«Системні технології» 4 (165) 2026 «System technologies»
DOI 10.34185/1562-9945-4-165-2026-07
УДК 004.056.5:316.472.4-053.6

С.Д. Лучик, І.В. Мудрицький, О.О. Мойко, Р.М. Стецик

КІБЕРГІГІЄНА МОЛОДІ У СОЦІАЛЬНИХ ПЛАТФОРМАХ: ВІД АНАЛІЗУ AITM-АТАК ДО МОДЕЛЕЙ БЕЗПЕЧНОЇ ПОВЕДІНКИ

Анотація. В статті проведено комплексне дослідження ризиків, з якими стикається молодіжна аудиторія у сучасних соціальних медіапросторах. Актуальність дослідження зумовлена стрімким розвитком методів соціальної інженерії, що переважно базуються на психологічних маніпуляціях. Представлено класифікацію соціальних мереж за віковими групами користувачів, що дозволило ідентифікувати пріоритетні вектори атак для кожної платформи. На основі емпіричного опитування виявлено критичні прогалини в цифровій обізнаності молоді: встановлено, що значна частина респондентів є вразливими до атак типу Adversary-in-the-Middle (AiTM) через нездатність розпізнати підроблені домени, а також ігнорують відсутність протоколів шифрування даних. Детально проаналізовано механіку перехоплення сесійних токенів та подальшого захоплення облікових записів (Account Takeover).

Практичне значення дослідження полягає у розробці триярусної моделі захисту, що включає загальносистемні, платформно-орієнтовані (Telegram, Instagram, TikTok) та мережеві (Wi-Fi безпека) рекомендації. Запропонований освітньо-поведінковий підхід зміщує акцент із суто технічних засобів захисту на формування активної цифрової стійкості користувача.

Ключові слова: соціальна інженерія, соціальні мережі, кібергігієна, атака AiTM (Adversary-in-the-Middle), захоплення акаунту (Account Takeover), фішинг, вразливість користувачів, цифрова стійкість.

Вступ. Соціальні мережі глибоко інтегрувались в сучасне життя українців. Вони створюють спільний цифровий простір для різних поколінь людей. За даними ресурсу «Громадський простір», станом на жовтень 2025 року в Україні соціальними мережами охоплено 58,5% населення. Порівняно з минулим роком кількість користувачів соціальних мереж зросла на 6,5% або на 1,4 млн осіб. На кінець 2025 року соцмережами користувалися 20,8 млн людей віком 18+ [1].

Сьогодні соціальні мережі - це не лише цифровий простір для фото, постів і реакцій користувачів. Аудиторія активно мігрує між платформами і шукає нові формати контенту. Соціальні платформи є лідерами серед джерел отримання новин. Серед них Telegram-канали, Facebook, Viber та інші. YouTube став для користувачів новим телебаченням, а TikTok — пошуковою системою. Відзнакою сучасних соціальних платформ є робота у режимі постійної взаємодії з користувачем, де різний контент ство-

© Лучик С.Д., Мудрицький І.В., Мойко О.О., Стецик Р.М., 2026
Copyright for this paper by its authors. Use permitted under License CC BY 4.0.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

рюється і поширюється надто швидко. Так швидко, що на нього можуть не встигнути відреагувати модератори мереж або правоохоронні органи. Проте, встигають злочинці. Усі публічні пости, які користувач створює або/і поширює, дають зловмиснику можливість здійснити психологічну оцінку вибраної жертви, і надалі маніпулювати цими даними для здійснення злочину або кіберзлочину. Зловмисники «атакують» не лише пересічних громадян, а й військовослужбовців, журналістів, волонтерів, державних службовців з метою отримання інформації, яка може виявитися корисною, або ж задля поширення фейкової інформації, під чужим іменем, що, зазвичай, спричинює значний інформаційний вплив на свідомість громадян, особливо молодих людей.

Постановка проблеми. Фахівці відмічають, що 98% кібератак здійснюються за допомогою саме методів психологічного маніпулювання людьми, або методів соціальної інженерії, щоб отримати конфіденційні дані чи увійти в систему з обмеженим доступом. При цьому злочинці використовують такі емоційні складники, як страх, соціальні та родинні зв'язки, невпевненість і неуважність. Велика кількість людей хоча б раз стикалася з підробними фішинговими листами від так званих колег, телефонними дзвінками від «представників банку» і «родичів, які опинилися в біді» тощо. Через простий аналіз профілю обраної жертви зловмисник може визначити вразливі тематики користувача і використати їх для подальшої атаки за допомогою соціальної інженерії.

Молодь є найактивнішою та найбільш представленою категорією користувачів у соціальних медіа, де їхня висока цифрова грамотність часто супроводжується психологічною вразливістю та браком життєвого досвіду в розпізнаванні маніпуляцій. Схильність до самовираження та надмірного поширення особистої інформації створює ідеальний «цифровий портрет» для зловмисників, дозволяючи їм застосовувати високоточні методи соціальної інженерії.

