КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1108
УДК 004.056:004.738.5

Габорець Ольга Андріївна
доктор філософії, доцент, доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки
Донецький державний університет внутрішніх справ, Кропивницький, Україна
ORCID: 0000-0001-7791-6795
olga-gaborets@ukr.net

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

Анотація. У статті розглянуто соціальну інженерію як один із найбільш результативних інструментів маніпулятивного впливу на користувачів у цифровому середовищі в умовах збройного конфлікту. Акцентовано, що в період війни соціальна інженерія набуває особливої небезпечності, оскільки поєднує психологічний тиск із технологічними каналами поширення інформації, що ускладнює критичне сприйняття повідомлень та підвищує ймовірність імпульсивної поведінки. Обґрунтовано, що головна ціль соціально-інженерних впливів у кризових умовах полягає не лише у введенні користувача в оману, а й у формуванні керованих поведінкових реакцій: паніки, швидкого поширення неперевірених повідомлень, зниження довіри до офіційних каналів комунікації, а також дезорганізації інформаційного простору.

Проаналізовано типові зразки маніпулятивних повідомлень у месенджерах, які імітують екстрені попередження про загрозу та містять заклики до негайних дій (наприклад, «терміново», «тривога», «відкрити карту цілей/загроз»). Показано, що ефективність таких повідомлень забезпечується використанням стійких психологічних тригерів, зокрема ефекту терміновості, апеляції до страху, інформаційної невизначеності та когнітивного перевантаження. Доведено, що поєднання псевдоофіційної стилістики з візуальними маркерами «легітимності» (символи небезпеки, короткі наказові формулювання, емоційно насичені заголовки) створює у користувача враження достовірності та сприяє автоматизованій реакції без належної перевірки джерела.

Окремо визначено індикатори, за якими можна ідентифікувати соціально-інженерний характер повідомлень: нав’язування невідкладності, локалізація загрози для конкретної території або групи населення, прямі поведінкові інструкції («перейти», «натиснути», «відкрити»), а також використання показників охоплення чи реакцій як засобу соціального підтвердження. Практичне значення дослідження полягає у формуванні базових превентивних рекомендацій щодо протидії соціальній інженерії: верифікація повідомлень через офіційні джерела, дотримання принципів цифрової гігієни, обмеження переходів за сумнівними посиланнями, розвиток медіаграмотності та стійкості до емоційного впливу. Зроблено висновок, що системна протидія соціальній інженерії під час війни потребує поєднання технічних, інформаційних і освітніх заходів, спрямованих на збереження інформаційної стабільності та безпечної поведінки користувачів у кіберпросторі.

Ключові слова: соціальна інженерія; кібербезпека; інформаційно-психологічний вплив; маніпулятивні повідомлення; фішинг; дезінформація; цифрова гігієна; медіаграмотність.

ВСТУП

Постановка проблеми. В умовах збройного конфлікту цифровий інформаційний простір набуває критичного значення як для оперативного інформування населення, так і для забезпечення національної стійкості. Водночас інтенсифікація комунікацій у соціальних мережах і месенджерах супроводжується зростанням кількості маніпулятивних повідомлень, спрямованих на дестабілізацію суспільних настроїв та порушення інформаційної безпеки. Однією з найбільш ефективних загроз у цьому

контексті є соціальна інженерія, що ґрунтується на використанні психологічних механізмів впливу (страху, терміновості, невизначеності, авторитету) з метою формування керованих поведінкових реакцій користувачів – від імпульсивного поширення фейкових повідомлень до переходу за потенційно небезпечними посиланнями. Проблема полягає в тому, що соціально-інженерні атаки під час війни часто маскуються під «екстрені оповіщення», апелюють до загроз життю та безпеці й активізують автоматичні реакції людини, що суттєво знижує рівень критичного мислення. За таких умов виникає необхідність наукового обґрунтування характерних ознак соціальної інженерії в кризовому інформаційному середовищі, визначення індикаторів маніпулятивних повідомлень і формування практичних рекомендацій щодо їх своєчасної ідентифікації та попередження негативних наслідків для суспільства й кібербезпеки.

Аналіз останніх досліджень і публікацій. Проблематика соціальної інженерії як інструмента інформаційного впливу в цифровому середовищі активно досліджується в межах сучасних наукових праць з кібербезпеки, інформаційно-психологічної протидії та аналізу гібридних загроз. У вітчизняних дослідженнях соціальна інженерія розглядається не лише як сукупність технік обману користувачів, а як системний феномен інформаційного впливу, що здатний формувати поведінкові установки та модифікувати сприйняття реальності в цифровому середовищі [1]. Автори акцентують увагу на тому, що соціальна інженерія ґрунтується на експлуатації психологічних механізмів довіри, страху та авторитету, що робить її особливо небезпечною в умовах кризових ситуацій.

