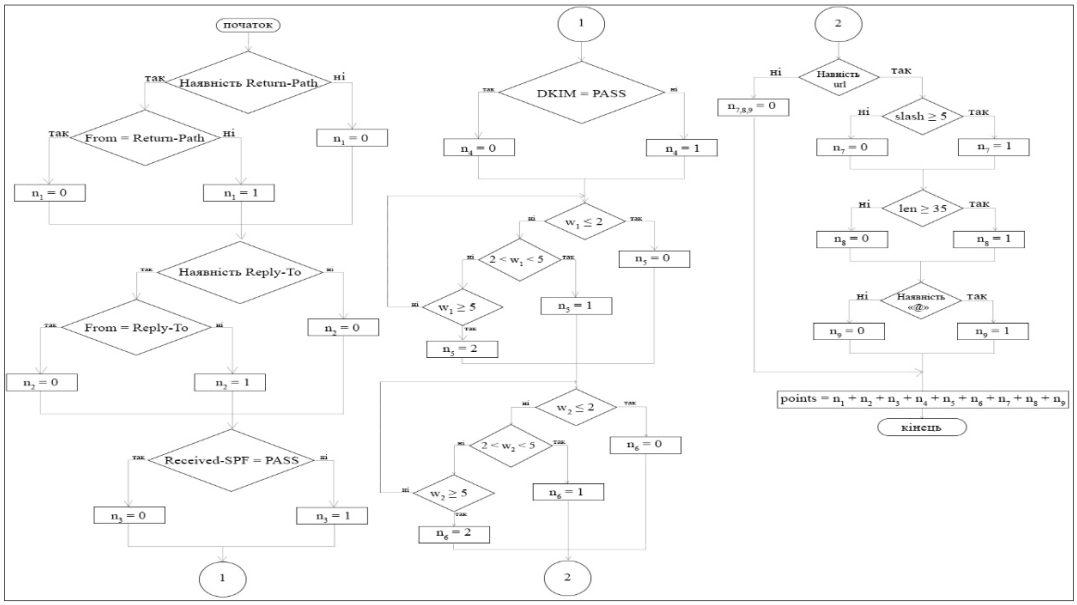

Рис. 1 Блок-схема розробленого алгоритму

Крок 1. Перевірка Return-Path, на виході якої отримуємо n_1 – бали фішингу за рівність *From = Return-Path*. Спочатку перевіряється наявність заголовка Return-Path. У деяких випадках, наприклад, при автоматичному повідомлені від системи безпеки, цей заголовок може бути відсутній. Якщо поле заголовка знайдено, воно зіставляється з полем заголовка From: при співпадінні $n_1 = 0$, якщо збігів не знайдено – $n_1 = 1$.

Крок 2. Перевірка Reply-To, на виході якої отримуємо n_2 – бали фішингу за рівність From = Reply-To. Спочатку перевіряється наявність заголовка Reply-To. Якщо поле заголовка знайдено, воно зіставляється з полем заголовка From: при співпадінні $n_2 = 0$, якщо збігів не знайдено – $n_2 = 1$.

Крок 3. Перевірка заголовка Received-SPF, де отримуємо n_3 – бали фішингу за рівність *Received-SPF = PASS*. При співпадінні $n_3 = 0$, якщо збігів не знайдено – $n_3 = 1$.

Крок 4. Перевірка співпадіння DKIM і PASS (n_4): при співпадінні $n_4 = 0$, якщо збігів не знайдено – $n_4 = 1$.

Після аналізу заголовків, алгоритм переходить до аналізу вмісту листа.

Крок 5. Сентимент аналіз, на виході якого отримаємо n_5 – кількість балів за перевірку листа за словником тональності: кожне слово листа зіставляється зі словником, при виявленні збігів (w_1) відбувається перевірка умов. Якщо збігів менше 2 – $n_5=0$, якщо у діапазоні між 2 та 5 – $n_5=1$, якщо більше 5 – $n5=2$.

Крок 6. Аналіз перевірки листа за словником спаму, на виході якої отримуємо n_6 – кількість балів за перевірку листа за словником спаму. Кожне слово листа зіставляється зі словником, при виявленні збігів (w_2) відбувається

перевірка умов. Якщо збігів менше двох – $n_6=0$, якщо у діапазоні між двома та п'ятьома – $n_6=1$, якщо більше п'яти, то $n_6=2$.

