

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ



ОСОБИСТІСТЬ ТА СУСПІЛЬСТВО В ЦИФРОВУ ЕРУ: ПСИХОЛОГІЧНИЙ ВИМІР

МАТЕРІАЛИ V МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

16 квітня 2025 року

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»**

**Факультет психології, політології та соціології
Кафедра психології**

*V МІЖНАРОДНА
НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ*

**«ОСОБИСТІСТЬ ТА СУСПІЛЬСТВО В ЦИФРОВУ
ЕРУ: ПСИХОЛОГІЧНИЙ ВИМІР»**

16 квітня 2025 року

Одеса – 2025

Редакційна колегія:

Відповідальний редактор – **Аракелян М.Р.**, доктор юридичних наук, професор, проректор з наукової роботи Національного університету «Одеська юридична академія», заслужений юрист України.

Члени редколегії:

Цільмак О.М. – доктор юридичних наук, професор, завідувачка кафедри психології Національного університету «Одеська юридична академія»;

Татьянчиков А.О. – кандидат психологічних наук, доцент, доцент кафедри психології Національного університету «Одеська юридична академія»;

Шмаленко Ю.І. – кандидат політичних наук, доцент, доцент кафедри психології Національного університету «Одеська юридична академія»;

Лісовенко А.Ф. – кандидат психологічних наук, доцент, доцент кафедри психології Національного університету «Одеська юридична академія»;

Ташматов В.А. – кандидат психологічних наук, доцент, доцент кафедри психології Національного університету «Одеська юридична академія».

Матеріали представлені в авторській редакції. Редакційна колегія не несе відповідальності за їх зміст.

Особистість та суспільство в цифрову еру: психологічний вимір : матеріали V міжнарод. наук.-практ. конф. (м. Одеса, 16 квітня 2025 року) / за заг. ред. проф. Аракеляна М.Р. Одеса : Національний університет «Одеська юридична академія», 2025. 160 с.

Суворова Анастасія Дмитрівна ВПЛИВ АРТ-ТЕРАПІЇ НА ЕМОЦІЙНИЙ СТАН ДІТЕЙ-ПЕРЕСЕЛЕНЦІВ..	130
Татьянчиков Андрій Олександрович, Булгакова Дарія Павлівна ВПЛИВ КІБЕРПРОСТОРУ НА ЕМОЦІЙНУ СФЕРУ ПІДЛІТКІВ.....	132
Ташматов Вячеслав Абдуллайович, Душина Анна Павлівна СТРЕС ЯК ДЕТЕРМІНАНТА РОЗВИТКУ ХІМІЧНОЇ ТА НЕХІМІЧНОЇ АДИКЦІЇ: КЛІНІКО-ПСИХОЛОГІЧНИЙ АСПЕКТ.....	135
Ташматов Вячеслав Абдуллайович, Козирь Анна Юріївна ЦИФРОВА МАСКА ОСОБИСТОСТІ: ПСИХОЛОГІЯ САМОПРЕЗЕНТАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ.....	138
Тихонова Ганна Романівна, Кернас Андрій В'ячеславович ІСТОРИЧНІ АСПЕКТИ РОЗВИТКУ НАПРЯМУ ЛОГОТЕРАПІЇ ВІКТОРА ФРАНКЛА.....	141
Тітієвський Віталій Олегович ПСИХОЛОГІЯ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ: ЯК НАВИЧКИ КІБЕРГІГІЄНИ ЗАХИЩАЮТЬ КОРИСТУВАЧА.....	143
Ульяницька Валерія Андріївна РОБОТА З КОМОРБІДНИМИ СТАНАМИ ПРИ РАС.....	146
Ульянов Вадим Олексійович, Степанюк Ярослав Васильович, Федонюк Сергій Валентинович, Поручинський Андрій Іванович ПСИХОЛОГІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ЕЛЕКТРОННОГО НАВЧАННЯ.....	149
Флоря Марія Маргарита Олександрівна ВПЛИВ ЛЕГКОГО ДОФАМІНУ НА ЖИТТЯ МОЛОДІ.....	152
Чернов Олександр Віталійович ВПЛИВ ПСИХІЧНИХ РОЗЛАДІВ НА КРИМІНАЛЬНУ ПОВЕДІНКУ	154
Шевченко Дар'я Ярославівна СВІДОМИЙ ВИБІР ПРОФЕСІЙНОГО ШЛЯХУ: ПСИХОЛОГІЧНІ ЧИННИКИ ТА ВПЛИВ ЦІННІСНИХ ОРІЄНТАЦІЙ.....	157

Список використаних джерел

1. Рубан А. Філософський аналіз «логотерапії» Віктора Франкла : магістерська робота : спец. 033 «Філософія» ; Нац. ун-т «Києво-Могилянська академія». Київ, 2021. 72 с.
2. Соломаха А.В. Логотерапія Віктора Франкла : магістерська кваліфікаційна робота. 2024.
3. Франкл В. Лікар та душа. Основи логотерапії. / 2-ге вид., доповн. Харків : Клуб сімейного дозвілля, 2021. 320 с.
4. Каріков С.А. Логотерапія Віктора Франкла в теоретичному та практичному контексті соціальної роботи : дис. канд. соціол. наук. 2023.
5. Запорожченко, О. Е. Екзистенційні виміри логотерапії В. Франкла *Сучасна психологія: проблеми та перспективи*. Ізмаїл : РВВ ІДГУ, 2020. С. 77-80.

Ключові слова: логотерапія, історичні аспекти розвитку, Віктор Франкл.

Key words: logotherapy, historical aspects of development, Viktor Frankl.

