УДК: 004.056.55:159.9 DOI: **10.33099/2311-7249/2025-53-2-43-50**

ДЖАЛЛАДОВА Ірада Агаверді-кизи,
доктор фізико-математичних наук, професор,
Київський національний економічний університет імені Вадима Гетьмана, Київ, Україна,
https://orcid.org/0000-0003-3158-6844

КАМІНСЬКИЙ Олег Євгенович,
доктор економічних наук, доцент,
Київський національний економічний університет імені Вадима Гетьмана, Київ, Україна,
https://orcid.org/0000-0003-0607-8944

СОЦІАЛЬНО-ПСИХОЛОГІЧНА СТІЙКІСТЬ СИСТЕМ КІБЕРБЕЗПЕКИ

Метою статті *є системний аналіз психологічної резильєнтності користувачів і нападників та дослідження соціально-психологічних й поведінкових компонентів як складової частини архітектури кіберзахисту.*

Методи дослідження. *Під час проведення дослідження застосовано системно-поведінковий підхід, когнітивне моделювання на основі теорії прийняття рішень, а також елементи імітаційного моделювання з використанням експоненційних функцій впливу. Зазначений методичний підхід дає змогу кількісно описати ефект психологічного тиску на зловмисника і користувача, оцінити рівень їхньої стійкості та сформувати практичні рекомендації для побудови адаптивних систем кіберзахисту.*

Отримані результати дослідження. *Проведено аналіз взаємозв'язку технічних і когнітивних чинників, які визначають ефективність дій зловмисника та здатність систем кіберзахисту протистояти психологічно зумовленим атакам. Формалізовано модель ймовірності дезорієнтації зловмисника, яка враховує інтенсивність технічного та когнітивного впливу. Запропоновано багатофакторну модель соціально-психологічної стійкості користувача, де враховано рівень обізнаності, емоційне навантаження та когнітивні упередження. Побудовано порівняльну таблицю ефективності різних сценаріїв захисту. Доведено, що комбінований техніко-психологічний вплив є найбільш результативним у системах протидії фішинговим атакам та інженерії довіри.*

Елементи наукової новизни. *Наукова новизна роботи зводиться до розширення концепції кібербезпеки через інтеграцію психологічного компонента в процес оцінювання ефективності систем захисту, а також у кількісному описі ефектів впливу соціальних, емоційних і когнітивних чинників на поведінку нападників.*

Теоретична й практична значущість викладеного у статті. *Теоретичне значення зводиться до обґрунтування підходів до моделювання поведінки уразливих користувачів і зловмисників, а практичне – до можливості впровадження запропонованих моделей у системи попередження кіберзагроз, інструменти аналізу інцидентів та системи навчання персоналу для підвищення кібергігієни. Отримані результати мають прикладне значення для розробки захисних рішень у корпоративних мережах, кіберфізичних системах, а також у соціальних мережах, де спостерігається більша кількість психологічно орієнтованих атак.*

Ключові слова: *кібербезпека, соціальна інженерія, психологічна стійкість, когнітивні упередження, емоційний вплив, поведінкове моделювання, фішинг, техніко-психологічний захист.*

Вступ

Термін «соціальна мережа» вперше був запроваджений соціологом Дж. Барнсом в 1954 році. Саме йому належить ідея розглядати взаємозв'язки між людьми за допомогою соціограм, де учасники позначаються точками, а зв'язки між ними – лініями [1]. Г. Рейнгольд висловив іншу ідею, зокрема, що віртуальні спільноти можуть виникати у мережі. Але виникають вони тільки коли люди відкрито комунікують між собою достатньо тривалий час, утворюючи таким чином мережу особистих відносин [2].

У 1990-х роках дослідження соціальних мереж набули стрімкого розвитку. Зокрема, завдяки роботам американського соціолога Марка Грановеттера. Він представив соціальні мережі як складні системи із індивідів (вузлів) і зв'язків між ними. Починаючи з 2000-х років, унаслідок стрімкого поширення Інтернету онлайн-мережі стали більш поширеними. Це відкрило нові можливості для збору даних [3]. Так, наприклад, соціологи дійшли висновку, що соціальні мережі слугують не лише каналами поширення інформації, а й засобами формування суспільної думки [4]. Хоча існує багато інших видів соціальних медіа, соціальні мережі залишаються найпопулярнішими. Facebook, Instagram та Youtube продовжують приваблювати людей незалежно від їхніх потреб: підтримувати зв'язок із друзями, стежити за актуальними подіями або розвивати професійну мережу контактів (рис. 1).

