УДК 004.056.53 DOI: 10.31673/2409-7292.2026.032709

**Корченко Анна Олександрівна**
доктор технічних наук, професор, професор кафедри безпеки інформації та телекомунікацій,
Національний технічний університет «Дніпровська політехніка», Дніпро, Україна
ORCID: 0000-0003-0016-1966
E-mail: annakor@ukr.net

**Аскеров Мукафат Гейбат огли**
кандидат технічних наук, професор кафедри мобільних та відеоінформаційних технологій
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0000-6611-2732
E-mail: mukafat_ask@ukr.net

**Давиденко Кирило Олександрович**
аспірант кафедри безпеки інформації та телекомунікацій,
Національний технічний університет «Дніпровська політехніка, Дніпро, Україна
ORCID: 0009-0001-9209-1274
E-mail: kirilldavy@gmail.com

**Герасименко Антон Андрійович**
Аспірант кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0008-4475-2040
E-mail: anton.hrsmnk@gmail.com

**Журов Юрій Станіславович**
IT-спеціаліст
SMB Cybersecurity Advisors, United States of America
ORCID: 0000-0002-8276-2230
E-mail: iurii.zhurov@smbsecurityadvisors.com

# МЕТОД ФОРМУВАННЯ ПРОФІЛЮ СОЦІОТЕХНІКА ЗА ВИЯВЛЕНОЮ ФІШИНГ-АТАКОЮ НА ІНФОРМАЦІЙНУ СИСТЕМУ

Фішингові атаки залишаються одним із найпоширеніших інструментів реалізації кіберзагроз, оскільки поєднують технічні механізми компрометації інформаційних систем із методами соціальної інженерії. Водночас сучасні засоби виявлення фішингу переважно орієнтовані на аналіз технічних параметрів атаки та не забезпечують формалізованого переходу від результатів її детекції до визначення характеристик виконавця, що ускладнює процеси атрибуції кібератак, кіберрозвідки та реагування на інциденти інформаційної безпеки. Метою роботи є розроблення методу формування профілю соціотехніка за результатами аналізу виявленої фішинг-атаки на інформаційну систему. Запропонований метод ґрунтується на розширенні узагальненого кортежу шляхом інтеграції множини ознак профілю порушника, сформованої відповідно до теоретико-множинної моделі класифікації сучасних підходів реалізації соціотехнічних атак та параметрів виявленої фішинг-атаки. Метод складається з чотирьох базових етапів: формування формалізованого представлення фішинг-атаки, визначення характеристик профілю соціотехніка, формування узагальненого профілю соціотехніка та його візуалізації. На відміну від існуючих підходів, запропонований метод забезпечує формалізований перехід від параметрів виявленої фішинг-атаки до формування інтегрального профілю її виконавця. За результатами апробації сформовано профіль соціотехніка для досліджуваної фішинг-атаки, визначено його ключові характеристики та побудовано діаграму, що забезпечує графічне представлення отриманого профілю. Отримані результати можуть бути використані для підтримки процесів атрибуції кібератак, кіберрозвідки, реагування на інциденти інформаційної безпеки та розроблення заходів протидії соціотехнічним атакам.

**Ключові слова**: фішинг, профіль соціотехніка, профіль порушника, соціальна інженерія, кіберрозвідка, інформаційна безпека.

## Актуальність

Фішинг залишається одним із найпоширеніших векторів реалізації кіберзагроз, оскільки поєднує технічні механізми компрометації інформаційних систем із методами соціальної інженерії. На відміну від багатьох інших кібератак, фішингові кампанії передбачають

попередню підготовку порушника, яка включає аналіз цільової аудиторії, вибір сценарію впливу та підбір технічних засобів реалізації атаки. Тому виявлена фішинг-атака містить не лише технічні індикатори компрометації, а й інформацію про можливі характеристики її виконавця. Це обумовлює необхідність дослідження підходів, що дозволяють не лише виявляти атаку, а й визначати характеристики її виконавця за результатами аналізу інциденту.

Як зазначається у роботах, присвячених профілюванню кіберзлочинців та атрибуції кібератак, формування профілю порушника є важливим не лише для його ідентифікації, а й для підтримки процесів реагування на інциденти, кіберрозвідки (Cyber Threat Intelligence), прогнозування подальших дій порушника, встановлення зв'язків між окремими атаками та вироблення ефективних заходів протидії [1-3]. Отримані профілі можуть використовуватися центрами моніторингу кібербезпеки (SOC), групами реагування на інциденти (CSIRT/CERT), підрозділами цифрової криміналістики, фахівцями Threat Hunting, а також правоохоронними органами під час атрибуції кібератак і розслідування кіберзлочинів [1-3].

У зв'язку з цим актуальним завданням є розроблення формалізованих методів побудови профілю соціотехніка, наприклад, на основі параметрів виявленої фішинг-атаки, що дозволяють перейти від факту детекції атаки до визначення характеристик її виконавця.

**Проблематика у кіберпросторі**

Сучасні фішингові кампанії характеризуються високим рівнем автоматизації та масштабованості завдяки використанню технологій Fast Flux DNS, динамічної ротації доменів і алгоритмічної генерації URL-адрес. За таких умов традиційні засоби детекції дозволяють встановити факт атаки, проте не забезпечують ідентифікацію порушника та прогнозування його подальших дій, що є важливим для ефективного реагування на інциденти інформаційної безпеки.

Крім того, більшість сучасних підходів зосереджується на виявленні технічних індикаторів компрометації, тоді як інформація про можливий профіль виконавця практично не формується. Це ускладнює атрибуцію атак, оцінювання рівня підготовки та мотивації порушника, визначення його можливих наступних дій, а також виявлення взаємозв'язків між окремими інцидентами. У сучасних дослідженнях підкреслюється, що саме інтеграція технічних ознак атаки з характеристиками потенційного порушника забезпечує більш обґрунтовану атрибуцію, підтримує процес прийняття рішень під час реагування на інциденти та підвищує ефективність діяльності центрів кіберзахисту й кіберрозвідки [1-3].