Значний масив наукових робіт присвячений аналізу соціальної інженерії як загрози кібербезпеці. У дослідженнях наголошується, що соціально-інженерні атаки дозволяють обходити технічні засоби захисту шляхом маніпуляції людським фактором, а фішинг залишається однією з найпоширеніших форм таких атак [2], [4]. Запропоновані в роботах класифікації та таксономії фішингових методів [4], а також структурні підходи до виявлення соціально-інженерних атак [5] і прогнозування фішингової активності з використанням статистичних методів [7] формують теоретико-прикладну основу для протидії таким загрозам.

Окремий напрям досліджень зосереджений на вдосконаленні методів захисту персональних даних та інформаційних систем від атак соціальної інженерії. У наукових працях пропонуються алгоритмічні та організаційні підходи до зниження вразливості користувачів і систем шляхом комбінування технічних засобів захисту з освітніми та превентивними заходами [6]. Водночас підкреслюється, що ефективність таких методів значною мірою залежить від здатності користувачів розпізнавати маніпулятивні повідомлення в реальному інформаційному потоці.

У зарубіжних дослідженнях соціальна інженерія та фішинг розглядаються в ширшому контексті інформаційно-психологічних операцій і когнітивного впливу. Зокрема, у роботах, присвячених аналізу психологічних операцій у сучасних конфліктах, доведено, що некінетичні впливи, реалізовані через цифрові комунікації, можуть мати стратегічні наслідки для безпеки держав і суспільств [3]. Такі підходи узгоджуються з сучасними уявленнями про гібридну війну, у межах якої інформаційні та психологічні інструменти застосовуються системно та цілеспрямовано.

Важливе місце в науковому дискурсі займають дослідження, присвячені виявленню дезінформації, фейків і пропаганди в медіапросторі з використанням методів машинного навчання та штучного інтелекту [8], [9]. У цих роботах обґрунтовується ефективність автоматизованих підходів до аналізу контенту та поведінкових патернів

користувачів, що відкриває нові можливості для протидії інформаційним загрозам у цифровому середовищі. Також розглядаються підходи до моделювання фішингових сценаріїв як інструмента аналітичного прогнозування кіберзагроз [10].

Разом із тим, попри значну кількість наукових напрацювань, недостатньо дослідженими залишаються прикладні аспекти соціальної інженерії саме в умовах збройного конфлікту, зокрема її функціонування як інструмента інформаційно-психологічних операцій, спрямованих на масову аудиторію. У наявних дослідженнях обмежено висвітлено питання ідентифікації маніпулятивних повідомлень у месенджерах і соціальних мережах, що стилізуються під екстрені оповіщення та містять прямі поведінкові інструкції. Недостатньо систематизованими залишаються й індикатори таких повідомлень, які поєднують текстові, візуальні та психологічні елементи впливу. Саме заповнення цих прогалин і становить наукову новизну та предмет дослідження в даній статті.

Метою статті є аналіз соціальної інженерії в умовах збройного конфлікту, визначення характерних індикаторів маніпулятивних повідомлень у цифрових каналах комунікації та обґрунтування практичних рекомендацій щодо підвищення стійкості користувачів до інформаційно-психологічних впливів і мінімізації кіберризиків.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Соціальна інженерія набуває особливої актуальності в умовах збройного конфлікту, коли виходить за межі поодиноких випадків обману та перетворюється на інструмент системного впливу в межах інформаційно-психологічних операцій. У російсько-українській війні такі операції мають комплексний і багаторівневий характер та реалізуються як заздалегідь сплановані технологічні дії, спрямовані на підрив психологічної стійкості суспільства, деморалізацію військовослужбовців, зниження довіри до державних інституцій і дестабілізацію інформаційного середовища. Унаслідок цього формується стан інформаційної турбулентності, за якого ускладнюється критичне осмислення повідомлень і зростає ймовірність ірраціональних реакцій. У такому контексті соціальна інженерія функціонує не лише як спосіб впливу на окремого користувача, а й як механізм керування масовою поведінкою, у межах якого кожне повідомлення може розглядатися як елемент ширшої стратегії гібридної війни, орієнтованої на конструювання вигідної противнику інформаційної реальності.

Інформаційно-психологічні операції (ІПСО) в умовах збройного конфлікту становлять системний і цілеспрямований комплекс заходів, спрямованих на вплив на свідомість, емоційний стан і поведінкові установки цільової аудиторії з метою досягнення стратегічних, оперативних або тактичних переваг. На відміну від спонтанного поширення дезінформації чи ізольованих актів пропаганди, ІПСО мають чітку архітектуру, етапність реалізації та інтегруються в загальну модель гібридної війни як самостійний інструмент впливу. У цьому контексті соціальна інженерія виступає не допоміжним елементом, а базовим механізмом реалізації ІПСО, оскільки саме вона забезпечує проникнення інформаційних впливів у когнітивну та емоційну сферу людини.