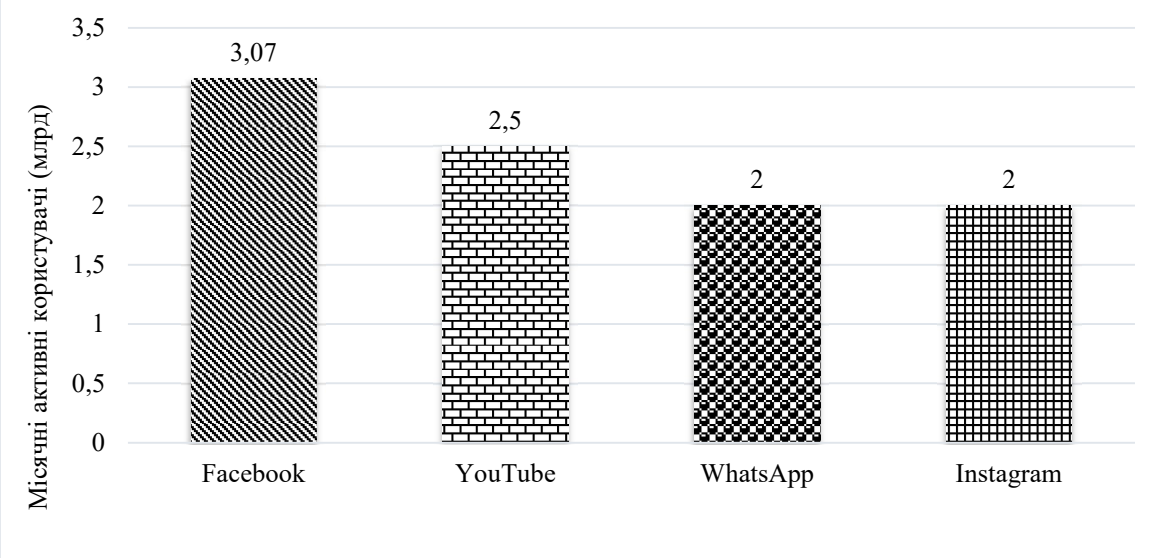

Рисунок 1 – Кількість користувачів основних соціальних мереж станом на 2025 рік [5]

Загалом, соціальні мережі є складним та багатовимірним феноменом, що охоплює широкий спектр процесів, пов'язаних з цифровою комунікацією, обміном інформацією і думками у Інтернеті. В результаті наукових досліджень сформовано різні теоретичні підходи, що сприяють глибшому розумінню ключових характеристик соціальних мереж та їхнього впливу на суспільство.

Постановка проблеми. Людський фактор залишається головною ланкою у ланцюзі безпеки. Соціальна інженерія експлуатує когнітивні упередження (довіра, страх, невідкладність), що знижує здатність навіть технічно сильних систем до ефективного самозахисту. Ризики у соціальних мережах залишаються актуальними, проте дезінформація є однією із найбільших загроз. Це свідомо неправдива, викривлена інформація, що поширюється із метою обману чи маніпулювання громадською думкою, політичними опонентами або конкурентами. Ставлення особистості до дезінформації в соціальних мережах визначається низкою когнітивних, емоційно-оцінних, ціннісно-смислових і поведінкових компонентів. Важливими когнітивними компонентами є уявлення про способи реалізації дезінформації, розуміння того, як інформація може бути спотворена чи неправдиво подана. Вони також містять знання про зв'язки з іншими ризиками, такими як соціальні, політичні чи економічні проблеми, а також про засоби захисту від дезінформації. Це передбачає усвідомлення методів виявлення неправдивої інформації і можливостей протидії дезінформації на рівні держави або організацій. Загрози можна умовно класифікувати за трьома основними категоріями: традиційні атаки, сучасні атаки і цільові атаки, як наведено авторами в табл. 1.

Таблиця 1

Вектори атак на соціальні мережі

Категорія атаки	Тип атаки	Опис
Традиційні атаки	Спам	Масова розсилка небажаних повідомлень з рекламною або шкідливою метою.
	Фішинг	Шахрайські спроби отримати конфіденційну інформацію, маскуючись під довірені джерела.
	Крадіжка особистих даних	Несанкціоноване отримання персональної інформації користувача.
Сучасні атаки	Клонування профілю	Створення підробленого акаунту, що імітує реального користувача.
	Викрадення	Несанкціоноване заволодіння обліковим записом або особистими матеріалами.
	Атака логічного висновку	Аналіз публічних даних для виведення прихованої або чутливої інформації.
	Атака Sybil	Створення численних фальшивих акаунтів для маніпулювання інформацією.
	Клікджекінг	Приховування шкідливих елементів під виглядом нешкідливих кнопок або посилань.
	Атака деанонімізації	Встановлення особи користувача на основі непрямих ознак.
	Кібершпигунство	Таємне спостереження або збір інформації для політичних, економічних чи приватних цілей.
Цільові атаки	Кіберзалякування	Систематичне залякування, тиск або психологічне насильство в онлайн-середовищі.
	Кіберстеження	Стеження за особою через цифрові канали.