**Аналіз останніх досліджень і публікацій**

Наявні дослідження можна умовно поділити на дві групи. Перша група охоплює технічні методи виявлення фішингу на основі параметрів URL, DNS та характеристик доменів, що використовують методи машинного навчання й аналізу аномальних станів [4-9]. Такі підходи спрямовані на вирішення задачі детекції та класифікації фішингових атак, однак не забезпечують формалізованого переходу від параметрів виявленої атаки до визначення характеристик її виконавця. Друга – представлена теоретико-множинними моделями класифікації соціотехнічних атак, які описують можливі ознаки та властивості порушників [10-12], проте не встановлюють прямого зв'язку між технічними параметрами конкретної атаки та відповідними характеристиками соціотехніка.

Отже, існує наукова прогалина між задачами технічної детекції фішингових атак та формування профілю їх виконавців. Для її усунення доцільним є розроблення формалізованого механізму побудови профілю соціотехніка на основі параметрів виявленої фішинг-атаки (DA, FC DNS, NSD, UL, SSL/Cert Age, SC, DR, TE, TLD) [5] шляхом розширення існуючого теоретико-множинного підходу [10] множиною ознак профілю порушника.

**Мета дослідження** полягає у розробленні формалізованого підходу до формування узагальненого профілю соціотехніка за результатами аналізу параметрів виявленої фішинг-атаки на інформаційну систему. Для реалізації поставленої мети та формалізації процесу побудови узагальненого профілю соціотехніка пропонується розширити функціональні можливості узагальненого кортежу [13] шляхом інтеграції нового компонента – множини

ознак (Feature Set, FS). Запропонований компонент формується відповідно до теоретико-множинної моделі класифікації сучасних підходів до реалізації соціотехнічних атак [10] та на основі аналізу параметрів виявленої фішинг-атаки на інформаційну систему (DA, FC DNS, NSD, UL, SSL/Cert Age, SC, DR, TE, TLD), визначених у [5].

**Методологія дослідження**

Методологія дослідження базується на поєднанні теоретико-множинного підходу, методу формалізації на основі розширеного узагальненого кортежу, параметричного аналізу виявленої фішинг-атаки та класифікації її характеристик відповідно до моделі сучасних підходів реалізації соціотехнічних атак. Для формування цілісного профілю соціотехніка використано методи систематизації й узагальнення визначених характеристик, а для представлення отриманих результатів – метод графічної візуалізації.

**Основна частина**

Для досягнення поставленої мети пропонується метод, що складається з чотирьох базових етапів. На першому етапі здійснюється формування формалізованого представлення виявленої фішинг-атаки на основі її параметрів. На другому – на основі сформованого формалізованого представлення визначаються характеристики соціотехніка. На третьому – формується узагальнений профіль соціотехніка, який може бути використаний для підтримки процесів атрибуції, реагування на інциденти та кіберрозвідки, а на заключному – здійснюється процес візуалізації профілю соціотехніка.

*Етап 1. Формування формалізованого представлення фішинг-атаки*

Для формування формалізованого представлення виявленої фішинг-атаки використовується розширений узагальнений кортеж, основу якого складають множини параметрів атаки, патернів детекції та ознак профілю соціотехніка. Результатом першого етапу є формалізоване представлення виявленої фішинг-атаки, що використовується для подальшого визначення характеристик соціотехніка.

$$\mathbf{CA_1^{\tau_f}}=<CA_1,\ \mathbf{P_1},\ \mathbf{T_1^e},\ \mathbf{P_1^{\tau_f}},\ \mathbf{DP_1},\ \mathbf{FS_1}> \text{ або}$$

$$\mathbf{CA_{Ph}^{\tau_f}}=<CA_{Ph},\ \mathbf{P_{Ph}},\ \mathbf{T_{Ph}^e},\ \mathbf{P_{Ph}^{\tau_f}},\ \mathbf{DP_{Ph}},\ \mathbf{FS_{Ph}}> \text{, а саме}$$

$$\mathbf{CA_1^{\tau_f}}=<CA_1,\ \{P_{11},\ P_{12},\ldots,\ P_{19}\},$$
$$\{\{\underset{\sim}{T}^e_{111},\underset{\sim}{T}^e_{112},\underset{\sim}{T}^e_{113}\},\ \{\underset{\sim}{T}^e_{121},\underset{\sim}{T}^e_{122},\underset{\sim}{T}^e_{123}\},\ \ldots,\ \{\underset{\sim}{T}^e_{191},\underset{\sim}{T}^e_{192},\underset{\sim}{T}^e_{193}\}\},$$
$$\{\underset{\sim}{\mathrm{P}}^{\tau_f \mathrm{p}}_{11},\ \underset{\sim}{\mathrm{P}}^{\tau_f \mathrm{p}}_{12},\ \ldots,\ \underset{\sim}{\mathrm{P}}^{\tau_f \mathrm{p}}_{19}\},\{\mathbf{DP_{11}},\ \mathbf{DP_{12}},\ldots,\ \mathbf{DP_{19}}\},$$

$$\{SC_{1,2,1};\ SC_{2,1,1}/SC_{2,2,1};\ ,SC_{3,2,1};\ SC_{4,1,1};\ SC_{5,1,1};\ SC_{6,1,1};\ SC_{7,1,1}/SC_{7,2,1};\ SC_{8,2,1};\ SC_{9,2,1};$$
$$SC_{10,2,1}/SC_{10,3,1};\ SC_{11,3,1}/SC_{11,4,1};\ SC_{12,2,2};\ SC_{13,1,1}/SC_{13,6,1};\ SC_{14,1,1}/SC_{14,6,1};\ SC_{15,2,1}\}>,$$