В умовах війни ІПСО спрямовані передусім на порушення психологічної рівноваги суспільства, дестабілізацію процесів ухвалення рішень і зниження рівня довіри до офіційних джерел інформації. Противник цілеспрямовано формує інформаційне середовище, у якому домінують тривога, невизначеність і відчуття втрати контролю, що істотно підвищує сприйнятливість населення до маніпулятивних повідомлень. За таких

умов людина починає шукати швидкі та емоційно заспокійливі відповіді, часто нехтуючи перевіркою джерел та логічним аналізом інформації. Саме ця когнітивна вразливість і становить ключову мішень ІПСО.

Соціальна інженерія в межах ІПСО ґрунтується на прогнозуванні типових поведінкових реакцій у кризових ситуаціях. Ворожі інформаційні центри заздалегідь моделюють сценарії поведінки цільових груп, використовуючи дані з відкритих джерел, соціальних мереж, коментарів, пошукових запитів і цифрових слідів користувачів. Такий підхід дозволяє ідентифікувати найбільш уразливі сегменти аудиторії та адаптувати маніпулятивні повідомлення під їхній емоційний стан, соціальний контекст і рівень інформаційної компетентності. У результаті ІПСО набувають персоналізованого характеру, коли один і той самий наратив може подаватися у різних формах залежно від адресата, що значно підвищує ефективність впливу.

Ключовою особливістю сучасних ІПСО є активне використання цифрових платформ як середовища реалізації соціально-інженерних сценаріїв. Месенджери, соціальні мережі та онлайн-спільноти стають не лише каналами поширення інформації, а й простором формування поведінкових патернів. Маніпулятивні повідомлення часто маскуються під офіційні звернення, екстрені попередження, аналітичні матеріали або «інсайдерську» інформацію, що створює ілюзію достовірності. Використання елементів візуальної легітимності – державної символіки, стилізованих інтерфейсів, псевдодокументів – істотно знижує критичність сприйняття й активує евристики довіри та авторитету.

Особливу небезпеку становлять ІПСО, спрямовані на створення інформаційного хаосу шляхом поєднання правдивих і хибних даних. У таких умовах користувачі втрачають здатність відрізняти автентичні повідомлення від фейкових, що призводить до когнітивного перевантаження та зростання тривожності. Це, своєю чергою, сприяє поширенню панічних настроїв, зниженню рівня довіри до офіційних каналів комунікації та формуванню альтернативних, часто деструктивних, інформаційних спільнот. Таким чином, ІПСО не лише впливають на індивідуальну поведінку, а й трансформують інформаційну екосистему загалом.

Важливою складовою ІПСО є їхня розвідувальна функція. Соціально-інженерні впливи використовуються не лише для маніпуляції, а й для збору даних про реакції населення, рівень тривожності, ступінь довіри до різних джерел і ефективність окремих наративів. Перехід користувачів за шкідливими посиланнями, активність у коментарях, швидкість поширення повідомлень і географія цифрової взаємодії дозволяють противнику в реальному часі коригувати свої інформаційні кампанії. У цьому сенсі ІПСО функціонують як замкнута система, у якій соціальна інженерія одночасно виконує роль інструменту впливу та механізму зворотного зв’язку.

Застосування штучного інтелекту значно підсилює потенціал ІПСО, оскільки дає змогу автоматизувати створення маніпулятивного контенту та підвищувати його адаптивність. Генерація персоналізованих повідомлень, імітація стилю офіційних комунікацій, створення синтетичних зображень і відео формують нову якість інформаційного впливу, у якій межа між реальним і штучно сконструйованим стає дедалі менш помітною. За таких умов соціальна інженерія трансформується з тактики обману в інструмент когнітивного управління, здатний системно змінювати поведінкові установки великих соціальних груп.

Противник активно застосовує фейки, маніпулятивні повідомлення, deepfake-відео, стилізації під офіційні документи, псевдоаналітичні «інсайди» та емоційно забарвлені наративи, що виконують не лише інформативну, а передусім емоційну функцію. Вони

розраховані на те, щоб змусити людину діяти автоматично й імпульсивно, під впливом страху, а не раціонального аналізу. Наявність у повідомленні навіть мінімальних атрибутів авторитетності – використання державної символіки, візуальних шаблонів офіційних каналів, стилізації під систему ППО або інтерфейс спецслужб – знижує здатність користувача до критичного сприйняття. Ефективність таких операцій підсилюється загальним психологічним станом суспільства під час війни: підвищеним рівнем стресу, дефіцитом достовірної інформації, тривалою емоційною напругою, браком часу для перевірки повідомлень і надмірною кількістю інформаційного шуму. У результаті цифрове середовище перетворюється на арену бойових дій, де мішенню стає не лише інфраструктура, а й свідомість користувачів, а інформаційний простір – на самодостатній театр воєнних операцій.