Аналіз останніх досліджень і публікацій. Проблематика кібератак, що здійснюється за допомогою соціальної інженерії, залишається об'єктом досліджень як українських, так і міжнародних досліджень. Досліджуючи праці зарубіжних авторів, соціальна інженерія визначається насамперед як метод психологічного впливу на людину.

Згідно з визначенням NIST, соціальна інженерія - це психологічна маніпуляція, спрямована на людську схильність до помилок, а не на вразливості програмного забезпечення. Зловмисники знають, що часто легше обдурити людину, ніж пробити брандмауер [2]. Jan-Willem H. Bullee та інші підкреслюють, що ефективність соціальної інженерії спрямована не на технічні, а на когнітивні чинники, а найбільш дієвим способом протидії соціальної інженерії є формування навичок кібергігієни шляхом навчання цифрової обізнаності користувачів [3].

Дослідник М. Халіл також акцентує увагу на передбачуваних когнітивних упередженнях, що застосовують злочинці. І визначає ключові тригери, на які вони покладаються при використанні методів соціальної інженерії. Це:

- страх і терміновість- найпоширеніший та найефективніший тригер, оскільки він змушує викликати негайну емоційну реакцію;
- авторитет і довіра - люди звикли підкорятися авторитетним особам;

- цікавість і жадібність - бажання отримати винагороду, приз - спонука людей натискати на шкідливі посилання або відкривати заражені вкладення [2].

Отже, соціальна інженерія надзвичайно небезпечна. Використовуючи людські слабкості та вразливості, вона легко вписується в повсякденну ділову діяльність людей, змушує кожного повірити у щось нереальне, неправдиве, щоб змусити їх надати особисту інформацію, яка надалі може бути використана для їхнього обману. S. Groš визначає соціальну інженерію як один з видів ведення інформаційної війни [4].

Небезпечність соціальної інженерії значно посилив штучний інтелект, який допомагає злочинцям імітувати голоси, створювати реалістичні електронні листи та навіть здійснювати фальшиві відеодзвінки. Багато з цих прийомів взагалі не залишають слідів шкідливого програмного забезпечення, вони досягають результату, тому що люди приймають їх за справжні.

В останні роки набув поширення термін «соціальний інжиніринг», який використовується у сфері захисту комп'ютерних мереж, програм і баз даних. Він позначає низку кіберзлочинів – шахрайських схем несанкціонованого доступу до конфіденційної інформації, поширення дезінформації та ведення ІПСО (інформаційно-психологічна операція) [6]. Основна мета соціальних інженерів – це отримання доступу до захищених систем з метою крадіжки інформації, паролів, даних, тощо.

Звичайно, що роботодавці інвестують кошти в навчання персоналу з питань безпеки, проте порушення продовжуються. Це вказує на глибокий «прогалину в діях щодо обізнаності». Багато співробітників знають, що дія є ризикованою, але все одно роблять її для зручності або економії часу. Це переосмислює проблему «людського фактора». Це не завжди помилка користувача; часто це помилка в проекті безпеки. Л. Половенко та С. Мерінова наголошують, що основною передумовою соціальної інженерії є низький рівень обізнаності працівників щодо соціотехнічних атак та безпека інформаційної системи залежить від вивчення працівниками основ соціального інжинірингу та неухильного дотримання вимог політики безпеки, дотримання правил «цифрової гігієни» [7].

Законодавство України про кібербезпеку встановлює ефективні механізми реагування на кіберзагрози та кіберінциденти. Так, Закон України «Про основні засади забезпечення кібербезпеки України» (2017 р.) визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. Проте, принципи застосування Закону не поширюються на соціальні мережі [8].

В Стратегії кібербезпеки України «Безпечний кіберпростір - запорука успішного розвитку країни» (2021 р.) вказується на стрімке поширення кіберзагроз на усі сфери життєдіяльності та необхідність постійного вдосконалення інструментарію їх реалізації. Підкреслюється невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації фахівців з питань кібербезпеки та кіберзахисту [9]. Однак, як і в по-

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

передньому документі, не виділяються окремо завдання боротьби з соціальною інженерією.

Отже, в сучасних умовах, умовах війни в Україні, коли соціальні платформи є основним інструментом комунікацій, а соціальна інженерія залишається причиною номер один порушень інформаційної та кібернетичної безпеки в державі, дослідження цих проблем слід продовжувати.

Мета статті. Метою статті є розробка комплексної моделі освітньо-поведінкового захисту молоді від методів соціальної інженерії в соціальних мережах на основі аналізу специфічних вразливостей (зокрема AiTM-атак та ATO), виявлених під час емпіричного дослідження рівня кібергігієни студентів та курсантів.

