УДК 004.056.5

Барбак В. Д., здобувач вищої освіти,
Ніколюк П. К., д-р фіз.-мат. наук, професор,
професор кафедри інформаційних технологій,
Донецький національний університет імені Василя Стуса

ВИКОРИСТАННЯ МЕТОДІВ ЗАХИСТУ ВІД ФІШИНГУ ТА ІДЕНТИФІКАЦІЯ ШАХРАЇВ У ЕЛЕКТРОННІЙ ПОШТІ

Анотація. Фішингові атаки залишаються однією з найбільших кіберзагроз, спрямованих на викрадення даних користувачів. Дослідження показало ефективність використання багатофакторної автентифікації та методів перевірки автентичності відправника для запобігання фішинговим атакам.

Ключові слова: *фішинг, кібербезпека, багатофакторна автентифікація, електронна пошта, захист даних.*

Вступ. Фішингові атаки залишаються однією з найбільш поширених та небезпечних кіберзагроз, націлених на викрадення конфіденційних даних користувачів, як-от паролі, фінансова інформація або доступ до корпоративних мереж. Зловмисники підробляють електронні листи так, щоб вони виглядали як офіційні повідомлення від відомих компаній або організацій. Метою таких атак є отримання доступу до інформації користувачів або проникнення в їхні особисті або корпоративні акаунти. З розвитком технологій захисту методи фішингу стають дедалі складнішими, що вимагає нових, більш ефективних підходів до виявлення та запобігання таким загрозам. У цій роботі досліджуються сучасні методи захисту від фішингових атак в електронній пошті та підходи до ідентифікації шахраїв.

Класифікація методів захисту від фішингу. Методи захисту від фішингових атак можна умовно розділити на три основні категорії:

1. Аналіз контенту електронного листа. Перевірка вмісту повідомлення, аналіз лінків і зображень за допомогою фільтрів, що працюють на основі правил або машинного навчання [3].

2. Перевірка автентичності відправника. Використання протоколів, як-от SPF, DKIM та DMARC, що забезпечують верифікацію правдивості адреси відправника та знижують імовірність підробки доменів [4].

3. Методи багатофакторної автентифікації (MFA). Додаткові фактори авторизації (наприклад, SMS, мобільні додатки або біометричні дані) підвищують захист навіть у випадках компрометації пароля [5].

Ідентифікація шахраїв на основі метаданих електронної пошти. Метадані електронних повідомлень містять важливу інформацію для ідентифікації шахрайських листів. Серед таких ознак є IP-адреса, геолокація відправника, доменні сертифікати та відповідність домену в листі. Методи фільтрації спаму аналізують ці ознаки для виявлення аномалій.

Один із підходів включає використання вагових коефіцієнтів для різних ознак листа, що допомагає визначати ймовірність фішингової атаки за формулою:

$$P(fish) = \frac{\sum_{i=1}^{n} w_i * A_i}{\sum_{i=1}^{n} w_i}, \quad (1)$$

де A_i – це ознаки, w_i – вагові коефіцієнти, які визначають важливість кожної ознаки.

Результати, наведені в цій роботі, отримані на основі аналізу фішингових атак на корпоративні поштові системи, взятих з досліджень, проведених у межах роботи J. Smith у журналі Journal of Cybersecurity (2019) та A. Shcherbakov у Information Security Journal (2021). Зокрема, методи перевірки автентичності відправника знизили кількість успішних атак на 45 %, а використання багатофакторної автентифікації (MFA) зменшило компрометацію облікових записів на 99 % [2, 3].

Дослідження J. Smith також виявило, що фільтри на основі машинного навчання опрацювали 85 % фішингових листів, що містили підроблені посилання або шкідливі вкладення. Аналіз метаданих, що включав перевірку IP-адрес і відсутність записів SPF і DKIM, показав ефективність в ідентифікації 70 % шахрайських листів [2].

Багатофакторна автентифікація як ефективний метод захисту. Багатофакторна автентифікація (MFA) надійно запобігає компрометації облікових записів, поєднуючи пароль із додатковим підтвердженням (одноразовим кодом або біометрією). Дослідження показали, що використання MFA знижує успішність фішингових атак на 99 %, що роблить її важливим заходом для захисту конфіденційних даних у корпоративній пошті [2].

Висновки. Фішинг стає все складнішим, використовуючи персоналізацію та соціальну інженерію для отримання довіри. Нові методи шифрування та приховування шкідливих посилань у HTML-коді ускладнюють автоматичне виявлення загроз. У перспективі очікується застосування штучного інтелекту для аналізу великих обсягів даних і впровадження поведінкової біометрії та блокчейн-технологій для безпеки цифрових ідентифікаторів.

Захист від фішингу є критичним для кібербезпеки. Комплексні заходи, як-от багатофакторна автентифікація, аналіз метаданих і машинне навчання, підвищують безпеку, але шахрайські методи постійно розвиваються, що вимагає адаптації підходів до запобігання атак.

Список використаних джерел

1. Співак І. О. Захист інформації у електронній пошті. Київ: Наукова думка, 2020.
2. Smith J. Phishing Attacks: Detection and Prevention. *Journal of Cybersecurity*. 2019. № 5. С. 34–47.
3. Shcherbakov A. Advanced Email Security Solutions. *Information Security Journal*. 2021. № 7. P. 89–102.
4. Ivanov D. Methods for Identifying Phishing Emails. *Cyber Defense Review*. 2020. № 8. P. 23–33.
5. Захарова О. М. Фішинг та способи його уникнення. Харків: Вид-во НТУ «ХПІ», 2019.