Особливо показовими в контексті інформаційно-психологічних операцій є маніпулятивні повідомлення, що поширюються через соціальні мережі та месенджери у формі псевдоновин про нібито масштабні руйнування, пожежі або масові жертви внаслідок ракетних атак. Такі повідомлення, як правило, супроводжуються емоційно насиченими візуальними матеріалами – темними відеофрагментами вибухів, кадрами вогню в нічний час, тривожними емодзі, а також категоричними формулюваннями, що не допускають сумніву або перевірки інформації. Їхня мета полягає не стільки в інформуванні, скільки у викликанні шокової реакції, різкого зростання тривожності та імпульсивного поширення повідомлення серед користувачів.

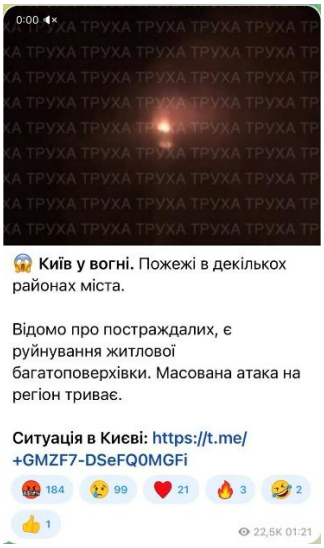

Рис. 1. Маніпулятивне повідомлення в соціальній мережі, спрямоване на створення паніки та емоційної дестабілізації населення в межах інформаційно-психологічної операції

На Рис. 1. представлено приклад подібного соціально-інженерного вкиду, стилізованого під «термінове повідомлення» про нібито пожежі та руйнування в кількох районах Києва. Візуальний ряд обмежується затемненим відео з джерелом світла, яке неможливо однозначно ідентифікувати, що унеможливлює перевірку локації, часу та контексту події. Водночас текст повідомлення побудований із використанням класичних маніпулятивних маркерів: узагальнених тверджень («Київ у вогні», «масована атака триває»), апеляції до страху за життя цивільного населення, натяків на постраждалих без конкретизації та посилання на сторонній Telegram-канал як нібито джерело уточненої інформації. Така конструкція формує у реципієнта відчуття невідкладної загрози й

стимулює негайний перехід за посиланням або поширення повідомлення без критичної оцінки його достовірності.

Психологічний механізм впливу в цьому випадку базується на поєднанні ефекту терміновості, евристики страху та феномену соціального зараження. Кількість емоційних реакцій під повідомленням (злість, плач, страх) створює ілюзію колективного підтвердження правдивості інформації, що додатково знижує рівень критичного мислення. В умовах реальної воєнної загрози такі вкиди є особливо небезпечними, оскільки вони можуть накладатися на справжні повітряні тривоги, дезорієнтувати населення, підривати довіру до офіційних каналів оповіщення та провокувати панічні або хаотичні поведінкові реакції.

Таким чином, наведений приклад ілюструє, як соціальна інженерія в межах ІПСО використовує візуальні й текстові тригери для цілеспрямованого впливу на емоційний стан населення, трансформуючи цифровий інформаційний простір на інструмент психологічного тиску. Інформаційно-психологічні операції мають диференційований характер впливу, оскільки їхня ефективність значною мірою залежить від соціального статусу, життєвого досвіду та психологічного стану цільової аудиторії. Для цивільного населення ІПСО переважно спрямовані на формування станів хронічної тривожності, дезорієнтації та втрати відчуття безпеки шляхом поширення панічних наративів і суперечливої інформації. Родини військовослужбовців є особливо вразливою групою, оскільки маніпулятивні повідомлення апелюють до страху за життя близьких, використовуючи персоналізовані дані та створюючи ситуації емоційного шоку й невизначеності. Волонтери часто стають мішенню ІПСО через експлуатацію їхньої високої мотивації та почуття відповідальності, що проявляється у фейкових запитах про допомогу, фінансових зборах або логістичних «термінових» зверненнях. Внутрішньо переміщені особи зазнають посиленого інформаційного тиску через поєднання соціальної нестабільності, втрати звичних соціальних зв'язків і дефіциту перевіреної інформації, що підвищує їхню сприйнятливість до маніпуляцій. Особи з досвідом психологічної травми демонструють знижену стійкість до ІПСО, оскільки повторні тригери страху, втрати або небезпеки можуть активувати травматичні реакції та знижувати здатність до критичного аналізу інформації. Одним із найбільш технологічно витончених прикладів такого диференційованого впливу є використання фейкових цифрових інтерфейсів, які створюють ілюзію контролю над загрозою. Подібні матеріали слугують не лише засобом поширення дезінформації, а й елементом поведінкового управління, спрямованого на послаблення психологічної стійкості суспільства в умовах збройного конфлікту.