У обох випадках якщо кількість збігів $w_n > 5$, n – номер словника, то бали фішинга дорівнюють 2. Зловмисники мають на меті приховати свою особистість та за допомогою маніпулятивних дій – речень – завдати користувачеві матеріальної або психологічної шкоди. У роботі припускається, що зловмисники можуть використовувати тактики маркетингу для збільшення імовірності ввести потенційну жертву в оману. Однією з таких тактик є метод «холодного листа». Холодний лист – це перший лист, який надсилається потенційному клієнту, тобто перший контакт з людиною. Дослідження [16-17] показали, що ідеальна довжина для листа (щоб він міг вважатися «холодним») варіюється від 50 до 200 слів. На основі цього отримано, що кількість слів-збігів не може перевищувати 10% від загальної кількості слів листа (табл. 1) та обрано середнє значення з можливих.

Таблиця 1

Відсоток збігів w_n

Кількість слів	Відсоток збігів, %
50	10
75	6,7
100	5
125	4
150	3,3
175	2,8
200	2,5

Відповідно до запропонованого алгоритму:

Крок 7. Перевірки на наявність посилань. Якщо посилання не знайдено, то $n_{7,8,9}$ – кількість балів фішингу за кожний критерій, буде дорівнювати 0. У іншому випадку:

7.1. Перевірка URL-посилань на кількість символів «/» – *slash*, на виході якої отримуємо n_7 – кількість балів фішингу за цей критерій. Якщо $slash \geq 5$ – $n_7 = 1$, в іншому випадку – $n_7 = 0$.

7.2. Перевірка URL-посилань на загальну кількість символів (*len*), на виході якої отримуємо n_8. Якщо $len \geq 35$ – $n_8 = 1$, в іншому випадку – $n_8 = 0$.

7.3. Перевірка на наявність в URL символу равлика «@», та, якщо він є, кількість балів за дану перевірку (n_9) дорівнюватиме 1, в іншому випадку – 0.

У таблиці 2 відображена максимальна кількість балів, яку може отримати кожний критерій аналізу окремо.

Таблиця 2

Розподіл балів фішингу

Заголовки					Вміст листа			
Return-Path (n_1)	Reply-To (n_2)	Received-SPF (n_3)	DKIM (Domain Keys Identified Mail (n_4)	Словник тональності тексту (n_5)	Словник «спаму» (n_6)	Наявність посилання		
						Символ @ (n_7)	Кількість // (n_8)	Довжина url (n_9)
1	1	1	1	2	2	1	1	1

Крок 8. Отримання загальної кількості балів: $points = n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 + n_8 + n_9$, де *points* – загальна кількість балів.

Крок 9. Висновок. Небезпечність листа залежить від кількості балів (табл. 3).

Таблиця 3

Залежність результату перевірки листа від значення загальної кількості балів

Результат	Кількість балів (points)
Небезпечно	points>3
Сумнівно	2 ≤ points ≤ 3
Безпечно	points<2

Користувачі Інтернету можуть використовувати розширення браузера, щоб оптимізувати його використання. Розширення веб-браузера – це доповнення до обраного користувачем веб-переглядача, які можуть вносити зміни на стороні клієнта, щоб змінити спосіб відображення веб-сторінок або надавати користувачеві інструменти, які допомагають йому під час перегляду Інтернету.

Розширення браузера можна використовувати для виявлення різних форм фішингових атак, наприклад, «GoldPhish» — це розширення Internet Explorer, яке використовується для виявлення фішингових веб-сторінок.

Розширення для браузера Athenalogic було розроблено для того, щоб дозволити користувачеві класифікувати електронні листи у своєму клієнті веб-пошти як легітимні або фішингові.

Як показано на рис. 2 станом на жовтень 2022 Google Chrome має 66,7% користувачів по світу [16] та близько 60% в Україні [17] (рис. 3). Саме тому розширення для веб-браузера було розроблено для Chrome, бо він залишається доступним для найбільшої кількості користувачів.