Для досягнення поставленої мети потрібно вирішити такі завдання:

- проаналізувати теоретичні аспекти класифікації сучасних соціальних мереж за віковими групами користувачів та ідентифікувати специфічні загрози, характерні для кожної платформи;
- дослідити емпіричним шляхом рівень обізнаності молодіжної аудиторії з правилами кібергігієни та виявити пріоритетні медіапростори, що мають найбільшу концентрацію ризиків соціальної інженерії;
- здійснити кількісну та якісну оцінку вразливостей респондентів до змодельованих кібератак;
- сформулювати рекомендації (загальносистемні, платформно-орієнтовані та мережеві), спрямовані на формування стійких навичок цифрової безпеки та превентивну протидію соціальній інженерії.

Викладення основного матеріалу дослідження. Соціальна мережа, як цифрова екосистема, являє собою комплексну онлайн-платформу, що об'єднує користувачів, контент, бізнес та сервіси в єдине середовище взаємодії. Вона функціонує як саморегульована система (як біологічна), де взаємозалежні елементи: профілі, контент, алгоритми тучного інтелекту, фінансові інструменти, впливають на поведінку людей.

Сучасний ландшафт соціальних мереж характеризується високою концентрацією користувачів на кількох платформах, що полегшує роботу соціальним інженерам через масштабність охоплення. У 2026 році світові тренди змістилися від простого споживання контенту до глибокої інтеграції зі штучним інтелектом та пошуковими алгоритмами. Така інтеграція супроводжується концентрацією даних, автоматизацією прийняття рішень та появою нових типів атак на AI-системи, що обумовлює необхідність підвищення рівня кібербезпеки, захисту даних, алгоритмів та інформаційних систем від нових кіберзагроз.

Визначимо основні тренди використання соціальних мереж користувачами різного віку та зв'язок їх з безпекою, тобто віково-орієнтовані соціальні мережі з платформною довірою. Користувачі різного віку схильні довіряти різним платформам, і саме ці платформи стають для них основним джерелом інформації, комунікації та формування думки. Таким чином, різні покоління остаточно закріпилися на "своїх" майданчиках (табл. 1):

Таблиця 1

Віково-орієнтовані соціальні мережі з платформною довірою

Клас соціальних мереж, вік	Платформа довіри	Тип довіри	Особливості
Дитячі та підліткові (0-12), включає вікові підгрупи:			
0-5	YouTube, YouTube Kids, TikTok (через батьків), Instagram (перегляд фото/відео)	Абсолютна візуально-емоційна довіра	Не є самостійними користувачами соціальних мереж, однак фактично активно присутні у цифровому середовищі через батьків або дитячі платформи.
6-9	YouTube, TikTok, Roblox, Minecraft, Месенджери (через батьків)	Авторитетно-рольова довіра	Цікавить ігровий, пригодницький та блогерський контент
10-12	TikTok, Instagram, Telegram, Viber, Discord	Соціально-мережева довіра	Соціальний контент, самопрезентація, спілкування, тренди.
Молодіжні, 12–25	TikTok, Instagram Snapchat, YouTube, Telegram, Discord, Twitch	Емоційна	Короткий відеоконтент; емоційна подача інформації; довіра до особистого досвіду блогерів; висока швидкість поширення інформації; високі ризики дезінформації
Соціально-інформаційні, 25-45	Facebook, X, LinkedIn, WhatsApp	Соціальна	Новини; професійні контакти; аналітика; обговорення подій; формування суспільної думки
Старша аудиторія, 45+	Facebook, YouTube, форуми, локальні групи	Традиційна	Корисна інформація та експертні поради; соціально-політична аналітика та новини; освітній контент з цифрової грамотності; сімейно-орієнтований контент

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Діти вікової групи 0-12 років переважно не є самостійними користувачами соціальних мереж. Однак, фактично активно присутні у цифровому середовищі через батьків або дитячі платформи. Їх використання соціальних мереж має опосередкований або розважально-освітній характер. У цій віковій групі важливо розрізняти не лише спосіб використання соціальних мереж, а й тип контенту, який вони споживають, оскільки саме контент формує поведінку, мислення та цифрові ризики.

Для вікової групи 0–12 років доцільно говорити про тип довіри до інформації та джерел у соціальних мережах, оскільки діти по-різному сприймають контент, блогерів, рекламу та онлайн-знайомства. Дуже важлива закономірність: Емоції → Авторитет → Соціальна група → Власна думка (після 13–14 років). Тобто:

- маленькі діти довіряють тому, що красиве;
- молодші школярі — тому, хто популярний;
- передпідлітки — тому, що кажуть друзі;
- підлітки — тому, що відповідає їх поглядам.

Це дуже важливо для розуміння тих ризиків і небезпек, які несуть соціальні мережі користувачам цієї вікової групи. Це інформаційні ризики (фейки, реклама, шкідливий контент), соціальні ризики (шахрайство, кібербулінг, грумінг, соціальна інженерія), психологічні ризики (тривожність, порушення сну, агресія, зниження самооцінки, ізоляція), технічні ризики (віруси, фішинг, злом акаунтів, витік даних, платні підписки, донати).