Показовим прикладом реалізації соціально-інженерних механізмів у межах інформаційно-психологічних операцій є цілеспрямоване поширення фейкових так званих «радарів» ракет і безпілотних літальних апаратів (Рис. 2), візуально стилізованих під інтерфейси військових систем спостереження та протиповітряної оборони. Такі інформаційні вкиди формують у користувачів ілюзію доступу до закритих або службових даних, що підкріплюється використанням графічних елементів, які підсвідомо асоціюються з офіційними та технологічно надійними джерелами інформації. Текстовий супровід подібних повідомлень зазвичай містить драматизовані формулювання на кшталт «під загрозою кілька міст» або «масштабна атака триває», а також посилання, які нібито дають змогу «підключитися до радара» чи «відстежувати рух ракет і БпЛА в реальному часі». Візуально такі матеріали відтворюють характерні атрибути технічних систем – радіальні зони сканування, маркери загроз, контури території України, сигнальні червоні індикатори небезпеки. Поєднання візуальної

псевдотехнічності з емоційно насиченим наративом суттєво підсилює переконливість повідомлення, знижує рівень критичного мислення та провокує імпульсивні поведінкові реакції, що відповідає типовим цілям і очікуваним результатам інформаційно-психологічних операцій.

Рис. 2. Фейковий «радар загроз», створений для поширення паніки та маніпуляції користувачами

Подібні повідомлення належать до категорії когнітивних атак, оскільки використовують глибинні психологічні механізми: ефект терміновості, страх перед ракетними загрозами, довіру до технологічних інтерфейсів, евристику наближення небезпеки, стан емоційного виснаження, неусвідомлене прагнення отримати контроль над ситуацією та феномен соціального зараження – швидке поширення емоційних реакцій у групі. Водночас такі «радари» нерідко слугують і технічним інструментом розвідки: переходячи за посиланням, користувач може не лише розкрити власні персональні дані чи надати доступ до геолокації, а й стати частиною аналітичної бази, яку противник використовує для картографування поведінкових реакцій населення в реальному часі. Саме тут важливу роль відіграють методи OSINT, які ворог застосовує для агрегування, класифікації та аналізу даних, зібраних як з відкритих джерел, так і з цифрової активності самих користувачів. Соціальна інженерія та OSINT у воєнних умовах дедалі частіше працюють синхронно: перша – провокує реакції, друга – фіксує й аналізує їх, формуючи розвідувальну аналітику для наступних фаз операцій.

Важливу роль у документуванні таких операцій відіграє CERT-UA, яка фіксує зростання кількості та складності соціально-інженерних атак, що поширюються через багаторівневі Telegram-мережі, автоматизовані ботоферми та координаційні панелі. CERT-UA встановлює, що більшість інформаційних вкидів функціонує за єдиним алгоритмом: первинний запуск фейку в контрольованих каналах, його синхронізоване розмноження ботами, формування штучного інформаційного резонансу, стимулювання користувачів до переходу за шкідливими посиланнями та подальший збір цифрових слідів. Такий аналіз підтверджує системність і високий рівень організації ворожих ІПСО, які поєднують психологічний, технічний і розвідувальний впливи в єдину операційну модель.

Схожим механізмом характеризуються й фейкові екстрені звернення в месенджерах із закликами «підключити мапу загроз протягом 15 хвилин» або «терміново перейти за посиланням». Вони апелюють до інстинкту виживання та використовують

маніпулятивно сформульовані фрази, що створюють відчуття невідкладної небезпеки. Особливо небезпечним є те, що подібні повідомлення можуть надходити в періоди реальних ракетних атак, змішуючи достовірні попередження з фейковими та підриваючи здатність населення орієнтуватися в інформаційному просторі. В умовах перевантаження тривожними стимулами користувачі легко втрачають здатність розрізняти автентичні джерела інформації, що є однією з ключових цілей інформаційно-психологічних операцій.

Соціальна інженерія у воєнний час проявляється також через інші типи повідомлень: фейкові запити про персональні дані «для виплат», підроблені повідомлення про загибель чи поранення військовослужбовців, псевдодокументи від командування з вимогами передати конфіденційну інформацію, повідомлення про «масову евакуацію», «оточення», «здачу позицій» тощо. Кожен із цих інструментів має спільну психологічну основу – створення емоційного шоку, який перехоплює контроль над увагою людини й змушує її діяти без аналізу.