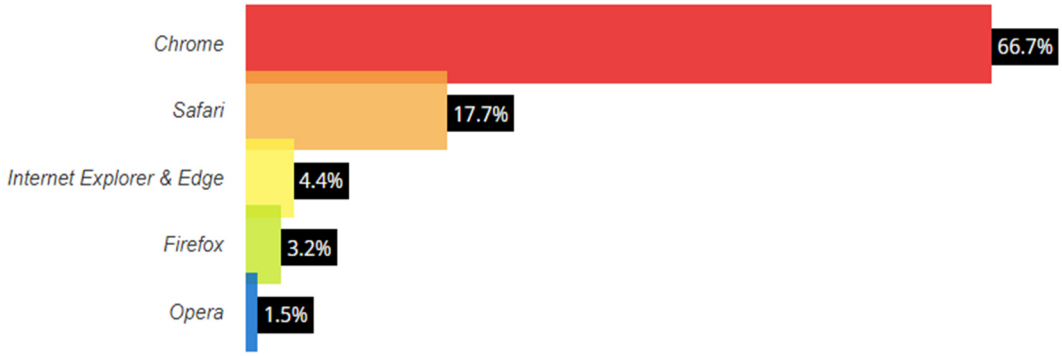

Рис. 2 Статистика популярності браузерів у світі

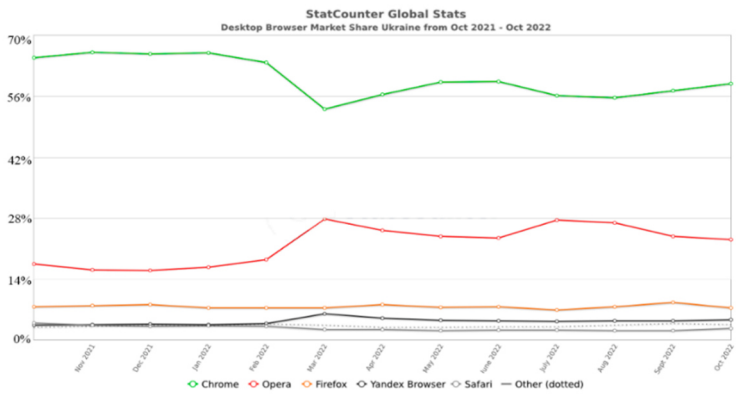

Рис. 3 Статистика популярності браузерів на ПК в України

Athena logic використовує розподіл балів для виявлення фішингових листів. Спочатку розширення аналізує заголовки, при кожному неспівпадінні додаються «бали фішингу» (далі – бали), потім вміст на наявність «спам-слів», слів з позитивним та/або негативним емоційним забарвленням і посилань за описаними вище критеріями.

Для оцінки ефективності розробленого в роботі розширення на практиці, було проведене дослідження, у якому порівнювались п’ять інших розширень (табл. 4, 5) з Athena logic.

Таблиця 4

Порівняння інших додатків для Chrome

Розширення	Опис	Переваги	Недоліки
MailTrout	Використовується метод на основі машинного навчання	Зручність використання; Розширення подається як освітній інструмент, який навчає користувачів самостійно виявляти фішингові електронні листи	Хибні спрацювання; великий час оброблень
Ter7AntiPhishing	Семантичний аналіз з використанням словника	Зручність використання	Малий відсоток вірно визначених фішингових листів; Лише для Gmail
PhishBlock Prediction	Аналізує url-адреси в листах Евристичний метод	Швидкий аналіз	Наявність певного відсотка помилково-позитивних результатів; Не переглядає вміст електронної пошти; Лише для Gmail
Detect spam emails	Семантичний аналіз з використанням словника	Зручність використання	Хибні спрацювання
Email Phishing Tool	Семантичний аналіз з використанням словника Аналізує url-адреси в листах Евристичний метод	Хороші результати на невеликих наборах даних.	Малий відсоток вірно визначених фішингових листів; Малий відсоток визначення фішингових url;

Таблиця 5

Результати дослідження

Розширення	Точність, %
MailTrout	48
Ter7AntiPhishing	31
PhishBlock Prediction	54
Detect spam emails	30
Email Phishing Tool	42
Athena Logic	94

Результати дослідження, представлені у табл. 5, показали ефективність Athena logic, що значно перевищує ефективність аналогів, та довели, що для успішного аналізу для виявлення фішингу, необхідно охоплювати обидві частини електронного листа. Так, розширення Ter7AntiPhishing та Detect spam emails показали низький відсоток точних результатів через залежність від словникового методу: листи з коротким та, на перший погляд, легітимним змістом, але з небезпечними посиланнями, вони виявили як безпечні.

Розширення PhishBlock Prediction безглузде у випадках відсутності у листах посилань. MailTrout у свою чергу сприймає легітимні листи за фішингові.

Висновки

У результаті виконання роботи був запропонований алгоритм виявлення фішингових листів, що використовує гібридний метод аналізу, та розроблена програмна реалізація цього методу у вигляді розширення для браузера Chrome. Розширення браузера можуть діяти як доступні інструменти безпеки, оскільки для використання вони потребують небагато технічних знань і можуть бути легко включені в стандартну онлайн-діяльність людини.

Завдяки своїй простоті створене розширення може бути особливо корисними для тих, хто має незначний досвід користування Інтернетом, і як інструменти безпеки можуть ефективно захистити найбільш вразливі групи.

В результаті порівняльного аналізу ефективності розробленого розширення браузера з існуючими аналогами встановлено, що він перевищує найкращий з існуючих на 40%.