Кібершпигунство, на нашу думку, є діяльністю, що передбачає використання цифрових технологій для збору конфіденційної інформації або інтелектуальної власності із метою її передачі ворожим сторонам. Наслідками кібершпигунства можуть бути: втрата стратегічної переваги, витік матеріалів, компрометація інформації, фінансові збитки чи навіть людські жертви. Одним із поширених методів у межах цієї діяльності, є використання соціального інженерінгу. Наприклад, зловмисники можуть проникати до профілів у соціальних мережах для отримання доступу до цінної інформації – службових завдань, електронної адреси або інших персональних даних, що згодом використовуються для точкових атак чи подальшого шпигунства.

Так, згідно з даними європейської страхової компанії North Queensland Insurance (QBE), кількість глобальних руйнівних кібер-операцій зросла на 105% до кінця 2024 року (тобто, з близько 103 до приблизно 211 за рік) [6]. Компанія IBM вказує, що середня вартість витоку даних становила 4,9 млн доларів у 2023 році (тобто зросла на 10 % за рік). Така динаміка свідчить про суттєве ускладнення кіберзагроз і вказує на потребу в посиленні заходів із кібербезпеки. У наукових і прикладних дослідженнях постійно ведеться пошук ефективних рішень для протидії загрозам у соціальних мережах, що свідчить про актуальність теми дослідження.

Аналіз останніх досліджень і публікацій. У роботі [7] D. Lacey та B. Woodrow зробили акцент на дослідженні когнітивно-психологічних механізмів, що впливають на сприйняття та поведінку користувачів мереж під час фішингових атак. Вони розглянули вплив таких факторів як імпульсивність, авторитет джерела, довіра та емоційний стан на ймовірність переходу на шкідливе повідомлення. Показано, що жертви найчастіше діють нераціонально, знаходяться під впливом упереджень і це значно знижує їхню резилентність (англ. resilience – пружність, еластичність) тобто здатність зберігати в несприятливих ситуаціях стабільний рівень психологічного та фізичного функціонування.

У дослідженні [8] було підтверджено, що поєднання технічної (наприклад, такий вид пастки, як «honeypot») і психологічної (введення в оману, імітація реакцій) дезінформації значно підвищує ефективність захисних заходів у кіберпросторі. Автори довели, що атакувальники частіше припускаються помилок, коли стикаються з переконливими когнітивними пастками. Результати дослідження відкривають перспективу застосування соціально-поведінкових технологій як активну ланку захисту.

Автори статті [9] моделюють поведінку зловмисника в умовах внутрішньої загрози за допомогою когнітивної архітектури ACT-R. Розроблена модель ураховує такі фактори, як пам'ять, навчання, увагу, контекст прийняття рішень та контекст впливу. Результати свідчать, що поведінка атакувальника може бути передбачена, якщо відомі його когнітивні особливості та стан. Результати дослідження відкривають можливості для розроблення адаптивних систем кіберзахисту, що враховують мікроповедінкові шаблони зловмисників.

У звіті агентства «IARPA» було досліджено вплив психологічного втручання на поведінку кіберзловмисників [10]. Серед головних ефектів було виявлено такі: attentional tunneling (звуження фокусу), loss aversion (страх втрати), а також ефект зниження обережності зловмисника за надмірної впевненості. Дослідження підтвердило, що використання когнітивної обробки до зловмисників, знижує точність атак і підвищує вразливість самих хакерів. Запропоновано захисну психологічну інженерію як новий напрям досліджень.

У роботі [11] було розглянуто доцільність інтеграції психічної стійкості та поведінкової обізнаності у політику кібергігієни. Дослідники наголошують, що навіть найсильніші технічні заходи безпеки безсилі, якщо працівники не здатні розпізнавати маніпуляції. Запропоновано комплексну реформу корпоративної культури безпеки, де психологія має стати ключовим елементом.

Усі дослідження підтверджують, що головною вразливістю сучасних кіберзахисних систем є людина, а не технічна інфраструктура, причому вплив на поведінку можливий не лише стосовно жертв, а й щодо самих зловмисників. Але у більшості досліджень не досліджено питання повної інтеграції психологічної стійкості у корпоративні політики кібербезпеки чи міжнародні стандарти, що свідчить про розрив між наукою і практикою та актуальність цього питання.

Мета статті – системний аналіз психологічної резильєнтності користувачів і нападників та дослідження соціально-психологічних й поведінкових компонентів як складової частини архітектури кіберзахисту.

Виклад основного матеріалу дослідження

Соціально психологічна стійкість (англ. Cyber Psychology Resilience) – це здатність користувачів, персоналу та організацій протистояти кібератакам, які використовують маніпуляції, соціальну інженерію, фішинг, когнітивні викривлення та емоційний вплив [13]. На відміну від технічних аспектів кібербезпеки, ця концепція зосереджується на людині – головному елементі інформаційної взаємодії, розглядаючи її як:

об'єкт впливу з боку атакувальника (жертву);

активного суб'єкта протидії, який приймає рішення й реалізує захист (аналітика, фахівця з безпеки, звичайного користувача).