Ще одним небезпечним різновидом соціально-інженерних атак є поширення повідомлень про нібито «зниклих безвісти військовослужбовців». Особливу загрозу становить те, що подібні оголошення ґрунтуються не на вигаданих даних, а на реальній інформації, яку самі родичі, знайомі або офіційні структури могли раніше опублікувати у відкритому доступі. Зловмисники цілеспрямовано моніторять соціальні мережі, локальні групи й навіть регіональні медіа, збираючи фрагменти правдивих біографічних відомостей, фотографій, дат народження, інформації про службу, що надає фейкам високого рівня правдоподібності. Використання реальних даних створює відчуття автентичності та послаблює критичне сприйняття аудиторії, адже більшість людей схильні довіряти повідомленням, які містять знайомі або фактичні елементи.

Водночас зловмисники часто не мають жодної достовірної інформації про фактичне місцеперебування військовослужбовця, однак це не заважає їм використовувати зібрані дані для побудови маніпулятивних сценаріїв. Вони можуть повідомляти, що «військовий перебуває у лікарні, але зв’язатися з ним неможливо», «потрапив у полон, але інформація потребує підтвердження» або «є можливість уточнити місце перебування, але лише після оплати». Такі повідомлення навмисно апелюють до тривоги, відчаю та природного бажання родичів діяти негайно, що суттєво підвищує їхню вразливість до обману.

Найбільшу небезпеку становить те, що самі родичі, перебуваючи у стресі, нерідко починають активно комунікувати зі зловмисниками, несвідомо розкриваючи додаткові відомості: номери телефонів, скріншоти листування, інформацію про підрозділ, останні контакти, місце перебування, прізвища побратимів, деталі операцій. У такий спосіб соціальна інженерія переходить від загального фейку до персоналізованої атаки: що більше даних надає родина, то більш переконливими стають подальші маніпуляції. Це відповідає моделі OSINT-експлуатації, за якої початковий фрагмент правдивої інформації стає ключем до формування цілісного профілю людини, її зв’язків й обставин служби.

Подібні повідомлення виконують одночасно кілька функцій у структурі ІПСО. По-перше, вони спрямовані на психологічний тиск на родину військовослужбовця, створення стану невизначеності та тривоги, що негативно впливає на морально-психологічний стан як родини, так і самого військового, якщо інформація доходить до нього. По-друге, вони виконують розвідувальну функцію: зібрані під час комунікації дані можуть використовуватися для картографування місць дислокації, виявлення складу підрозділів або навіть планування подальших комбінованих атак. По-третє, вони

мають фінансовий мотив, що проявляється у вимаганні коштів за «інформацію» про долю військовослужбовця – одну з найцинічніших форм воєнного шахрайства, що спирається на максимальне емоційне виснаження родини.

Використання реальних фотографій і біографічних даних (як у випадку з поширенням інформації про зниклого бійця) формує небезпечний ефект довіри, коли навіть користувачі з високим рівнем критичності сприймають повідомлення як правдиве через наявність автентичних елементів. Це відрізняє такі атаки від традиційних фейків і робить їх значно ефективнішими, оскільки вони поєднують правду, емоцію та маніпуляцію – три складові, що забезпечують максимальний психологічний вплив.

Широке використання OSINT у зв'язці із соціальною інженерією суттєво посилює ефективність таких атак. Відкриті джерела дають змогу визначати соціальні кола, ідентифікувати службових осіб, відстежувати динаміку настроїв у регіонах, структурувати інформацію про переміщення населення, волонтерських груп і підрозділів, а також виявляти потенційні точки соціальної напруги. Аналізуючи інформацію з публічних профілів, коментарів, фотографій, геоміток, обговорень у місцевих чатах і навіть характер поширення дописів, противник отримує змогу реконструювати соціальну карту спільнот та визначати, де саме його інформаційна атака може бути найбільш результативною. Окрему цінність становлять цифрові сліди, які користувачі залишають, переходячи за посиланнями фейкових повідомлень: частота взаємодії, тривалість перегляду, географічний розподіл активності та типові маршрути поведінки в мережі. Це дає змогу ворогу не лише збирати дані, а й тестувати, які наративи працюють найефективніше для різних цільових груп, які формати спричиняють найбільше емоційне збурення та які повідомлення мають максимальний потенціал до вірусного поширення. У цьому сенсі соціальна інженерія стає не лише засобом впливу, а й потужним інструментом аналітики, що забезпечує замкнений цикл корекції інформаційних операцій і підвищує адаптивність ІПСО, роблячи їх дедалі точнішими, персоналізованішими й ефективнішими.

