УДК 004.7

Габорець О.А., д.філ., доцент
Донецький державний університет внутрішніх справ

ФІШИНГ ЯК БАЗОВИЙ ДЕТЕРМІНАНТ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В СИСТЕМІ КІБЕРБЕЗПЕКИ

Стрімкий розвиток цифрових технологій, інтеграція інформаційних систем у всі сфери суспільного життя та глобалізація інформаційного простору зумовили появу якісно нових загроз у сфері кібербезпеки. Однією з таких загроз є соціальна інженерія, яка трансформувалася з допоміжного інструменту кіберзлочинності у самостійний і надзвичайно ефективний механізм інформаційного впливу. Її ключова особливість полягає у спрямованості не на технічні компоненти системи, а на людину як носія інформації та суб'єкта прийняття рішень. У цьому контексті людський фактор виступає найбільш вразливою ланкою системи кібербезпеки, оскільки поведінка користувача часто визначається не раціональним аналізом, а емоційними реакціями та когнітивними спрощеннями [1].

У структурі соціальної інженерії фішинг займає центральне місце, виконуючи роль базового детермінанта, який забезпечує практичну реалізацію більшості соціоінженерних сценаріїв. Фішинг є універсальним інструментом, що дозволяє поєднати технологічні засоби впливу з психологічними механізмами маніпуляції. Його функціонування ґрунтується на створенні штучного інформаційного середовища, у якому користувач сприймає отримане повідомлення як достовірне та безпечне, що спонукає його до виконання дій, вигідних для зловмисника. Важливо підкреслити, що фішинг не обмежується лише електронною поштою, а активно реалізується через соціальні мережі, месенджери, SMS-повідомлення та вебресурси, що значно розширює масштаби його застосування.

З позиції теоретичного аналізу фішинг слід розглядати як багаторівневий феномен, що функціонує на перетині психології, комунікації та інформаційних технологій. На когнітивному рівні він використовує особливості обробки інформації людиною, зокрема схильність до евристичного мислення та автоматизованого прийняття рішень. На комунікативному рівні фішинг реалізується через створення повідомлень, які відповідають очікуванням користувача та відтворюють звичні моделі взаємодії з інформаційними системами. На технологічному рівні він базується на використанні інструментів масового розповсюдження інформації, підміни доменів, клонування вебсайтів та автоматизованих систем генерації контенту.

Особливу увагу слід приділити психологічним механізмам, які забезпечують ефективність фішингових атак. Серед них ключову роль відіграє ефект авторитету, що передбачає використання імен відомих організацій, брендів або державних установ для підвищення рівня довіри до повідомлення. Не менш важливим є ефект дефіциту та терміновості, який змушує користувача діяти швидко, не маючи часу на критичний аналіз інформації. Значну роль відіграє також ефект соціального підтвердження, що базується на припущенні, що якщо певну дію вже виконали інші, вона є правильною. У сукупності ці механізми формують поведінкову модель, у межах якої користувач стає об’єктом маніпуляції, навіть не усвідомлюючи цього.

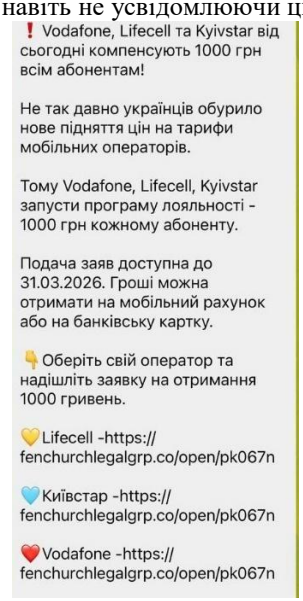

Рис. 1. Приклад фішингового повідомлення з використанням маніпулятивних технік

Зазначені теоретичні положення знаходять своє практичне підтвердження у реальних прикладах фішингових атак. Зокрема, показовим є повідомлення, що поширюється серед користувачів мобільного зв’язку та містить інформацію про нібито компенсацію у розмірі 1000 гривень від провідних мобільних операторів. Даний приклад (*рис. 1*) демонструє класичну модель соціоінженерної атаки, у якій поєднуються різні психологічні тригери. Використання назв відомих операторів створює ефект авторитету, що підвищує довіру до повідомлення. Пропозиція отримання грошової винагороди активує

мотиваційний механізм, пов’язаний із прагненням до вигоди. Зазначення обмеженого строку подання заявки формує відчуття терміновості, що знижує рівень критичного мислення. Додатково використовується механізм персоналізації, оскільки користувачу пропонується обрати свого оператора, що створює ілюзію індивідуального підходу.