Тобто, концепція соціально-психологічної стійкості в кібербезпеці є міждисциплінарним підходом, який пояснює здатність індивідів та організацій протистояти, адаптуватися й ефективно реагувати на психологічний, інформаційний та технічний тиск під час кіберінцидентів. Ця концепція розглядає людину як динамічний елемент

кіберпростору та поєднує наукові підходи з таких галузей:

когнітивної психології – для розуміння мислення, упереджень і реакцій на кіберзагрози;

прикладної кібербезпеки в її поведінковому вимірі;

поведінкової економіки – для аналізу прийняття ірраціональних рішень в умовах інформаційної невизначеності;

теорії прийняття рішень – для моделювання вибору дій у ситуаціях ризику;

елементів теорії ігор, зокрема, в частині моделювання стратегічної поведінки.

Аналіз впливу когнітивних упереджень доцільно здійснювати за двома напрямами. Перший стосується кінцевих користувачів (потенційних жертв атак), для яких проводиться оцінювання рівня стійкості до фішингових повідомлень та інших форм соціальної інженерії. Другий напрям фокусується на поведінкових реакціях атакувальників, зокрема, на зміну їхніх стратегій під впливом цілеспрямованих маніпуляцій, технічних або психологічних пасток, що моделюються в умовах контрольованого середовища. Застосування моделі «Insider Attack Game» у поєднанні з когнітивною архітектурою ACT-R дасть змогу змоделювати, як зловмисник приймає рішення у контексті кіберзагрози, зокрема, в умовах, коли його поведінка залежить не лише від технічного середовища, але й від психологічних і поведінкових факторів. Insider Attack Game є ігровою моделлю (тобто, game-theoretic simulation), яка описує сценарій, коли внутрішній користувач системи (інсайдер) приймає рішення, чи вчинити зловмисну дію, враховуючи ризики, ймовірність викриття, наслідки та стимули. Відповідно *ACT-R* (Adaptive Control of Thought–Rational), це когнітивна архітектура, розроблена для моделювання людського мислення, навчання та прийняття рішень [9].

Побудуємо математичну модель. Для початку визначимо рівень когнітивної стійкості за концептуальною моделлю, що заснована на модифікованій моделі для оцінки ризику помилки користувача в умовах інформаційного тиску [12]. Позначимо R – рівень стійкості (0…1), тоді він визначається за формулою:

$$R = 1 - (aB + \beta E + \gamma U), \quad (1)$$

де: B – індекс когнітивних упереджень (confirmation bias, trust bias);

E – рівень емоційної навантаженості (страх, терміновість);

U – навички обізнаності/Security Awareness;

α, β, γ – вагові коефіцієнти.

Когнітивні упередження (Cognitive Biases (B)) – це стійкі психологічні схеми, які спотворюють сприйняття інформації [9]. У контексті кібербезпеки вони використовуються як інструмент соціальної інженерії для маніпуляції жертвами, як наведено в табл. 2.

Таблиця 2

Когнітивні упередження (Cognitive Biases (B))

Типи упереджень	Пояснення	Приклад впливу
Confirmation Bias	Людина шукає лише ту інформацію, яка підтверджує її переконання	Фішинговий лист, який «підтверджує» підозри щодо безпеки акаунту, змушує натиснути на шкідливе посилання
Authority Bias	Схильність довіряти повідомленням від начебто авторитетних джерел	Шахраї використовують логотипи банків, Microsoft, Google
Scarcity Bias / Urgency Effect	Люди діють імпульсивно за наявності загрози втрати або під тиском часу	Повідомлення з написом: «Ваш акаунт буде заблоковано через 15 хвилин!»

Емоційне навантаження (Emotional Load (E)) можемо визначити, як рівень емоційного впливу, який викликає повідомлення або взаємодія з іншими особами. Зловмисники активно використовують емоції для примусового впливу, як це наведено в табл. 3.

Таблиця 3

Емоційне навантаження (Emotional Load (E))

Тип емоції	Пояснення	Приклад
Страх	Викликати паніку щодо безпеки, штрафів або втрати доступу	«Ви підозрюєтесь у фінансовому шахрайстві. Перейдіть за посиланням для пояснення»
Терміновість	Змушує жертву діяти миттєво, не роздумуючи	«Ваш акаунт буде видалено за 30 хв!»
Схвильованість/радість	Ефект позитивної несподіванки, наприклад «Ви виграли iPhone»	Вірусне спонукання до кліку

Усвідомленість у сфері безпеки (Security Awareness (U)) – це сукупність знань, навичок і поведінкових патернів, які зменшують вразливість людини до маніпуляцій [14], як показано в таблиці 4.