Список літератури

1. Jansson K., Von Solms R., Phishing for phishing awareness. *Behaviour and Information Technology*. 2013.V32, #6, P.584-593
2. Alkhalil Z, Hewage C, Nawaf L., Khan I. Phishing Attacks: *A Recent Comprehensive Study and a New Anatomy*, 2021
3. Radicati S. Email statistics report. The Radicati Group, Inc; 2016.
4. Cisco Advanced Phishing Protection. URL: https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-email-security/at-a-glance-c45-740894.pdf
5. Office 365 Advanced Threat Protection. URL: https://docs.microsoft.com/ru-ru/microsoft-365/security/office-365-security/office-365-atp
6. Бойл П. Впровадження розширення браузера для виявлення фішингових електронних листів за допомогою обробки природної мови,
7. Gascon, H., Ullrich, S., Stritter, B., Rieck, K. Reading Between the Lines: Content-Agnostic Detection of Spear-Phishing Emails. Research in Attacks, Intrusions, and Defenses. 2018. *Lecture Notes in Computer Science*, Vol 11050. URL:https://doi.org/10.1007/978-3-030-00470-5_4
8. Ради національної безпеки і оборони України, НКЦК: у 2021 році в Україні зафіксовано вже майже 14 мільйонів інцидентів у сфері кібербезпеки. URL: https://www.rnbo.gov.ua/ua/Diialnist/4797.html
9. Global-Phish-Report 2019. URL: https://www.avanan.com/hubfs/2019-Global-Phish-Report.pdf
10. Klensin J. Simple Mail Transfer Protocol, 2008. URL: https://www.rfc-editor.org/info/rfc5321
11. Crocker D. DKIM Frequently Asked Questions. URL: https://www.dkim.org/info/dkim-faq.html
12. Ukrainian tone dictionary. URL: https://github.com/lang-uk/tone-dict-uk

13. Manguri K.N., Ramadhan R.R. Mohammed A.P. Twitter Sentiment Analysis on Worldwide COVID-19 Outbreaks. *Kurdistan Journal of Applied Research*. 2020. P. 54–65. URL: https://doi.org/10.24017/covid.8.
14. Data Breach Investigations Report - Executive Summary, 2017
15. Орунсолу А.А., Содия А.С.. Акинвале А.Т. Прогностическая модель для обнаружения фишинга. *Журнал Университета короля Сауда — компьютерные и информационные науки.* URL:https://doi.org/10.1016/j.jksuci.2019.12.005
16. Renahan M. The Ideal Length of a Sales Email, Based on 40 Million Emails. *HubSpot Blog*. URL: https://blog.hubspot.com/sales/ideal-length-sales-email.
17. Kristensen E. What's the Ideal Email Length?. *The Ecommerce Revenue Engine | Drip*. URL: https://www.drip.com/blog/ideal-email-length.
18. Browser and Platform Market Share, 2022. URL: https:// web.archive.org/web/20221018205527/https://www.w3counter.com/globalstats.php
19. Desktop Browser Market Share Ukraine. 2022. URL: https://gs.statcounter.com/browser-market-share/desktop/ukraine

PROTECTION OF INFORMATION AND TELECOMMUNICATION NETWORKS FROM MALICIOUS SOFTWARE IN THE CONTEXT OF MODERN HYBRID WARS

O.M. Symonova, I.I.Bobok

National Odesa Polytechnic University,
ave. Shevchenko, 1, Odesa, 65044, Ukraine; e-mail: simonova.a.m@ukr.net

Phishing is used to spread malicious software and infect critical infrastructure networks. Since 2000, phishing has been gaining popularity among cybercriminals. One of the first big attempts was made in 2001, when in the chaos after the September 11 attacks, attackers sent their victims e-mails allegedly to verify their identity. The obtained data was used to steal bank data. Email has become one of the reliable means of real-time communication through which a huge number of people and organizations share their messages and data. With the dramatic increase in the number of email users, attackers are using email in a variety of ways to trick users into revealing their credentials. An example of email being used for a phishing attack is the spread of the Petya and NotPety virus in 2017, which originated from a Ukrainian state energy company and is considered part of the Russian-Ukrainian hybrid war. The issue of countering phishing attacks in Ukraine and around the world in general remains acute. Internet users are constantly faced with attempts to get hold of their data. Large companies can also become victims, which can endanger the security of the state if a phishing attack is part of a cyber war. The work included an improved algorithm for detecting dangerous e-mails, which differs from the existing ones by a comprehensive approach to analysis using a previously unapplied method in this direction, which made it possible to increase the efficiency of the analysis with a short calculation time. The results of this work can be used to protect information and telecommunication networks from the spread of malicious software and/or data leakage.

Keywords: phishing, e-mail, cyber security, information security