де $\mathbf{CA_{Ph}^{\tau_f}}$ – фішингове атакуюче субдовкілля; $CA_{Ph}$ – ідентифікатор фішинг-атаки; $\mathbf{P_{Ph}}$ – підмножина можливих параметрів, утворюючих $m_i$-вимірне параметричне субдовкілля, що використовується для виявлення фішинг-атаки; $\mathbf{T_{Ph}^e}$ – підмножини можливих нечітких (лінгвістичних) еталонів, утворюючих $m_i$-вимірне еталонне субдовкілля, що відображає характерні судження експерта відносно аномальності стану відповідних параметрів із підмножини $\mathbf{P_{Ph}}$ в $m_i$-вимірному параметричному субдовкіллі; $\mathbf{P_{Ph}^{\tau_f}}$ – підмножина поточних значень нечітких параметрів утворюючих $m_i$-вимірне параметричне субдовкілля, яке формується на основі $\mathbf{T_{Ph}^e}$; $\mathbf{DP_{Ph}}$ – підмножина загальних патернів детекції (Detection patterns - **DP**), утворюючих $i$-е детекційне субдовкілля, що необхідне для виявлення $i$-ї кібератаки (фішинг-атаки); $\mathbf{FS_{Ph}}$ – множина ознак узагальненого профілю соціотехніка, що сформована за п'ятнадцятьма класифікаційними ознаками $\mathbf{S_i}$ ($i = \overline{1,15}$) відповідно до сучасних підходів реалізації соціотехнічних атак (СПРСА) [11]; символ «/» – використовується для позначення одночасного використання двох елементів однієї множини класифікаційних ознак.

Для детального формування компонентів профілю соціотехніка $\mathbf{FS_{Ph}}$ здійснимо послідовний аналіз кожної класифікаційної ознаки $\mathbf{S_i}$ відповідно до параметрів виявленої фішинг-атаки та теоретико-множинної моделі СПРСА [11].

*Етап 2. Визначення характеристик профілю соціотехніка*

На цьому етапі на основі сформованого формалізованого представлення виявленої фішинг-атаки визначаються характеристики соціотехніка, результатом якого є множина характеристик профілю соціотехніка.

Аналіз *часового аспекту* атаки ($\mathbf{S_1} = \mathbf{S}_{\text{ЧА}}$) свідчить про її належність до класу атак попереднього планування (ППЛ-атака, $\mathbf{C_{1,2}} = \text{С}_{\text{ЧА,ППЛ}} = \text{ППЛ}$). Реєстрація домену у короткостроковому діапазоні (1-30 днів, що виявлено у 62 випадках із 80 досліджених записів), налаштування fast-flux DNS з інтенсивністю ротації 6-10 змін (56 випадків із 80 записів), формування складної структури піддоменів (≥4, частота становить 44 випадки із 80 записів) та генерація довгих URL (71-100 символів, що зафіксовано у 52 випадках із 80 записів) у сукупності вказують на завчасно підготовлену технічну інфраструктуру. Спонтанна реалізація атаки такого рівня технічної складності є практично неможливою, що однозначно визначає часовий профіль порушника як такий, що передбачає систематичну підготовчу діяльність.

З точки зору *галузевої афіліації* ($\mathbf{S_2} = \mathbf{S}_{\text{ГА}}$) виявлена атака кваліфікується як спрямована проти корпоративного сектору або громадських установ ($\mathbf{C_{2,1}} = \text{С}_{\text{ГА,КС}} = \text{КС}$ або $\mathbf{C_{2,2}} = \text{С}_{\text{ГА,ГУ}} = \text{ГУ}$). Спрямований характер удару по конкретній інформаційній системі організації, а не по випадкових індивідуальних користувачах, свідчить про свідомий вибір жертви та попереднє вивчення цільової інфраструктури. Це є характерною ознакою атак, орієнтованих на інституційні цілі з метою отримання організаційно значущих даних або несанкціонованого доступу до корпоративних ресурсів.

Щодо *взаємодії з політикою безпеки* ($\mathbf{S_3} = \mathbf{S}_{\text{ПБ}}$), атака реалізована за деполітизаційним методом ($\mathbf{C_{3,2}} = \text{С}_{\text{ПБ,ДП}} = \text{Д}$), тобто порушник цілеспрямовано обходить існуючі захисні механізми організації, а не лише використовує їхні слабкі місця. Імітація легітимного домену через складну ієрархію піддоменів, використання URL-структур, що зовні нагадують довірені ресурси, та відсутність або мінімальний вік SSL-сертифіката (1–30 днів, що зафіксовано у 52 випадках із 80 досліджених записів) свідчать про те, що соціотехнік володіє достатніми знаннями про типові засоби фільтрації та цілеспрямовано конструює атаку таким чином, щоб обійти стандартні засоби захисту.

За механізмом *ініціалізації* ($\mathbf{S_4} = \mathbf{S}_{\text{І}}$) атака належить до класу умовно-активних ($\mathbf{C_{4,1}} = \text{С}_{\text{І,УМ}} = \text{УМ}$, а саме $SC_{4,1,1} = SC_{\text{І,УМ,УА}}$), оскільки активується в момент переходу користувача за підготовленим фішинговим посиланням. Це означає, що соціотехнік свідомо закладає в атаку елемент пасивного очікування. Інфраструктура залишається у стані готовності та активується лише після взаємодії жертви з фішинговим об'єктом, що є ознакою заздалегідь спланованої та технічно зрілої стратегії.

Аналіз *типу звернення* ($\mathbf{S_5} = \mathbf{S}_{\text{ТЗ}}$) дозволяє класифікувати атаку як аверсну ($\mathbf{C_{5,1}} = \text{С}_{\text{ТЗ,АВ}} = \text{АВ}$), тобто таку, що передбачає пряме цілеспрямоване звернення соціотехніка до жертви через розповсюдження фішингових посилань каналами електронної пошти або месенджерів. Відсутність реверсної моделі (коли жертва сама ініціює контакт) підтверджує активну наступальну позицію порушника.

За *інструментарієм реалізації* ($\mathbf{S_6} = \mathbf{S}_{\text{ІН}}$) атака є виключно програмною ($\mathbf{C_{6,1}} = \text{С}_{\text{ІН,ПМ}} = \text{ПМ}$). Автоматизована реєстрація доменів, програмне керування fast-flux DNS-інфраструктурою, алгоритмічна генерація фішингових URL та розгортання підроблених вебсторінок не передбачають використання апаратних або нетипових засобів, що вказує на наявність у соціотехніка спеціалізованого програмного інструментарію або доступу до відповідних сервісів у довкіллі кіберзлочинних угруповань.