Таблиця 4

Усвідомленість у сфері безпеки (Security Awareness (*U*))

Компонент	Опис	Вплив
Знання про фішинг	Користувач розпізнає шаблони фальшивих повідомлень	Значно знижує ймовірність кліку
Критичне мислення	Сумнів до будь-якої незапрошеної інформації	Покращує здатність ігнорувати маніпуляції
Досвід атаки	Особи, що стикалися з шахрайством, демонструють вищу обережність	Посилення стійкості до повторної атаки

Як ми бачимо, когнітивні упередження суттєво знижують стійкість користувача, особливо в ситуаціях стресу або незрозумілих повідомлень, чим сильніше емоційне навантаження, тим вищий ризик помилки користувача, тобто навіть обізнані користувачі схильні діяти імпульсивно. Чим сильніше емоційне навантаження, тим вищий ризик помилки користувача, відповідно навіть обізнані користувачі схильні діяти імпульсивно. Аналіз факторів впливу наведено в таблиці 5.

Таблиця 5

Аналіз факторів впливу на рівень когнітивної стійкості

Фактор	Опис	Вплив на стійкість R
Cognitive Biases (*B*)	confirmation bias, authority bias	знижує *R* через α
Emotional Load (*E*)	страх, терміновість	сильний знижувальний ефект (β)
Security Awareness (*U*)	тренування, знання	підвищує *R* через γ

У процесах моделювання поведінки зловмисника та його взаємодії із захисними системами, які поєднують технічні засоби (такі типи пасток, як: honeypots, deception traps) та психологічний тиск (страх, невизначеність, когнітивне перевантаження), доцільним є використання експоненційної моделі впливу. Ймовірність потрапляння в пастку для користувача, яка дає змогу визначати групи підвищеного ризику (наприклад, нові співробітники, співробітники з низьким технічним бекграундом), визначаємо за виразом, побудованим на основі модифікованої моделі ймовірності потрапляння в пастку соціальної інженерії [8]:

$$P_{\text{victim}} = (1 - R) * V_e * I_{soc}, \quad (2)$$

де: V_e – емоційне навантаження повідомлення;

I_{soc} – соціальний тиск.

Впровадження психологічних пасток для атакувальників передбачає використання таких методів:

фальшиві ресурси із «занадто привабливими» назвами;

затримка відповіді, або симуляція «реакції» жертви;

«дзеркало поведінки», що спотворюють сприйняття реальності для зловмисника.

Математично ймовірність того, що атакувальник буде введений в оману, визначається за виразом, який концептуально базується на роботах Ferguson-Walter [8], де вплив на когніцію атакувальника моделюється як кумулятивний і нелінійний:

$$P_{\text{mislead}} = 1 - exp(-\lambda D), \quad (3)$$

де: D – інтегральна «сила впливу» (міра сумарного ефекту технічного та психологічного тиску), розрахована за шкалою 0–2;

λ – чутливість зловмисника до дезорієнтації (умовно постійна);

Значення D вибрані з урахуванням досліджень [8; 12], які свідчать, що додавання психологічної складової має експоненційний ефект, а не лінійний. У виразі (3) $\lambda = 1$, умовно прийнята як середня чутливість зловмисника до дезорієнтації (може змінюватися для різних груп атакувальників). Модель є спрощеною, але відповідає експериментальним результатам, описаним у роботах [8; 9; 12]. Результати експерименту наведено в табл. 6.

Таблиця 6

Експериментальні умови та отримані результати

Умова	*D*, сила впливу	P_{mislead}	Примітка
Контроль	0.69	≈ 0.50	Базова реакція, без втручань
Технічна пастка	1.05	≈ 0.65	Вплив тільки технічних засобів
Інформована пастка	1.39	≈ 0.75	Додано ефект очікування/страху
Комбінована (тех+інфо)	1.90	≈ 0.85	Найсильніший когнітивно-технічний вплив

Результати аналізу таблиці 6 свідчать, що ефективність дезорієнтації атакувальника значно зростає за умови комбінування психологічних і технічних засобів. У контрольному сценарії атакувальник не зустрічає жодного протидійного механізму, тому ймовірність введення в оману становить лише близько 50%. Технічна пастка (наприклад, honeypot) вже помітно підвищує цей

показник до 65 %. Інформованість про ризик парадоксально також підвищує ефективність пастки, оскільки сприйняття ризику змінює стратегію дій атакувальника. Найвищий ефект, 85 % можливо досягти в умовах комбінованого впливу, що вказує на необхідність інтеграції поведінкових стратегій у системи кіберзахисту.

Значення D, що використані в моделі, формалізованій виразом (3), відображають квантитативну оцінку суми ефектів технічних і психологічних впливів (пастки honeypots, decoy, повідомлення про пастку) та підтверджуються когнітивною моделлю, що враховує навчання, увагу, упередження. Складова D може бути подана як сума або середньозважене значення та є структурною інтерпретацією багатофакторного впливу, що базується на принципах когнітивної архітектури, ризик-менеджменту та кіберпсихології й моделювання рішень [8; 9]:

$$D = \omega_1 T + \omega_2 P + \omega_3 C, \quad (4)$$

де: T – технічний вплив (honeypots, фальшиві сервіси);

P – психологічний тиск (невизначеність, страх, знання про нагляд);

C – когнітивне перевантаження (інформаційний шум, вибірковість уваги);

ω_1, ω_2, ω_3 – вагові коефіцієнти (визначаються емпірично або за допомогою моделей машинного навчання).