Ситуацію ускладнює широке застосування штучного інтелекту, який дає змогу автоматизувати продукування фейків, підвищувати їхню якість та адаптивність. Алгоритми можуть створювати персоналізовані повідомлення на основі відкритих даних про користувачів, імітувати стиль комунікації державних органів або навіть синтезувати голоси відомих осіб. Це означає, що сучасні соціально-інженерні атаки дедалі рідше виглядають як грубий обман, а дедалі частіше – як професійно спроєктовані комунікативні конструкції.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У ході дослідження встановлено, що соціальна інженерія в умовах збройного конфлікту перетворюється на один із найбільш результативних інструментів деструктивного впливу в цифровому інформаційному середовищі. На відміну від класичних моделей шахрайства, її ключова небезпека полягає у здатності швидко формувати керовані поведінкові реакції масової аудиторії через експлуатацію психологічних тригерів страху, терміновості та невизначеності. Унаслідок цього знижується критичність сприйняття інформації, посилюється схильність до імпульсивних дій та зростають ризики дестабілізації суспільних комунікацій.

На основі аналізу прикладів маніпулятивних повідомлень у цифрових каналах комунікації визначено характерні індикатори соціально-інженерних впливів: імітація екстрених попереджень («тривога», «терміново»), локалізація загрози для конкретної

території, псевдоофіційна стилістика й візуальні маркери «достовірності», а також прямі поведінкові інструкції («відкрити», «перейти», «підключити»). Обґрунтовано, що окрему групу ризиків становлять повідомлення з елементами «карт загроз/цілей» або «радарів», які створюють ілюзію контролю над ситуацією та спонукають користувача до взаємодії з потенційно сумнівними інформаційними ресурсами.

Практична значущість отриманих результатів полягає у можливості їх застосування для підвищення цифрової стійкості населення та профілактики негативних наслідків соціально-інженерних атак. До базових превентивних заходів належать: перевірка повідомлень через офіційні канали, дотримання принципів цифрової гігієни, обмеження взаємодії з неперевіреними посиланнями та розвиток медіаграмотності як механізму зниження вразливості до емоційного тиску.

Перспективи подальших досліджень полягають у поглибленні типологізації соціально-інженерних сценаріїв у воєнний час, уточненні критеріїв оперативної ідентифікації маніпулятивних повідомлень у месенджерах і соціальних мережах, а також у розробленні практикоорієнтованих освітніх і комунікаційних підходів, спрямованих на формування стійких навичок безпечної поведінки користувачів у цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Haborets, O. A., & Lunhol, O. M. (2025). Social engineering as a phenomenon of information influence in the digital environment. *National Interests of Ukraine, 11*(16), 95–104.
2. Zhmurko, O. (2024). Social engineering as a cybersecurity threat: Prevention and protection methods. *Security Pedagogy, 9*(1), 37–42. https://doi.org/10.31649/2524-1079-2024-9-1-037-042
3. Naseeb, J. (2025). Analyzing psychological operations: A case study of Indo-Pak hostility (2010–2024). *NUST Journal of International Peace & Stability, 8*(1), 77–90. https://doi.org/10.37540/njips.v8i1.187
4. Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2017). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems, 67*(2), 247–267. https://doi.org/10.1007/s11235-017-0334-z
5. Luhovets, D. V., & Petrenko, A. B. (2021). Structure for detecting phishing attacks of social engineering. In *Proceedings of the 6th International Scientific and Practical Conference "International Scientific Innovations in Human Life"* (pp. 201). Cognum Publishing House.
6. Laptiev, S. (2022). Improved method of personal data protection against attacks using social engineering algorithms. *Cybersecurity: Education, Science, Technique, 4*(16), 45–62. https://doi.org/10.28925/2663-4023.2022.16.4562
7. Dobryshyn, Yu. (2024). Application of statistical methods for predicting phishing attacks. *Cybersecurity: Education, Science, Technique, 3*(23), 56–70. https://doi.org/10.28925/2663-4023.2024.23.5670
8. Danylyk, V., Vysotska, V., & Nazarkevych, M. (2024). Methods for identifying disinformation, fake news, and propaganda in mass media based on machine learning. *Cybersecurity: Education, Science, Technique, 1*(25), 449–467. https://doi.org/10.28925/2663-4023.2024.25.449467
9. Nazarkevych, M., Vysotska, V., Yurynets, R., & Nakonechnyi, N. (2025). Methods for detecting disinformation in social networks based on artificial intelligence. *Cybersecurity: Education, Science, Technique, 2*(30), 209–223. https://doi.org/10.28925/2663-4023.2025.30.965
10. Prokopovych-Tkachenko, D., Bakuta, A., Zvieriev, V., Kozachenko, I., & Cherkaskyi, O. (2025). Modeling phishing scenarios in Ukraine's cyberspace: An analytical approach using Grafana dashboards. *Cybersecurity: Education, Science, Technique, 1*(29), 331–347. https://doi.org/10.28925/2663-4023.2025.29.881

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Olha Haborets
PhD, Associate Professor, Associate Professor of the Department of Operational and Investigative Activities and Information Security
Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine
ORCID: 0000-0001-7791-6795
olga-gaborets@ukr.net