З позиції *порушення характеристик безпеки* ($\mathbf{S_7} = \mathbf{S}_{\text{ПХ}}$) атака є одночасно К-дієвою ($\mathbf{C_{7,1}} = \text{С}_{\text{ПХ,К}} = \text{К}$) та Ц-дієвою ($\mathbf{C_{7,2}} = \text{С}_{\text{ПХ,Ц}} = \text{Ц}$). Таким чином, фішинг-атака порушує одночасно дві фундаментальні характеристики безпеки інформації. Основною метою є порушення конфіденційності шляхом викрадення облікових даних, токенів автентифікації або персональних відомостей. Водночас підміна легітимного вебресурсу підробленим порушує цілісність інформаційного довкілля організації, формуючи хибне уявлення про джерело інформації та підриваючи довіру до офіційних каналів комунікації.

Оцінка *ступеня важкості* ($\mathbf{S_8} = \mathbf{S}_{\text{СВ}}$) однозначно відносить виявлену атаку до класу складних ($\mathbf{C_{8,2}} = \text{С}_{\text{СВ,С}} = \text{С}$). Багатошарова технічна реалізація, що поєднує fast-flux DNS, складну структуру піддоменів (NSD ≥ 4, частота становить 44 випадки із 80 досліджених записів)), довгі обфусковані URL (UL в діапазоні 71-100 символів, що зафіксовано у 52 випадках із 80 записів) та маніпуляції з SSL-сертифікатами, свідчить про те, що соціотехнік не є виконавцем простих шаблонних схем, а діє відповідно до технічно вибагливого сценарію, що потребує спеціалізованих знань та відповідної інфраструктури.

За *реляційними ознаками* ($\mathbf{S_9} = \mathbf{S}_{\text{РО}}$) атака кваліфікується як полімономна ($\mathbf{C_{9,2}} = \text{С}_{\text{РО,ПМ}} = \text{ПМ}$). Один порушник або організована група здійснює масований вплив на множину потенційних жертв із використанням масштабованої фішингової інфраструктури. Аналіз вибірки із 80 різних фішингових URL-адрес підтверджує системний характер кампанії та свідчить про застосування автоматизованих засобів генерації й тиражування фішингового контенту.

Аналіз *типу атакованого джерела* ($\mathbf{S_{10}} = \mathbf{S}_{\text{АД}}$) дозволяє ідентифікувати цільову аудиторію як таку, що включає передусім легковажних осіб ($\mathbf{C_{10,2}} = \text{С}_{\text{АД,ЛГ}} = \text{ЛГ}$) та людей-контактерів ($\mathbf{C_{10,3}} = \text{С}_{\text{АД,КН}} = \text{КН}$). Перший тип становлять користувачі, які не схильні перевіряти автентичність URL перед переходом за посиланням. Другий, відповідно персонал організацій, що виконує функції, пов'язані з обробкою зовнішніх запитів і комунікацій, а отже, з підвищеною імовірністю взаємодії з фішинговим контентом.

Щодо *типу доступу* ($\mathbf{S_{11}} = \mathbf{S}_{\text{ТД}}$), атака орієнтована на конфіденційний ($\mathbf{C_{11,3}} = \text{С}_{\text{ТД,КН}} = \text{КН}$) або секретний ($\mathbf{C_{11,4}} = \text{С}_{\text{ТД,СК}} = \text{СК}$) рівень доступу. Це свідчить про те, що соціотехнік усвідомлює цінність цільових облікових даних та цілеспрямовано вибирає жертв із відповідними правами доступу, що є ознакою розвідувальної підготовки, яка передувала атаці.

За *дистанційністю реалізації* ($\mathbf{S_{12}} = \mathbf{S}_{\text{Д}}$) атака класифікується як МТ-віддалена ($\mathbf{C_{12,2}} = \text{С}_{\text{Д,В}} = \text{В}$, а саме $SC_{12,2,2} = SC_{\text{Д,В,МТ}} = \text{МТ}$). Вся інфраструктура функціонує виключно через мережу Інтернет без будь-якої фізичної присутності соціотехніка, що суттєво ускладнює його ідентифікацію та атрибуцію атаки традиційними засобами.

Аналіз *маніпулятивних технік* ($\mathbf{S_{13}} = \mathbf{S}_{\text{МН}}$) виявляє поєднання авторитетності ($\boldsymbol{C}\mathbf{C_{13,1}} = \text{С}_{\text{МН,АВ}} = \text{АВ}$) та обмеженості ($\mathbf{C_{13,6}} = \text{С}_{\text{МН,ОБ}} = \text{ОБ}$). Імітація легітимного домену через складну структуру піддоменів та наявність сертифіката створює ілюзію авторитетного та надійного джерела. Одночасно типові для фішингу повідомлення про терміновість дій (блокування акаунту, закінчення терміну дії тощо) експлуатують психологічний механізм обмеженості часу для прийняття рішення, знижуючи критичність сприйняття жертви.

За *типом виконавця* ($\mathbf{S_{14}} = \mathbf{S}_{\text{ТС}}$) соціотехнік ідентифікується як хакер ($\mathbf{C_{14,1}} = \mathbf{C}_{\text{ТС,ХК}} = \text{ХК}$) або шахрай ($\mathbf{C_{14,6}} = \mathbf{C}_{\text{ТС,ШХ}} = \text{ШХ}$). Технічна складність реалізованої інфраструктури вказує на наявність відповідних технічних компетенцій, характерних для хакерського профілю, тоді як фінансова або інформаційна мотивація, закладена в механізм атаки, корелює з профілем шахрая. Не виключається належність виконавця до організованого кіберзлочинного угруповання, де технічна та соціально-інженерна компетенції поєднуються в рамках розподілу ролей.

За *масштабом* ($\mathbf{S_{15}} = \mathbf{S}_{\text{М}}$) виявлена атака беззаперечно кваліфікується як глобальна ($\mathbf{C_{15,2}} = \text{С}_{\text{М,ГБ}} = \text{ГБ}$). Масове автоматизоване розповсюдження фішингових URL,

використання fast-flux DNS для забезпечення стійкості інфраструктури та відсутність географічної прив'язки атаки свідчать про те, що діяльність соціотехніка виходить за межі локального інциденту та є частиною масштабної кіберзлочинної кампанії.