Інтерпретація значень виконується так:

1. За $D \approx 0$ та $P \approx 0$ – зловмисник вільний у своїх діях.

2. За $D = 0.7$ та $P \approx 0.5$ – середній рівень впливу (поріг нерішучості).

3. За $D \geq 1.9$ та $P \approx 0.85$ – висока ймовірність дезорієнтації.

Переваги експоненційної моделі зводяться до того, що вона дає змогу врахувати нелінійний характер впливу та точніше моделювати граничні ефекти та ефект насичення.

Отже, додавання когнітивного елементу до кіберзахисту значно підсилює його результативність, що підтверджує актуальність запропонованого підходу у практиці безпеки. Соціально-психологічна стійкість має розглядатися як стратегічний компонент кіберзахисту на рівні з технічними засобами, а її оцінювання, як частина процесів ризик-менеджменту та цифрової безпеки.

Висновки й перспективи подальших досліджень

У результаті дослідження встановлено, що соціально-психологічні фактори відіграють критичну роль у забезпеченні ефективності систем кіберзахисту. Когнітивні упередження користувачів, емоційне навантаження та рівень обізнаності суттєво впливають на ймовірність успішного фішингу чи соціальної інженерії. Побудована модель стійкості дає змогу кількісно оцінити вплив зазначених чинників та формалізувати рівень вразливості до психологічних маніпуляцій.

Запропонована експоненційна модель впливу довела свою ефективність у моделюванні поведінки атакувальника під час взаємодії з техніко-психологічними пастками. На прикладі емпіричних даних продемонстровано, що комбінований підхід (технічні та когнітивні засоби) має найвищу результативність дезорієнтації зловмисника, до 85 % успішності.

Крім захисту корпоративних систем, результати дослідження мають особливу актуальність для середовища соціальних мереж, де психологічні атаки набувають масового характеру. Алгоритми персоналізації контенту, підсилення інформаційних бульбашок та маніпулятивні меседжі формують емоційний та когнітивний тиск на користувачів, знижуючи їхню критичність і стійкість до фішингу, дезінформації й шкідливих посилань. Урахування соціально-психологічних факторів у розробленні систем виявлення аномальної поведінки в соцмережах дасть змогу вчасно виявляти ознаки впливових кампаній, цифрових шахрайств та інформаційних атак, орієнтованих на емоційну маніпуляцію. Практичною значущістю викладеного у дослідженні є можливість інтеграції результатів у системи раннього попередження, політики кібергігієни та модулі навчання персоналу.

Надалі є доцільним розвивати науковий напрям мультиагентних симуляцій поведінки зловмисників та впроваджувати елементи поведінкової інженерії в системи управління інцидентами за допомогою апарату стохастичної математики. Такий підхід дасть змогу отримувати точкові прогнозні рішення в умовах невизначеності, зокрема, у період воєнного стану.

Список бібліографічних посилань

1. Barnes J. A. Class and committees in a Norwegian island parish. 1954. URL: https://psycnet.apa.org/doi/10.1177/001872675400700102 (Accessed: 05 June 2025). **2. Данько Ю. А.** Соціальні мережі як форма сучасної комунікації: плюси і мінуси. *Сучасне суспільство*. 2012. Вип 2. С. 179–184. **3. Rheingold, H.** The Virtual Community: Homesteading on the Electronic Frontier] / H. Rheingold. Reading, MA: Addison-Wesley, 1993. URL: https://www.britannica.com/topic/virtual-community (Accessed: 05 June 2025). **4. Філіпенко Л. В.** Роль соціальних мереж у формуванні суспільної думки під час російсько-української війни. *СОЦІОПОЛІС: Журнал соціальних та політичних наук.* 2024. № 1. С. 10–19 URL: https://sociopolis.in.ua/index.php/ journal/article/view/5/3 (дата звернення 05.06.2025). **5. DataReportal.** Global Social Media Users – 2025. *DataReportal.* 2025. URL: https://datareportal.com/social-media-users (дата звернення: 05 June 2025). **6. QBE Europe.** Annual global cyber attacks double from 2020 to 2024. QBE Insurance Group. 2024. URL: https://www.qbeeurope.com/news-and-events/press-releases/annual-global-cyber-attacks-double-from-2020-to-2024-qbe (Accessed: 05 June 2025). **7. Lacey D., Woodrow B., Piotrowski T.** Cyberpsychology of Deception: a Mini Review of the Psychological Factors Influencing Scam Compliance *EasyChair Preprints.* 2024. №10849. URL: https://easychair.org/publications/preprint/s5gh (Accessed: 05 June 2025). **8. Kimberly F.-W., Major M., Johnson Ch. K., Muhleman D. H.** Examining the Efficacy of Decoy-based and