Вікова група 12–25 років є найактивнішою категорією користувачів соціальних мереж. Це вже не просто споживачі контенту, а повноцінні учасники цифрового середовища, які формують інформаційний простір, тренди, онлайн-спільноти та цифрову економіку. Так, соцмережі стають середовищем спілкування та самоствердження для підлітків віком 12-15 років, інструментом формування особистості та соціального статусу для молодих людей віком 16-18 років, інструментом навчання, роботи та соціальних зв’язків для молоді віком 19-21 років, інструментом кар’єри, бізнесу та нетворкінгу для більш старшої групи осіб віком 22-25 років.

До основних ризиків для користувачів соцмереж віком 12–25 років слід віднести: онлайн-шахрайство, фішинг, залежність від соцмереж, нелегальний контент, вербування через соцмережі тощо. Найбільш небезпечне середовище для молоді створюють такі мережі як TikTok, Telegram, Discord.

Для вікової групи користувачів соцмереж віком 25-45 років характерний високий рівень прагматизму у використанні соціальних мереж. Їх професійна діяльність і приватне життя нерозривно пов'язані з використанням соціальних медіаплатформ.

Ризики для користувачів соцмереж даної вікової групи обумовлені їхньою високою цифровою активністю та інтеграцією соціальних мереж у професійну діяльність, що робить їх пріоритетними цілями для складних атак із застосуванням соціальної інженерії, таргетованого фішингу та дезінформаційних кампаній. Основними загрозами є компрометація персональних і корпоративних даних через надмірне поширення інформації, фінансові втрати внаслідок вразливості до маніпулятивних технік, а також психологічне виснаження, спричинене синдромом FOMO та алгоритмічною поляризацією

контенту. Крім того, формування стійкого цифрового сліду створює довгострокові репутаційні ризики та можливості для несанкціонованого збору даних методами OSINT, що в умовах низької інформаційної гігієни може призвести до деструктивного впливу на професійний статус та особисту безпеку користувача.

Старша вікова категорія (45+ років) користувачів соціальних мереж демонструє консервативний підхід до вибору платформ (переважно Facebook, YouTube, месенджери типу Viber/WhatsApp) та має високий рівень цифрової довіри. Досить часто використання соцмереж спрямовується на підтримку родинних і дружніх зв'язків, а також на пошук тематичних спільнот за інтересами (садівництво, здоров'я, побут тощо).

Основними загрозами для цієї вікової групи є фінансові втрати через соціальну інженерію (зокрема схеми «допомоги близьким» або псевдомедичні послуги), викрадення особистих даних внаслідок нехтування базовими правилами кібергігієни (відсутність складної автентифікації, перехід за фішинговими посиланнями), а також висока ймовірність стати інструментом для масового поширення фейків. На відміну від молодших груп, загрози для даної категорії часто мають більш виражений психоемоційний характер, що призводить до глибокої соціальної дезорієнтації та значних матеріальних збитків.

Отже, проведені класифікація соціальних мереж і аналіз ризиків та небезпек для користувачів для кожної групи мереж виявив наступне. У різних соціальних мережах домінують різні методи соціальної інженерії, що зумовлено віковою аудиторією платформи, функціональними можливостями та рівнем довіри між користувачами. Так, Facebook та Instagram переважно використовуються для емоційно-маніпулятивних шахрайських схем, Telegram — для поширення фішингу та шкідливого програмного забезпечення, TikTok — для масових шахрайських кампаній, а LinkedIn — для таргетованих атак соціальної інженерії на організації та співробітників.

При розробці ефективних методів захисту від кіберзлочинців в соціальних мережах необхідно враховувати специфіку вразливостей різних вікових груп користувачів. Нами було проведено спеціалізоване соціальне опитування серед молодих людей: студентів, курсантів закладів вищої освіти для визначення вразливостей. У соціальному опитуванні взяли участь понад 500 респондентів, вікова група яких 14-24 роки. Частину вибірки (понад 80%) склали особи віком від 18 до 24 років та 15% віком 14-17 років. Соціальне опитування проводилося за допомогою платформи Google Forms у формі онлайн-анкетування.

Результати практичного дослідження демонструють, що значна частина користувачів все ж таки залишається вразливою до соціально-інженерних атак (табл. 2).

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Таблиця 2

Реакція респондентів на змодельовані сценарії атак

Сценарій атаки	Схильність до ризику (%)	Кількість осіб
Перехід за посиланням «Ваш акаунт буде заблоковано!»	7.2%	37
Введення даних на htpps://instagram.com.ua	24.5%	125
Перехід з проханням підписати петицію за посиланням “https://bit.ly/petitsia”	12.9%	66
Участь у підозрілих конкурсах у соціальних мережах	7.8%	40
Пропозиція покупки товару на дуже вигідною ціною	6.1%	31
Довіра до сайтів із протоколом http	21.1%	108

Детальний аналіз статистичних даних, отриманих у результаті проведення онлайн опитування, дозволяє зробити висновки:

- критична вразливість — підроблені домени (24.5%): Майже кожен четвертий респондент (125 осіб) готовий ввести дані на фейковому ресурсі instagram.com.ua. Це свідчить про низьку увагу до адресного рядка (URL), що є ідеальним підґрунтям для фішингу;
- технічна довірливість (21.1%): високий рівень довіри до незахищеного протоколу http (108 осіб) демонструє прогалину в базових знаннях про шифрування даних;
- соціально-цивільна маніпуляція (12.9%): використання скорочених посилань (наприклад, bit.ly) під виглядом петицій є ефективним гачком, оскільки молодь має активну громадянську позицію.