SOCIAL ENGINEERING AS A TOOL OF INFORMATION AND PSYCHOLOGICAL OPERATIONS IN THE CONTEXT OF ARMED CONFLICT

Abstract. The article examines social engineering as one of the most effective tools of manipulative influence on users in the digital environment under conditions of armed conflict. It is emphasized that during wartime social engineering acquires particular danger, as it combines psychological pressure with technological channels of information dissemination, which complicates the critical perception of messages and increases the likelihood of impulsive behavior. It is substantiated that the main goal of social engineering influence in crisis conditions lies not only in misleading the user, but also in shaping controlled behavioral responses, such as panic, rapid dissemination of unverified messages, reduced trust in official communication channels, as well as disorganization of the information space.

Typical examples of manipulative messages in messengers that imitate emergency threat warnings and contain calls for immediate action (for example, “urgent,” “alert,” “open the map of targets/threats”) are analyzed. It is shown that the effectiveness of such messages is ensured by the use of stable psychological triggers, in particular the urgency effect, appeals to fear, informational uncertainty, and cognitive overload. It is proven that the combination of pseudo-official stylistics with visual markers of “legitimacy” (danger symbols, short imperative formulations, emotionally charged headlines) creates an impression of credibility for the user and contributes to an automated reaction without proper verification of the source.

Indicators by which the social engineering nature of messages can be identified are separately defined, including the imposition of urgency, localization of the threat to a specific territory or population group, direct behavioral instructions (“go,” “click,” “open”), as well as the use of reach or reaction indicators as a means of social confirmation. The practical significance of the study lies in the formation of basic preventive recommendations for countering social engineering: verification of messages through official sources, adherence to the principles of digital hygiene, limitation of following suspicious links, development of media literacy and resistance to emotional influence. It is concluded that systematic counteraction to social engineering during wartime requires a combination of technical, informational, and educational measures aimed at preserving information stability and safe user behavior in cyberspace.

Keywords: social engineering; cybersecurity; information and psychological influence; manipulative messages; phishing; disinformation; digital hygiene; media literacy.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Haborets, O. A., & Lunhol, O. M. (2025). Social engineering as a phenomenon of information influence in the digital environment. *National Interests of Ukraine*, *11*(16), 95–104.
2. Zhmurko, O. (2024). Social engineering as a cybersecurity threat: Prevention and protection methods. *Security Pedagogy*, *9*(1), 37–42. https://doi.org/10.31649/2524-1079-2024-9-1-037-042
3. Naseeb, J. (2025). Analyzing psychological operations: A case study of Indo-Pak hostility (2010–2024). *NUST Journal of International Peace & Stability*, *8*(1), 77–90. https://doi.org/10.37540/njips.v8i1.187
4. Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2017). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*(2), 247–267. https://doi.org/10.1007/s11235-017-0334-z
5. Luhovets, D. V., & Petrenko, A. B. (2021). Structure for detecting phishing attacks of social engineering. In *Proceedings of the 6th International Scientific and Practical Conference “International Scientific Innovations in Human Life”* (pp. 201). Cognum Publishing House.

6. Laptiev, S. (2022). Improved method of personal data protection against attacks using social engineering algorithms. *Cybersecurity: Education, Science, Technique, 4*(16), 45–62. https://doi.org/10.28925/2663-4023.2022.16.4562
7. Dobryshyn, Yu. (2024). Application of statistical methods for predicting phishing attacks. *Cybersecurity: Education, Science, Technique, 3*(23), 56–70. https://doi.org/10.28925/2663-4023.2024.23.5670
8. Danylyk, V., Vysotska, V., & Nazarkevych, M. (2024). Methods for identifying disinformation, fake news, and propaganda in mass media based on machine learning. *Cybersecurity: Education, Science, Technique, 1*(25), 449–467. https://doi.org/10.28925/2663-4023.2024.25.449467
9. Nazarkevych, M., Vysotska, V., Yurynets, R., & Nakonechnyi, N. (2025). Methods for detecting disinformation in social networks based on artificial intelligence. *Cybersecurity: Education, Science, Technique, 2*(30), 209–223. https://doi.org/10.28925/2663-4023.2025.30.965
10. Prokopovych-Tkachenko, D., Bakuta, A., Zvieriev, V., Kozachenko, I., & Cherkaskyi, O. (2025). Modeling phishing scenarios in Ukraine's cyberspace: An analytical approach using Grafana dashboards. *Cybersecurity: Education, Science, Technique, 1*(29), 331–347. https://doi.org/10.28925/2663-4023.2025.29.881

Отримано редакцією журналу / Received: 25.01.26
Прорецензовано / Revised: 15.02.26
Схвалено до друку / Accepted: 26.03.26