Результати ідентифікації відповідних класів атак, а також обґрунтування їх вибору на основі параметрів DA, FC DNS, NSD, UL, SSL/Cert Age, SC, DR, TE та TLD узагальнимо у вигляді зведеної таблиці профілю соціотехніка (табл. 1), що дозволяє систематизувати встановлені характеристики порушника та сформувати цілісний профіль його поведінкових і технічних особливостей.

Таблиця 1

Зведена таблиця профілю соціотехніка

| **Ознака ($S_i$)** | **Клас атаки** | **Обґрунтування за параметрами** |
|---|---|---|
| **$S_1$** – часовий аспект | ППЛ-атака | Комплекс ознак, реєстрація «молодого» домену у діапазоні 1-30 днів та швидка ротація *fast-flux DNS* з інтенсивністю 6-10 змін. Заздалегідь розгорнута інфраструктура повністю виключає спонтанність дій порушника |
| **$S_2$** – галузева афіліація | КС/ГУ-атаки | Спрямований характер кіберудару безпосередньо по інформаційній системі конкретної організації (а не по випадкових індивідуальних користувачах). Є класичною ознакою орієнтації на інституційну ціль |
| **$S_3$** – взаємодія з політикою безпеки | ДП-методи | Цілеспрямований обхід стандартних фільтрів та захисних механізмів організації через імітацію довірених ресурсів та мінімальний вік SSL-сертифіката (0-30 днів) |
| **$S_4$** – ініціалізація | УА-атака | Елемент пасивного очікування, інфраструктура перебуває в постійній готовності й активується безпосередньо в момент переходу жертви за фішинговим посиланням |
| **$S_5$** – тип звернення | АВ-методи | Пряме, наступальне та цілеспрямоване звернення соціотехніка до жертви через розповсюдження посилань каналами електронної пошти (розсилка фішингових URL) |
| **$S_6$** – інструментарій | ПМ-методи | Застосування виключно програмно-методологічних засобів автоматизації: скрипти автоматичної реєстрації доменів, керування мережею *fast-flux DNS*, алгоритмічна генерація довгих URL та клонування інтерфейсів вебресурсів. |
| **$S_7$** – порушення характеристик | К/Ц-дієві | Одночасне викрадення облікових даних користувачів для порушення конфіденційності та підміна легітимного вебресурсу підробленим для порушення цілісності довкілля |
| **$S_8$** – ступінь важкості | С-атаки | Висока складність сценарію атаки, зумовлена багатошаровою архітектурою, синхронне використання *fast-flux DNS*, складна ієрархія піддоменів (NSD≥4) та довгі обфусковані URL. |
| **$S_9$** – реляційні ознаки | ПМ-атаки | Один порушник або організована група здійснює масований, системний та масштабований вплив на велику множину жертв із автоматизованим тиражуванням контенту |
| **$S_{10}$** – тип атак, джерела | ЛГ/КН-джерельні | Цільова аудиторія включає легковажних користувачів (не перевіряють URL) та персонал організацій (контактерів), який за обов'язками обробляє потік зовнішніх запитів |
| **$S_{11}$** – тип доступу | КН/СК-доступ | Вектор атаки націлений на заволодіння конфіденційними або секретними обліковими записами, що беззаперечно вказує на проведення порушником попередньої розвідки (OSINT) щодо ієрархії прав усередині організації |
| **$S_{12}$** – дистанційність | МТ-віддалені | Вся інфраструктура функціонує виключно через мережу Інтернет без будь-якої фізичної присутності соціотехніка, що суттєво ускладнює його ідентифікацію та атрибуцію |
| **$S_{13}$** – маніпулювання | АВ/ОБ-маніп. | Створення ілюзії авторитетності джерела (через піддомени та SSL) у поєднанні із психологічним тиском щодо обмеженості часу (терміновості дій) для зниження пильності жертви |
| **$S_{14}$** – тип соціотехніка | ХК/ШХ-виконавчі | Гібридний профіль поєднує високі технічні компетенції хакерського складу дій та фінансово-інформаційну мотивацію класичного кримінального шахрая, що вказує на можливий розподіл ролей у межах злочинного угруповання |
| **$S_{15}$** – масштаб | ГБ-атаки | Діяльність соціотехніка виходить за межі локального інциденту, тобто атака має глобальний характер, позбавлена географічної прив'язки та є частиною великої кіберкампанії |

© Корченко А.О., Аскеров М.Г., Давиденко К.О., Герасименко А.А., Журов Ю.С. Метод формування профілю соціотехніка за виявленою фішинг-атакою на інформаційну систему. Сучасний захист інформації, 3(67), 37–46. https://doi.org/10.31673/2409-7292.2026.032709

*Етап 3. Формування узагальненого профілю соціотехніка*

На цьому етапі окремі характеристики інтегруються у єдиний профіль соціотехніка. Сформований профіль є результатом роботи запропонованого методу та може використовуватися для подальшої підтримки атрибуції кібератак, прогнозування наступних дій порушника та прийняття рішень під час реагування на інциденти інформаційної безпеки.

Таким чином, множина ознак узагальненого профілю соціотехніка $\mathbf{FS_{Ph}}$, де кожна складова відповідає значенню підкритерію $\mathbf{SC_{ijk}}$ або критерію $\mathbf{C_{ij}}$ відповідної ознаки класифікаційної моделі [10] за рівнями $\mathbf{S_i}$ $(i = \overline{1,15})$ має вигляд:

$$\mathbf{FS_{Ph}} = \{SC_{\text{ЧА,ППЛ,ППЛ}};\ SC_{\text{ГА,КС,КС}}/SC_{\text{ГА,ГУ,ГУ}};\ SC_{\text{ПБ,ДП,ДП}};\ SC_{\text{І,УМ,УА}};\ SC_{\text{ТЗ,АВ,АВ}};\ SC_{\text{ІН,ПМ,ПМ}};\ SC_{\text{ПХ,К,К}}/SC_{\text{ПХ,Ц,Ц}};\ SC_{\text{СВ,С,С}};\ SC_{\text{РО,ПМ,ПМ}};\ SC_{\text{АД,ЛГ,ЛГ}}/SC_{\text{АД,КН,КН}};\ SC_{\text{ТД,КН,КН}}/SC_{\text{ТД,СК,СК}};\ SC_{\text{Д,В,МТ}};\ SC_{\text{МН,АВ,АВ}}/SC_{\text{МН,ОБ,ОБ}};\ SC_{\text{ТС,ХК,ХК}}/\ SC_{\text{ТС,ШХ,ШХ}};\ SC_{\text{М,ГБ,ГБ}}\} =$$
$$\{\text{ППЛ; КС/ГУ; ДП; УА; АВ; ПМ; К/Ц; С; ПМ; ЛГ/КН;}$$
$$\text{КН/СК; МТ; АВ/ОБ; ХК/ШХ; ГБ}\},$$