Важливим елементом аналізованого повідомлення є наявність гіперпосилань, які ведуть на сторонні вебресурси, що не мають відношення до офіційних сайтів мобільних операторів. Це є характерною ознакою фішингових атак, оскільки основною метою таких посилань є збір персональних даних користувачів або встановлення шкідливого програмного забезпечення. З технічної точки зору, подібні ресурси часто створюються за допомогою конструкторів сайтів або шляхом клонування офіційних сторінок, що дозволяє зловмисникам швидко адаптувати їх до нових сценаріїв атак.

У сучасних умовах розвитку інформаційних технологій фішинг дедалі більше інтегрується з іншими інструментами кіберзлочинності, зокрема OSINT-технологіями та штучним інтелектом. Використання відкритих джерел інформації дозволяє зловмисникам збирати детальні дані про потенційних жертв, що забезпечує високий рівень персоналізації атак. Завдяки цьому фішингові повідомлення стають більш переконливими та складнішими для розпізнавання. Крім того, сучасні алгоритми штучного інтелекту дозволяють автоматизувати процес створення таких повідомлень, адаптуючи їх до індивідуальних характеристик користувача. У наукових дослідженнях цей процес визначається як «алгоритмічне управління довірою», коли поведінка користувача прогнозується і коригується за допомогою цифрових технологій .

У правовому аспекті проблема фішингу ускладнюється відсутністю чіткого нормативного визначення соціальної інженерії в законодавстві, що створює труднощі у кваліфікації відповідних правопорушень. Водночас фішингові атаки часто підпадають під ознаки шахрайства, незаконного втручання в роботу інформаційних систем або порушення правил захисту інформації. Це свідчить про необхідність удосконалення нормативно-правової бази у сфері кібербезпеки та розробки спеціалізованих механізмів протидії соціоінженерним загрозам.

У системі кібербезпеки фішинг виконує функцію первинного вектора доступу до інформаційних ресурсів, що робить його особливо небезпечним. Навіть за наявності сучасних технічних засобів захисту, таких як системи виявлення вторгнень або багатофакторна

автентифікація, людський фактор залишається критичним елементом, який може нівелювати ефективність цих заходів. Саме тому протидія фішинговим атакам повинна базуватися на комплексному підході, що поєднує технічні, організаційні та освітні заходи. Як підкреслюється у наукових джерелах, важливу роль відіграє формування культури інформаційної безпеки, розвиток критичного мислення та підвищення рівня обізнаності користувачів щодо сучасних кіберзагроз .

У контексті гібридних загроз фішинг набуває додаткового значення як інструмент інформаційно-психологічного впливу. Його використання може бути спрямоване не лише на отримання конфіденційної інформації, але й на дестабілізацію суспільства, поширення дезінформації та формування панічних настроїв. Таким чином, фішинг виходить за межі суто кримінального явища та стає елементом ширших інформаційних операцій.

Отже, фішинг є базовим детермінантом соціальної інженерії, який визначає характер сучасних кіберзагроз і виступає універсальним інструментом маніпуляції поведінкою користувачів у цифровому середовищі. Його ефективність обумовлена поєднанням технологічних можливостей і глибокого розуміння психологічних особливостей людини. Подальші дослідження у цій сфері повинні бути спрямовані на розробку інноваційних методів виявлення фішингових атак, удосконалення освітніх програм з кібербезпеки та формування стійкості користувачів до маніпулятивних впливів.

Список використаних джерел

1. Габорець О. А., Лунгол О. М. Соціальна інженерія як феномен інформаційного впливу в цифровому середовищі. Національні інтереси України. 2025. № 11(16). С. 95-104. DOI: https://doi.org/10.52058/3041-1793-11(16)