Psychological Cyber Deception. *USENIX Security Symposium* (2021). URL: https://www.usenix.org/system/files/sec21fall-ferguson-walter.pdf (Accessed: 05 June 2025). **9. Cranford E. A., Gonzalez C., Aggarwal P., Tambe M., Cooney S., Lebiere C.** Towards a Cognitive Theory of Cyber Deception: Modeling Adversarial Behavior in Insider Threat Scenarios Using ACT-R. Carnegie Mellon University, Dynamic Decision Making Lab. 2021. URL: https://www.cmu.edu/dietrich/sds/ddmlab/papers/CranfordGonzalezAggarwalTambeCooneyLebiere2021.pdf (Accessed: 05 June 2025). **10. Office of the Director of National Intelligence (IARPA).** Understanding the Mind of a Hacker: The ReSCIND Program. *The Wall Street Journal*. 2024. URL: https://www.wsj.com/video/events/understanding-the-mind-of-a-hacker/04C55ED6-50A1-42C5-B2CC-561682579531.html (Accessed: 05 June 2025). **11. Khadka K., Ullah A. B.** Human factors in cybersecurity: an interdisciplinary review and framework proposal. *Int. J. Inf. Secur*. 2025. № 24. P. 119. DOI: https://doi.org/10.1007/s10207-025-01032-0. **12. Hadlington L.** Human factors in cybersecurity: examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*. 2017. Vol. 3. №7. DOI: https://doi.org/10.1016/j.heliyon.2017.e00346. **13. Cyber psychological resilience.** Sustainability Directory. 2025. URL: https://fashion.sustainability-directory.com/term/cyber-psychological-resilience (Accessed: 06 July 2025). **14. Bederna, Z.** Components of Security Awareness and Their Measurement. Part 1. *ISACA Journal*. 2020. Vol. 5. URL: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/components-of-security-awareness-and-their-measurement-part-1 (Accessed: 06 July 2025).

SOCIO-PSYCHOLOGICAL STABILITY OF CYBER SECURITY SYSTEMS

DZHALLADOVA Irada, Doctor of Physical and Mathematical Sciences, Professor, Kyiv National Economic University named after Vadim Hetman, Kyiv, Ukraine, https://orcid.org/0000-0003-3158-6844

KAMINSKY Oleg, Doctor of Economic Sciences, Associate Professor, Kyiv National Economic University named after Vadim Hetman, Kyiv, Ukraine, https://orcid.org/0000-0003-0607-8944

Formulation of the problem in general. *The purpose of the article is a systematic analysis of the psychological resilience of users and attackers, and a study of socio-psychological and behavioural components as an integral part of the cyber defence architecture.*

Research methods. *During the course of the investigation, a system-behavioural approach, cognitive modelling based on the theory of decision making, as well as elements of simulation modelling based on exponential exponentials were established. functions in flux. Therefore, a methodical approach allows us to clearly describe the effect of psychological pressure on the malicious and the corrupt, assess the level of their stability and formulate practical recommendations for encouraging adaptive systems cyber defence specialists.*

Literature review. *Based on recent studies, the most significant risk factor in cybersecurity is people, rather than the technology infrastructure. D. Lacey and B. Woodrow's work suggests that factors like impulsivity, source authority, trust, and emotional state weaken resilience to phishing attempts. Ferguson-Walter and others proved that the use of both technical (honeypot) and psychological (manipulative) traps enhances protective layers by controlling the actions of attackers, thereby forcing them to err. The work of Cranford and others modelling the actions of attackers using the cognitive architecture ACT-R took into account memory, attention, and context of decision-making, making room for systems that adapt to varying protective needs. The IARPA report confirms that focused psychological factors like fear of loss and overconfidence targeted at attackers render ineffective their own defences and render them susceptible to hacking. Study stresses the critical need to embed psychological resilience and behavioural awareness into the culture of corporate security, because without mastery to discern cues of manipulation, even the most sophisticated technology fails. At the same time, in most works, the issue of full integration of socio-psychological sustainability into international standards and policies is insufficiently considered, which demonstrates the existence of a gap between scientific approaches and practical implementation.*

Research results. *The article formalises a model of the severity of disorientation of an attacker, which is influenced by the intensity of technical and cognitive infusion. A multi-factor model of the socio-psychological stability of the teacher has been established, and the level of awareness, emotional attraction and cognitive anticipation has been ensured. A table of the effectiveness of various protection scenarios has been generated. It has been proven that combinations of technical and psychological infusion are the most effective in systems against phishing attacks and trust engineering.*

Research novelty. *The scientific novelty of the work lies in the expanded concept of cybersecurity through the integration of the psychological warehouse in assessing the effectiveness of security systems, as well as in the comprehensive description of the effects of the influx of social, emotional and cognitive factors on the behaviour of attackers.*

The theoretical and practical significance *of what is stated in the statistics. Theoretically, the significance lies in the grounded approaches to modelling the behaviour of aggressive cybercriminals and criminals, and practically, in the possibility of implementing models in the cyber threat prevention system, analysis tools, Incidents and systems trained on personnel to promote cyber hygiene. The obtained results may be of practical importance for the development of chemical solutions in corporate networks, cyber-physical systems, as well as in social networks, where there is an increasing number of psychologically oriented attacks.*