Отже, аналіз реакції респондентів на змодельовані атаки (табл. 3) виявив парадокс: молодь демонструє високу стійкість до прямих загроз блокування (лише 7.2% ризику), проте виявляється критично вразливою до інструментів візуальної імітації довірених ресурсів. Показник у 24.5% успішних атак через підміну домену instagram.com.ua свідчить про те, що архітектура загроз у молодіжному середовищі змістилася від "залякування" до "мімікрії" під звичні цифрові сервіси.

Результати опитування підтверджують, що значна частина осіб віком від 14 до 24 років готові ввести свої дані на підробленому домені https://instagram.com.ua. Це створює ідеальні умови для використання сучасних методів сучасних методів перехоплення доступу. Зокрема, слід виділити архітектуру AiTM (Adversary-in-the-Middle) та подальшого ATO (Account Takeover).

Згідно матриці MITTRE ATT&CK, T1557 Adversary-in-the-Middle (AiTM) описує тип атаки, при якій зловмисник створює проксі-сервер між користувачем та сервісом. У контексті нашого соціального опитування було виявлено, що 24.5% респондентів пе-

рейшли б за посиланням instagram.com.ua, внаслідок чого не розпізнали підроблений домен та стали потерпілими внаслідок атаки AiTM.

На відміну від фішингових посилань, атака типу AiTM не потребує копії сайту, оскільки зловмисник розгортає сервер-посередник, який у реальному часі транслює запити до справжнього сайту чи сервісу. Серед головних переваг атаки такого типу слід виділити:

- обхід Multi-Factor Authentication: коли користувач вводить свої кредити для входу та здійснює етап мультифакторної автентифікації на підробленому домені, зловмисник отримує усі дані та транслює їх до легітимного сервісу чи сайту;
- викрадення токена: після успішного входу легітимний сервіс/сайт видає сесійний cookie, який підтверджує, що користувач пройшов перевірку. Зловмисник отримує його та потім транслює до користувача;
- авторизований доступ: внаслідок отримання сесійного cookie, зловмисник імпортує його у власний браузер. Це надає зловмиснику повний доступ до облікового запису та не потребує паролю MFA. Успішна реалізація цього етапу є лише проміжним етапом, що веде на Account Takeover (ATO). Отримавши доступ до акаунту соціальної мережі внаслідок здійснення атаки AiTM, зловмисник прагне отримати повний контроль над обліковим акаунтом, щоб користувач не зміг повернути контроль;
- зміна даних: в першу чергу зловмисник змінює електронну пошту та номер телефону;
- скидання паролів: після успішної зміни електронної адреси та номеру телефону зловмисник реалізує скидання паролю. Оскільки зловмисник вже змінив пошту, справжній власник не має доступу до його зміни.

Отримані результати емпіричного дослідження дозволяють констатувати критичний розрив між високою інтенсивністю використання соціальних мереж молоддю та реальним рівнем їхньої цифрової стійкості. Схильність 24.5% респондентів до взаємодії з підробленими доменами (на прикладі instagram.com.ua) свідчить про те, що сучасна архітектура атак типу Adversary-in-the-Middle (AiTM) ефективно експлуатує візуальну довіру користувача, повністю нівелюючи традиційні технічні бар'єри безпеки.

Комплексний аналіз механіки Account Takeover (ATO) у поєднанні з даними опитування підтверджує наступні деструктивні тенденції:

- нівелювання багатофакторної автентифікації (MFA): Високий відсоток успішних переходів за фішинговими посиланнями доводить, що для підготовленого зловмисника MFA більше не є панацеєю, оскільки техніка AiTM дозволяє перехоплювати сесійні токени в реальному часі;
- психологічна непідготовленість: Найнижчий рівень ризику (7.2%) при сценарії "блокування акаунту" вказує на те, що молодь навчилася розпізнавати прямий агресивний тиск, проте виявляється безпорадною перед методами "м’якої мімікрії" під легітимні сервіси;

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

- технологічна інерційність: Довіра 21.1% опитаних до незахищеного протоколу http свідчить про ігнорування базових індикаторів безпеки браузера, що робить автоматизований збір даних максимально ефективним;

- експлуатація ідентичних облікових даних: оскільки користувачі часто використовують однакові кредити для входу (логін, пароль) для різних сервісів, успішне захоплення одного акаунту може призвести до перебору акаунтів інших сервісів/соціальних мереж;

- використання фактора довіри: зламаний акаунт стає джерелом розповсюдження нових атак, оскільки зловмисник може розсилати надалі фішингові посилання друзям з метою отримання несанкціонованого доступу до акаунтів соціальних мереж інших осіб чи з метою отримання фінансової вигоди, нанесення удару по репутації/довірі тощо.