і відповідно на базі цього узагальнений кортеж приймає наступний вигляд:

$$\mathbf{CA_{Ph}^{\tau_f}} = <\text{CA}_{Ph},\ \{P_{PhDA}, P_{PhFC\ DNS}, P_{PhNSD}, P_{PhUL}, P_{PhSSL}, P_{PhSC}, P_{PhDR}, P_{PhTE}, P_{PhTLD}\},$$
$$\{\{\underset{\sim}{T}^{e}_{PhDA}, \underset{\sim}{T}^{e}_{PhDA}, \underset{\sim}{T}^{e}_{PhDA}\}, \{\underset{\sim}{T}^{e}_{PhFC\ DNS}, \underset{\sim}{T}^{e}_{PhFC\ DNS}, \underset{\sim}{T}^{e}_{PhFC\ DNS}\}, \ldots, \{\underset{\sim}{T}^{e}_{PhTLD}, \underset{\sim}{T}^{e}_{PhTLD}, \underset{\sim}{T}^{e}_{PhTLD}\}\},$$
$$\{\underset{\sim}{\mathrm{P}}^{\tau_f \mathrm{p}}_{PhDA}, \underset{\sim}{\mathrm{P}}^{\tau_f \mathrm{p}}_{PhFC\ DNS}, \ldots, \underset{\sim}{\mathrm{P}}^{\tau_f \mathrm{p}}_{PhTLD}\}, \{\mathbf{DP_{PhDA}}, \mathbf{DP_{PhFC\ DNS}}, \ldots, \mathbf{DP_{PhTLD}}\},$$
$$\{\text{ППЛ; КС/ГУ; ДП; УА; АВ; ПМ; К/Ц; С; ПМ; ЛГ/КН;}$$
$$\text{КН/СК; МТ; АВ/ОБ; ХК/ШХ; ГБ}\}>.$$

*Етап 4. Візуалізація профілю соціотехніка*

На цьому етапі здійснюється візуалізація сформованого узагальненого профілю соціотехніка шляхом побудови кругової діаграми. Вхідними даними цього етапу є сформована множина ознак профілю соціотехніка $\mathbf{FS_{Ph}}$, отримана на попередньому етапі.

На початку будується шаблон профілю соціотехніка за групами характеристик (рис. 1), який відображає структуру профілю та взаємозв'язок усіх п'ятнадцяти класифікаційних ознак моделі СПРСА[11]. Вона використовується як шаблон для подальшої візуалізації результатів формування профілю конкретної фішинг-атаки.

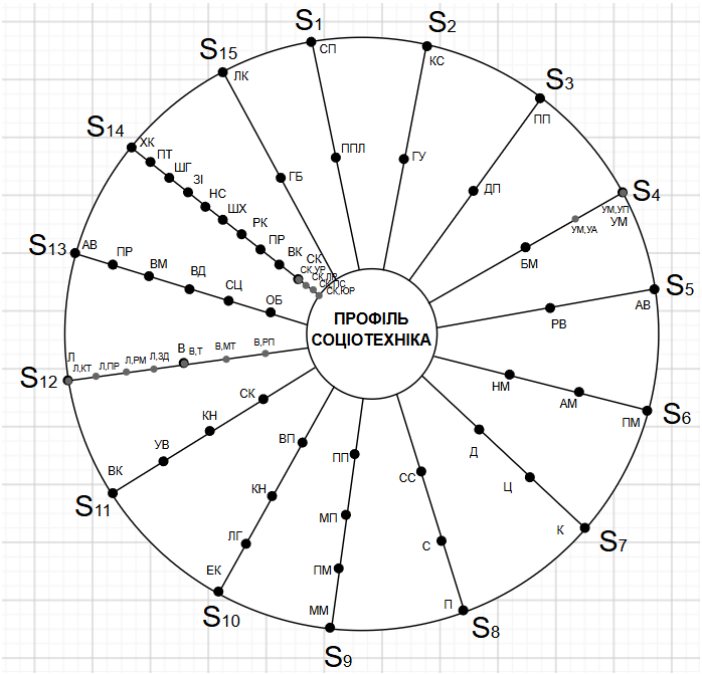


Рис. 1. Шаблон профілю соціотехніка за групами характеристик

Для наочного відображення сформованого набору ознак побудуємо кругову діаграму профілю соціотехніка (рис. 2), у якій кожен сектор відповідає окремій класифікаційній ознаці $\mathbf{S_i}$ та відображає встановлений клас атаки відповідно до моделі [10]. Така візуалізація дозволяє комплексно представити структуру виявленої фішинг-атаки, виокремити ключові характеристики порушника та спростити подальший аналіз його поведінкового й технічного профілю.