Conclusions and future work. *The study has confirmed that socio-psychological factors such as cognitive biases, emotional stress, and level of awareness are of primary importance to users' resistance to phishing and social engineering, and the model put forth enables them to assess risk quantitatively. The social media environment, wherein*

psychological attacks are ubiquitous, would benefit especially from the model's empirical data, where an attacker could be disoriented up to 85 per cent of the time when both cognitive and technical means are employed. This work can be integrated into early detection systems, cyber hygiene policies, and training modules, while adding multi-agent simulations and behavioural engineering to accurately predict uncertain, including wartime, conditions, which would further refine the research.

Keywords: *cybersecurity, social engineering, psychological resilience, cognitive anticipation, emotional infusion, behavioural modelling, phishing, technical-psychological protection.*

References

1. Barnes, J. A., (1954). Class and committees in a Norwegian island parish [online]. Available at: https://psycnet.apa.org/doi/10.1177/001872675400700102 [Accessed: 05 June 2025]. **2. Danko, Yu. A.,** (2012). Social networks as a form of modern communication: pros and cons. *Suchasne suspilstvo*. 2, 179-184. **3. Rheingold, H.,** (1993). The Virtual Community: Homesteading on the Electronic Frontier [online]. Reading, MA : Addison-Wesley. Available at: https://www.britannica.com/topic/virtual-community [Accessed: 05 June 2025]. **4. Filipenko, L. V.,** (2024). The role of social networks in shaping public opinion during the Russian-Ukrainian war [online]. *SOTSIOPOLIS: Zhurnal sotsialnykh ta politychnykh nauk*. 1, 10-19. Available at: https://sociopolis.in.ua/index.php/journal/article/view/5/3 [Accessed: 05 June 2025]. **5. DataReportal.** Global Social Media Users – 2025 [online]. DataReportal. 2025. Available at: https://datareportal.com/social-media-users [Accessed: 05 June 2025]. **6. QBE Europe,** (2024). Annual global cyber attacks double from 2020 to 2024 [online]. QBE Insurance Group. Available at: https://www.qbeeurope.com/news-and-events/press-releases/annual-global-cyber-attacks-double-from-2020-to-2024-qbe [Accessed: 05 June 2025]. **7. Lacey, D., Woodrow, B. and Piotrowski, T.,** (2024). Cyberpsychology of Deception: a Mini Review of the Psychological Factors Influencing Scam Compliance [online]. *EasyChair Preprints*. 10849. Available at: https://easychair.org/publications/preprint/s5gh [Accessed: 05 June 2025]. **8. Kimberly, F.-W., Major, M., Johnson, Ch. K., Muhleman, D. H.** Examining the Efficacy of Decoy-based and Psychological Cyber Deception [online]. *USENIX Security Symposium* (2021). Available at: https://www.usenix.org/system/files/sec21fall-ferguson-walter.pdf [Accessed: 05 June 2025]. **9. Cranford, E. A., Gonzalez, C., Aggarwal, P., Tambe, M., Cooney, S. and Lebiere, C.,** (2021). Towards a Cognitive Theory of Cyber Deception: Modeling Adversarial Behavior in Insider Threat Scenarios Using ACT-R [online]. Carnegie Mellon University, Dynamic Decision Making Lab. 2021. Available at: https://www.cmu.edu/dietrich/sds/ddmlab/papers/CranfordGonzalezAggarwalTambeCooneyLebiere2021.pdf [Accessed: 05 June 2025]. **10. Office of the Director of National Intelligence (IARPA),** (2024). Understanding the Mind of a Hacker: The ReSCIND Program [online]. The Wall Street Journal. Available at: https://www.wsj.com/video/events/understanding-the-mind-of-a-hacker/04C55ED6-50A1-42C5-B2CC-561682579531.html [Accessed: 05 June 2025]. **11. Khadka, K., Ullah, A. B.,** (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal. *Int. J. Inf. Secur*. 24, 119. DOI: https://doi.org/10.1007/s10207-025-01032-0.
12. Hadlington, L., (2017). Human factors in cybersecurity: examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*. 3, 7. DOI: https://doi.org/10.1016/j.heliyon.2017.e00346. **13. Cyber psychological resilience,** (2025). [online]**.** Sustainability Directory. Available at: https://fashion.sustainability-directory.com/term/cyber-psychological-resilience [Accessed: 06.07.2025]. **14. Bederna, Z.,** (2020). Components of Security Awareness and Their Measurement [online]. Part 1. *ISACA Journal.* 5. Available at: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/components-of-security-awareness-and-their-measurement-part-1 (Accessed: 06 July 2025).

Рукопис надійшов до редакції *05.08.2025*
Рукопис прийнято до друку після рецензування *12.08.2025*
Дата публікації *29.08.2025*