Таким чином, успішна реалізація етапу АТО є закономірним результатом низької уваги молоді до деталей цифрового середовища та відсутності навички динамічної верифікації джерела інформації. Це обґрунтовує необхідність радикального перегляду стратегій захисту: перехід від статичних інструкцій до формування адаптивної моделі кібергігієни, що базується на критичному аналізі інтерфейсів та впровадженні поведінкових алгоритмів "нульової довіри" (Zero Trust) у повсякденну комунікацію.

Сформулюємо рекомендації, спрямовані на формування у молодіжної аудиторії користувачів соціальних мереж стійких навичок цифрової безпеки та протидії соціальній інженерії.

На основі отриманих даних про критичні вразливості (зокрема, 24.5% ризику в сегменті імітації доменів та 21.1% нехтування протоколами шифрування), пропонується триярусна модель рекомендацій: загальні, платформні, мережеві.

1. Загальносистемні заходи превентивної кібергігієни.

Ці заходи спрямовані на формування фундаментальних навичок безпечної поведінки, що не залежать від конкретного програмного середовища:

- *динамічна верифікація автентичності ресурсів* − впровадження принципу «критичної паузи» перед здійсненням транзакційних дій або введенням облікових даних. Необхідно розвивати навичку візуального аудиту URL-структури для виявлення тайпосквотингу та гомографічних атак (заміна символів схожими за накресленням);

- *перехід до стійких методів мультифакторної автентифікації (MFA)* − враховуючи вразливість SMS-кодів до перехоплення через AiTM-проксі, рекомендовано пріоритезацію апаратних засобів (U2F/FIDO2) або програмних генераторів одноразових паролів (TOTP), що функціонують локально на пристрої користувача;

- *використання менеджерів паролів як технічних фільтрів* − застосування спеціалізованого ПЗ для зберігання паролів виконує роль автоматизованого детектора фішингу, оскільки такі системи блокують автозаповнення форм на доменах, що не збігаються з еталонним записом у базі.

Мінімізація цифрового сліду (Anti-OSINT стратегія) − свідоме обмеження публікації метаданих, геолокацій та персональних відомостей, які можуть бути викори-

стані соціальними інженерами для побудови сценаріїв «претекстингу» (створення вигаданої ситуації для отримання довіри).

2. Платформно-орієнтовані заходи безпеки.

Враховуючи архітектурні особливості соціальних мереж, виявлених під час дослідження як пріоритетні, заходи захисту мають бути адаптовані під їхній специфічний інструментарій.

Сегмент месенджерів (на прикладі Telegram).

Конфігурація приватності метаданих − повне приховання номера телефону та обмеження прав на додавання до групових чатів категорією «Мої контакти». Це нівелює вектор атаки через автоматизовані скрипти масового спаму;

активація двоетапної перевірки (Cloud Password) − створення додаткового фактора захисту на рівні сервера месенджера, що є критично важливим для протидії викраденню сесійних токенів.

Сегмент візуальних соцмереж (на прикладі Instagram).

Верифікація історії облікових записів − використання інструментів внутрішнього аудиту («About this account») для перевірки частоти зміни імені користувача та географії входу, що дозволяє ідентифікувати акаунти, захоплені внаслідок атак ATO (Account Takeover);

обмеження вхідної взаємодії − Налаштування фільтрації Direct Messages та коментарів за ключовими словами-тригерами соціальної інженерії (наприклад, «giveaway», «verification», «support»), що знижує ймовірність первинного контакту зі зловмисником.

Сегмент алгоритмічних платформ (на прикладі TikTok).

Критична фільтрація контентного впливу − Розвиток навичок розпізнавання дипфейків (Deepfakes) та маніпулятивних відео, що поширюються під виглядом експертного контенту з метою перенаправлення користувача на зовнішні фішингові ресурси;

заборона крос-платформної авторизації − уникнення використання функції «Увійти за допомогою...» на неперевірених сервісах, що запобігає каскадному витоку даних між різними соціальними профілями.

Запропонований комплекс заходів базується на переході від реактивного захисту (боротьба з наслідками) до цифрової стійкості. Освітньо-поведінкова модель, інтегрована в навчальний процес студентів та курсантів, дозволяє сформувати «суб'єктивний бар'єр безпеки», який є ефективним навіть у випадках, коли технічні засоби захисту виявляються безсилими перед новими методами соціальної інженерії.

3. Заходи безпеки при використанні публічних та незахищених мереж передачі даних (Wi-Fi)

Окремим вектором вразливості молодіжної аудиторії є використання безкоштовних публічних точок доступу Wi-Fi у закладах освіти, кафе та транспорті. Враховуючи, що 21.1% респондентів не звертають уваги на відсутність шифрування (протокол http), ризик перехоплення трафіку стає критичним. Рекомендується впровадження таких стратегій:

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Примусова інкапсуляція трафіку (VPN-технології). Використання надійних VPN-сервісів (Virtual Private Network) при підключенні до будь-яких публічних мереж. Це створює захищений тунель, який унеможливлює зчитування сесійних токенів та паролів, навіть якщо зловмисник контролює точку доступу (атака типу "Evil Twin").