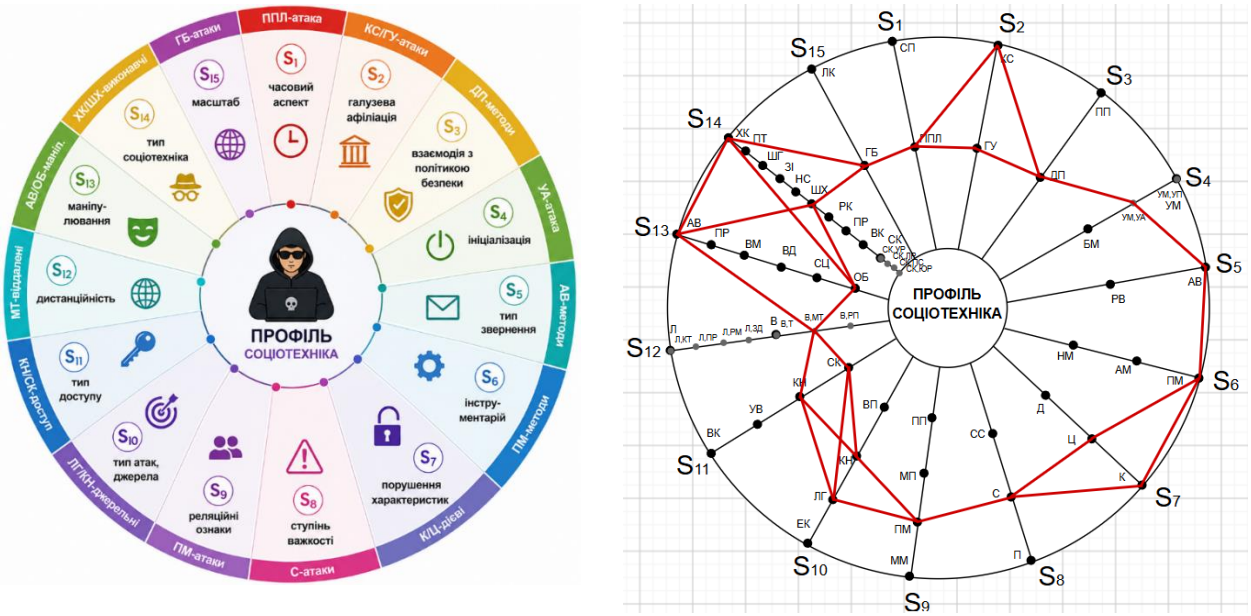


Рис. 2. Профіль соціотехніка за результатами аналізу виявленої фішинг-атаки на інформаційну систему

Побудована діаграма відображає профіль соціотехніка, сформований за результатами аналізу виявленої фішинг-атаки на інформаційну систему. Кожен сектор відповідає одній із п'ятнадцяти класифікаційних ознак $\mathbf{S_i}$, а його наповнення визначається відповідним критерієм $\mathbf{C_{ij}}$ або підкритерієм $\mathbf{SC_{ijk}}$ моделі СПРСА [11]. Отримана візуалізація забезпечує цілісне графічне представлення сформованого профілю соціотехніка та спрощує його подальший аналіз.

**Висновки**

Запропоновано метод формування профілю соціотехніка, який за рахунок етапів: формування формалізованого представлення фішинг-атаки, визначення характеристик профілю соціотехніка, формування узагальненого профілю соціотехніка та його візуалізацію, дозволяє забезпечити формалізований перехід від параметрів виявленої фішинг-атаки до формування інтегрального профілю її виконавця. Отриманий профіль свідчить про те, що виявлена фішинг-атака є результатом діяльності технічно компетентного порушника, який діє дистанційно в рамках заздалегідь спланованої та масштабованої кіберзлочинної кампанії, спрямованої на порушення конфіденційності та цілісності інформаційних ресурсів організації шляхом маніпулятивного впливу на персонал із застосуванням програмних засобів автоматизації. Ключовими диференційними ознаками, що вирізняють цього соціотехніка, є: попереднє планування інфраструктури ($\mathbf{S_1}$), деполітизаційний характер обходу захисту ($\mathbf{S_3}$), умовно-активна ініціалізація через URL-перехід ($\mathbf{S_4}$), поєднане порушення конфіденційності й цілісності ($\mathbf{S_7}$), полімономна масштабованість кампанії ($\mathbf{S_9}$) та комбінований маніпулятивний профіль АВ/ОБ ($\mathbf{S_{13}}$). Сформований профіль може бути використаний як основа для розроблення цільових заходів протидії, налаштування систем виявлення аномалій, підтримки процесів атрибуції кібератак, а також підготовки превентивних заходів щодо підвищення рівня кібербезпеки персоналу організації.

© Корченко А.О., Аскеров М.Г., Давиденко К.О., Герасименко А.А., Журов Ю.С. Метод формування профілю соціотехніка за виявленою фішинг-атакою на інформаційну систему. Сучасний захист інформації, 3(67), 37–46. https://doi.org/10.31673/2409-7292.2026.032709

## Перелік посилань

1.Bada M., Nurse J.R.C. Profiling the Cybercriminal: A Systematic Review of Research // 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). IEEE, 2021. P. 1–8. https://doi.org/10.1109/CyberSA52016.2021.9478246

2.Nguyen V. Attribution of Spear Phishing Attacks: A Literature Survey. Edinburgh, Australia: Defence Science and Technology Organisation (DSTO), Technical Report, 2013. 167 p. URL: https://apps.dtic.mil/ sti/pdfs/ ADA589740.pdf.

3.Rogndokken M.R., Delport P.M.J., van Niekerk J. Facilitating Informed Cyberattack Attributions: The PACT Model // Procedia Computer Science. Vol. 263. 2025. P. 399-409. https://doi.org/10.1016/j.procs.2025.07.049.

4.Корченко А., Іванченко Є., Сатибалдієва Ф., Жумангалієва Н., Давиденко К. Метод формування еталонного субдовкілля для виявлення фішингових URL-адрес // Захист інформації. 2023. № 2. Т. 25. С. 82–95. https://doi.org/10.18372/2410-7840.25.17757.

5.Корченко А. О., Давиденко К. О., Аскеров М. Г., Журов Ю. С. Метод формалізації багатовимірного еталонного субдовкілля для виявлення фішингових URL-адрес // Сучасний захист інформації. 2026. № 2(66). С. 70–87. https://doi.org/10.31673/2409-7292.2026.021105.

6.Корченко А. Методи ідентифікації аномальних станів для систем виявлення вторгнень: монографія. Київ: Компринт, 2019. 361 с.

7.Safi A., Singh S. A Systematic Literature Review on Phishing Website Detection Techniques // Journal of King Saud University – Computer and Information Sciences. 2023. Vol. 35. P. 590-611. https://doi.org/10.1016/ j.jksuci. 2023.01.004.