Деактивація функцій автоматичного підключення. Налаштування мобільних пристроїв на ручне підтвердження кожного з'єднання. Це запобігає автоматичній авторизації смартфона у підроблених мережах зловмисників, які імітують відомі публічні назви (наприклад, "Free_WiFi_University").

Гігієна транзакційних дій. Встановлення суворої заборони на здійснення фінансових операцій, вхід у поштові скрипки чи соціальні мережі під час перебування у незахищених мережах. Публічний Wi-Fi має використовуватись виключно для споживання неперсоналізованого контенту.

Контроль сертифікатів безпеки. Розвиток навички ігнорування ресурсів, що викликають попередження браузера про недійсні SSL-сертифікати. В умовах AiTM-атаки зловмисник часто намагається підмінити оригінальний сертифікат сайту власним, що є ключовим маркером небезпеки.

Висновки. Результати проведеного дослідження засвідчили, що:

- соціальна інженерія залишається одним із найбільш ефективних векторів атак. Використання психологічних маніпуляцій та емоційного тиску дозволяє зловмисникам успішно атакувати різні групи населення. Молодь є найбільш масовою групою користувачів соціальних мереж і їх акаунти досить часто попадають під дію атак злочинців;
- атаки типу AiTM становлять велику небезпеку, оскільки дозволяють зловмисникам обійти мультифакторну автентифікацію шляхом перехоплення сесійних токенів у реальному часі, перенаправляючи трафік від користувача до легітимного сервера через власний проксі-сервер.

Отримані результати дослідження підтверджують, що в умовах постійного зростання кіберзагроз, захист інформаційного простору вимагає переходу від базових методів захисту до динамічних моделей захисту, що завжди змінюється. Запропоновані загальносистемні, платформно-орієнтовані та мережеві заходи безпеки формують комплексну стратегію захисту. Вона спрямована не лише на технічне блокування загроз, а й на трансформацію поведінкових патернів користувача, що в умовах динамічної еволюції кіберзлочинності є найбільш ефективним інструментом забезпечення національної та особистої безпеки в інформаційному просторі.

Перспектива подальших досліджень полягає у розробці ефективних алгоритмів виявлення соціально-інженерних атак та реалізації освітніх програм з кібергігієни для найвразливіших верств населення − дітей та людей літнього віку оскільки їхній рівень цифрової грамотності і стійкості значно нижчий за інших.

ЛІТЕРАТУРА

1. Соцмережі 2026: важлива статистика для комунікацій НУО. *Громадський простір.* URL: https://www.prostir.ua/?kb=sotsmerezhi-2026-vazhlyva-statystyka-dlya-komunikatsij-nuo (дата звернення: 22.02.2026)

2. Khalil M. The Human Hack: 2025 Social Engineering Statistics, Trends, and Future Threats. *DeepStrike*. URL: https://deepstrike.io/blog/social-engineering-statistics-2025 (дата звернення: 25.02.2026).
3. Bullée, JW.H., Montoya, L., Pieters, W. et al. The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of Experimental Criminology*. 2015. Vol. 11, №1. Pp. 97–115. URL: https://doi.org/10.1007/s11292-014-9222-7
4. Groš S. Social engineering warfare as a tactic of information warfare. *European Integration Studies*. 2024. Vol. 20, №2. Pp. 67–86. URL: https://doi.org/10.46941/2024.2.3
5. Social Engineering. Glossary, Computer Security Resource Center. Information Technology Laboratory. NIST. URL: https://deepstrike.io/blog/social-engineering-statistics-2025 (дата звернення: 28.02.2026).
6. Бондаренко І. С. Контроверсійність концепту «соціальний інжиніринг» в умовах суспільно-політичних потрясінь. *Вчені записки ТНУ імені В. І. Вернадського.* Серія: Філологія. Журналістика. 2025. Том 36 (75). № 1. Частина 2. С. 293-299. https://doi.org/10.32782/2710-4656/2025.1.2/47
7. Половенко Л. П., Мерінова С. В. Виявлення ознак соціальної інженерії та технологія протидії соціальним хакерам на підприємстві. *Підприємництво та інновації.* 2019. № 10. С. 183–187. URL: https://doi.org/10.37320/2415-3583/10.28
8. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII: станом на 20.02.2026. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 28.02.2026).
9. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серпня 2021 року № 447/2021: станом на 05.03.2026. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 05.03.2026).

REFERENCES

1. Sotsmerezhi 2026: vazhlyva statystyka dlia komunikatsii NUO [Social Media 2026: Important Statistics for NGO Communications] (2026). Hromadskyi prostir. Retrieved from https://www.prostir.ua/?kb=sotsmerezhi-2026-vazhlyva-statystyka-dlya-komunikatsij-nuo [in Ukrainian].
2. Khalil M. (2025). The Human Hack: 2025 Social Engineering Statistics, Trends, and Future Threats. DeepStrike. Retrieved from https://deepstrike.io/blog/social-engineering-statistics-2025 [in English].
3. Bullée, JW.H., Montoya, L., Pieters, W. et al. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of Experimental Criminology*. Vol. 11, №1. Pp. 97–115. Retrieved from https://doi.org/10.1007/s11292-014-9222-7 [in English].
4. Groš S. (2024). Social engineering warfare as a tactic of information warfare. *European Integration Studies.* Vol. 20, №2. Pp. 67–86. Retrieved from https://doi.org/10.46941/2024.2.3 [in English].

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

5. Social Engineering. Glossary, Computer Security Resource Center. Information Technology Laboratory (2025). *NIST*. Retrieved from https://deepstrike.io/blog/social-engineering-statistics-2025 [in English].
6. Bondarenko, I. S. (2025). Kontroversiinist kontseptu «sotsialnyi inzhynirynh» v umovakh suspilno-politychnykh potriasin [The controversial nature of the concept of "social engineering" in times of socio-political upheaval]. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: Filolohiia. Zhurnalistyka.* Vol. 36 (75). #1. Part 2. Pp. 293-299. https://doi.org/10.32782/2710-4656/2025.1.2/47 [in Ukrainian].
7. Polovenko L. P. & Merinova S. V. (2019). Vyiavlennia oznak sotsialnoi inzhenerii ta tekhnolohiia protydii sotsialnym khakeram na pidpryiemstvi [Identifying signs of social engineering and technology to counter social hackers in the enterprise]. *Pidpryiemnytstvo ta innovatsii.* №10. Pp. 183-187. https://doi.org/10.37320/2415-3583/10.28 [in Ukrainian].
8. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy 05 zhovtnia .2017 roku № 2163-VIII [Law of Ukraine on the Basic Principles of Ensuring Cybersecurity in Ukraine from October 5 2017, № 2163-VIII]. (2017, October 5). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].
9. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku «Pro Stratehiiu kiberbezpeky Ukrainy» [On the decision of the National Security and Defense Council of Ukraine of May 14, 2021 “On the Cybersecurity Strategy of Ukraine”]: Ukaz Prezydenta Ukrainy vid 26 serpnia 2021 roku № 447/2021. Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#Text [in Ukrainian].

Received 20.04.2026.
Accepted 24.04.2026.
Published 30.04.2026

Youth cyberhygiene on social platforms: from analysis of aitm attacks to models of safe behavior

Abstract. This article presents a comprehensive study of the risks faced by young people in today’s social media environments. The relevance of the study stems from the rapid development of social engineering methods, which are predominantly based on psychological manipulation. A classification of social networks by user age groups is presented, which has enabled the identification of priority attack vectors for each platform. Based on an empirical survey, critical gaps in young people’s digital literacy have been identified: it was found that a significant proportion of respondents are vulnerable to Adversary-in-the-Middle (AiTM) attacks due to an inability to recognise fake domains, as well as ignoring the absence of data encryption protocols. The mechanics of session token interception and subsequent account takeover have been analysed in detail.

The practical significance of the study lies in the development of a three-tier protection model, which includes system-wide, platform-specific (Telegram, Instagram, TikTok) and network-related (Wi-Fi security) recommendations. The proposed educational and behavioural approach shifts the focus from purely technical protection measures to fostering active digital resilience in users.

Keywords: social engineering, social networks, cyber hygiene, AiTM (Adversary-in-the-Middle) attack, account takeover, phishing, user vulnerability, digital resilience.

Лучик Світлана Дмитрівна - професорка кафедри інформаційних систем та технологій Харківського національного університету внутрішніх справ, доктор економічних наук, професор.
ORCID: http://orcid.org/0000-0003-0757-1140
Мудрицький Ігор Володимирович - курсант Харківського національного університету внутрішніх справ.
ORCID: http://orcid.org/0009-0005-9105-0648
Мойко Олександр Олександрович - курсант Харківського національного університету внутрішніх справ.
ORCID: http://orcid.org/0009-0000-3828-6196
Стецик Роман Мирославович - курсант Харківського національного університету внутрішніх справ.
ORCID: http://orcid.org/0009-0009-1263-184X

Luchyk Svitlana Dmytrivna − Professor of the Department of Information Systems and Technologies of the Kharkiv National University of Internal Affairs, Doctor of Economic Sciences, Professor.
ORCID: http://orcid.org/0000-0003-0757-1140
Mudrytskyi Ihor Volodymyrovych − Cadet of the Kharkiv National University of Internal Affairs.
ORCID: http://orcid.org/0009-0005-9105-0648
Moiko Oleksandr Oleksandrovych − Cadet of the Kharkiv National University of Internal Affairs.
ORCID: http://orcid.org/0009-0000-3828-6196
Stetsyk Roman Myroslavovich − Cadet of the Kharkiv National University of Internal Affairs.
ORCID: http://orcid.org/0009-0009-1263-184X

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)