8.Alkawaz M.H., Steven S.J., Hajamydeen A.I., Ramli R. A Comprehensive Survey on Identification and Analysis of Phishing Website Based on Machine Learning Methods // 2021 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE). 2021. P. 82-87. https://doi.org/10.1109/ISCAIE51753.2021.9431794.

9.Basit A., Zafar M., Liu X., Javed A.R., Jalil Z., Kifayat K. A Comprehensive Survey of AI-Enabled Phishing Attacks Detection Techniques // Telecommunication Systems. 2021. Vol. 76, No. 1. P. 139–154. https://doi.org/10.1007/ s11235-020-00733-2.

10. Korchenko O., Korchenko A., Zybin S., Davydenko K. An Approach for Classifying Socio-Technical Attacks // Radioelectronic and Computer Systems. 2025. № 2. P. 230–252. https://doi.org/10.32620/reks.2025.2.15.

11. Корченко О., Корченко А., Зибін С., Давиденко К. Сучасні підходи реалізації соціотехнічних атак // Information Technology: Computer Science, Software Engineering and Cyber Security. 2025. № 2. С. 48–71. https://doi.org/10.32782/IT/2025-2-6.

12. Корченко А., Давиденко К. Теоретико-множинний підхід до класифікації сучасних методів соціотехнічних атак // ITSec: Безпека інформаційних технологій: матеріали XIV Міжнар. наук.-техн. конф. (Тернопіль, 22–24 травня 2025 р.). Тернопіль–Київ: ЗУНУ–ДУІКТ, 2025. С. 109–111.

13. Корченко А. А. Кортежная модель формирования набора базовых компонент для выявления кибератак // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2014. Вип. 2(28). С. 29-36.

**Anna Korchenko**
Doctor of technical sciences, professor, professor of the department of information security and telecommunications
National Technical University Dnipro Polytechnic, Dnipro, Ukraine
ORCID: 0000-0003-0016-1966
E-mail: annakor@ukr.net

**Mukafat Askerov**
Candidate of Technical Sciences, Professor, Department of Mobile and Video Information Technologies
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0000-6611-2732
E-mail: mukafat_ask@ukr.net

**Kyrylo Davydenko**
PhD student at the Department of Information Security and Telecommunications
National Technical University Dnipro Polytechnic, Dnipro, Ukraine
ORCID: 0009-0001-9209-1274
E-mail: kirilldavy@gmail.com

**Anton Herasymenko**
PhD student of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0008-4475-2040
Email: anton.hrsmnk@gmail.com

© Корченко А.О., Аскеров М.Г., Давиденко К.О., Герасименко А.А., Журов Ю.С. Метод формування профілю соціотехніка за виявленою фішинг-атакою на інформаційну систему. Сучасний захист інформації, 3(67), 37–46. https://doi.org/10.31673/2409-7292.2026.032709

**Iurii Zhurov**
IT specialist
SMB Cybersecurity Advisors, United States of America
ORCID: 0000-0002-8276-2230
E-mail: iurii.zhurov@smbsecurityadvisors.com

# A METHOD FOR FORMING A SOCIAL ENGINEER PROFILE BASED ON A DETECTED PHISHING ATTACK ON AN INFORMATION SYSTEM

Phishing attacks remain one of the most widespread cyber threat vectors, as they combine technical mechanisms for compromising information systems with social engineering techniques. At the same time, existing phishing detection approaches are primarily focused on analyzing the technical parameters of an attack and do not provide a formalized transition from detection results to identifying the characteristics of the attacker, which complicates cyberattack attribution, cyber threat intelligence, and information security incident response. The aim of this study is to develop a method for constructing a social engineer profile based on the analysis of a detected phishing attack on an information system. The proposed method is based on extending a generalized tuple by integrating a set of attacker profile features formed according to the set-theoretic classification model of modern social engineering attack implementation approaches and the parameters of the detected phishing attack. The method consists of four main stages: constructing a formalized representation of the phishing attack, determining the characteristics of the social engineer profile, constructing an integrated social engineer profile, and visualizing the resulting profile. Unlike existing approaches, the proposed method provides a formalized transition from the parameters of a detected phishing attack to the construction of an integrated profile of its perpetrator. The proposed method was validated using a representative phishing attack, resulting in the construction of a social engineer profile, identification of its key characteristics, and generation of a diagram that provides a graphical representation of the resulting profile. The obtained results can be used to support cyberattack attribution, cyber threat intelligence, information security incident response, and the development of countermeasures against social engineering attacks.

**Keywords**: phishing, social engineer profile, attacker profile, social engineering, cyber threat intelligence, information security.

Надійшла до редакції (Received): 10.07.2026
Прийнята до друку (Accepted): 08.09.2026
Опубліковано онлайн (Available online): 15.09.2026



UDC 004.896:620.9:697 DOI: 10.31673/2409-7292.2026.034410

**Andrii Verlan**
Doctor of Technical Sciences, Professor of the Department of IPZE NN IATE
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine,
Norwegian University of Natural Sciences and Engineering, Trondheim, Norway
ORCID: 0000-0002-6469-2638
E-mail: a.verlan@edu.kpi.ua

**Andrii Dyachuk**
Postgraduate student of the Department of IPZE NN IATE
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: 0009-0003-6979-278X
E-mail: diachuk.a.o.-tv51f@edu.kpi.ua

# GENERATIVE NEURAL NETWORK APPROACHES FOR ADAPTIVE BUILDING ENERGY FORECASTING AND CONTROL: A REVIEW OF METHODS AND MICROSERVICES ARCHITECTURES

This article presents a comprehensive review of the transition from static, rule-based Building Management Systems to data-driven artificial intelligence for optimizing energy consumption in the built environment. While discriminative neural networks have advanced energy forecasting, their practical deployment is frequently hindered by

© Корченко А.О., Аскеров М.Г., Давиденко К.О., Герасименко А.А., Журов Ю.С. Метод формування профілю соціотехніка за виявленою фішинг-атакою на інформаційну систему. Сучасний захист інформації, 3(67), 37–46. https://doi.org/10.31673/2409-7292.2026.032709