Тітієвський Віталій Олегович

*здобувач I курсу магістратури факультету адвокатури
та антикорупційної діяльності*

Національний університет «Одеська юридична академія»

Науковий керівник: кандидат юридичних наук, доцент Геращенко О.С.

ПСИХОЛОГІЯ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ: ЯК НАВИЧКИ КІБЕРГІГІЄНИ ЗАХИЩАЮТЬ КОРИСТУВАЧА

У сучасному цифровому середовищі, де інформаційні потоки охоплюють усі сфери життя від особистої комунікації до фінансових операцій, значення безпечної взаємодії у кіберпросторі постійно зростає. Людина стає не лише користувачем технологій, а й потенційною мішенню кіберзлочинності, яка дедалі частіше спрямована не на злам технічних систем, а на використання психологічної вразливості. Саме на цьому ґрунті зростає популярність так званих соціоінженерних атак, у яких основний об'єкт впливу – психіка користувача [1]. Зловмисники, використовуючи маніпулятивні прийоми, змушують людину самостійно надавати доступ до конфіденційної інформації, відкривати шкідливі посилання або встановлювати небезпечне програмне забезпечення. У зв'язку з цим, формування навичок кібергігієни як системи звичок і правил безпечної цифрової поведінки є надзвичайно актуальним. Адже саме поєднання технічної обізнаності з психологічною стійкістю формує здатність користувача чинити опір атакам соціальної інженерії.

Згідно з опитуванням, у 2021 році 83% респондентів зазначили, що їхня організація стала жертвою принаймні однієї успішної фішингової атаки через електронну пошту, що на 4,6% більше порівняно з 2020 роком. Крім того, 78%

організацій повідомили про випадки атак із використанням програм-вимагачів, які також здійснювалися електронною поштою [2].

Проблема полягає в тому, що більшість користувачів, навіть добре обізнаних у базових принципах інформаційної безпеки, не усвідомлюють характеру соціоінженерних загроз, оскільки вони не супроводжуються «технічними» ознаками злому. Наприклад, фішинг, як найпоширеніша форма соціальної інженерії, базується на копіюванні зовнішнього вигляду знайомих ресурсів: банків, поштових служб, державних платформ, із метою викликати довіру й спонукати користувача до дії – натиснути посилання, ввести пароль чи оплатити послугу. Такі атаки часто мають високий рівень персоналізації, що посилює ефект достовірності. Іншими формами є вішинг – телефонні дзвінки від «працівників служби безпеки», які просять підтвердити дані; смишинг – фішинг через SMS-повідомлення; бейтинг – залишення заражених флеш-носіїв у публічних місцях із провокативними мітками [3]. У всіх випадках на перший план виходить емоційна реакція: терміновість, страх, цікавість, почуття провини або довіри до авторитету. Згідно з психологічними дослідженнями, люди у стані стресу або поспіху частіше погоджуються на дії, які у спокійних умовах здалися б підозрілими. Таким чином, соціальна інженерія експлуатує базові когнітивні механізми, що ускладнює її виявлення та протидію.

Додаткову складність становить те, що навіть після впровадження технічного захисту – антивірусів, міжмережевих екранів, VPN-з'єднань – користувач залишається вразливим, якщо він самостійно передає доступ до своїх облікових записів. Проблема поглиблюється загальною цифровою неграмотністю, відсутністю освіти з кібергігієни у більшості навчальних закладів, а також недооцінкою психологічного чинника в моделюванні інформаційної безпеки. Особливо вразливою є категорія людей похилого віку, підлітків і працівників установ, які не проходили спеціального навчання або симуляцій атак. Кіберзлочинці дедалі активніше використовують соціальні мережі для збирання персональних даних, на основі яких формуються індивідуальні сценарії впливу, зокрема ті, що апелюють до особистих емоційних зв'язків, інтересів чи цінностей. У корпоративному середовищі це може призводити до витoku внутрішньої інформації, фінансових втрат або пошкодження репутації компанії, що особливо небезпечно у сфері охорони здоров'я, фінансів і державного управління.

Усвідомлення загроз соціальної інженерії вимагає зміни парадигми захисту: з технократичної моделі – до поведінкової. Основним рішенням виступає впровадження системи кібергігієнічної освіти, яка повинна стати частиною як загального навчального процесу, так і безперервного професійного розвитку працівників. Важливо, щоб знання не обмежувалися лише теорією, а мали практичне втілення через тренінги, симуляції атак, розбір кейсів та індивідуальну оцінку ризиків. Формування таких навичок, як розпізнавання фішингових повідомлень, верифікація цифрових підписів, перевірка автентичності сайтів, шифрування персональних файлів та застосування багатофакторної автентифікації, має відбуватися систематично. Особливу увагу слід приділяти розвитку критичного мислення, стресостійкості, навичок уповільнення реакції у кризових ситуаціях, що прямо впливає на здатність протистояти психологічному впливу.

Крім того, доцільно розробляти візуальні пам'ятки, інструкції з безпеки, онлайн-платформи для самостійного навчання, що зробить знання доступнішими широкому колу користувачів.

Організації мають формувати внутрішню політику поведінкової безпеки, яка б включала аналіз інцидентів, аудит обізнаності персоналу, регулярні оцінювання ризиків і оновлення сценаріїв реагування. Ефективності набувають «тестові атаки» без попередження, за результатами яких працівники отримують персоналізований зворотний зв'язок. У державному секторі ключовим завданням має стати створення інтегрованої стратегії національної цифрової обізнаності, яка включатиме інтерактивні кампанії, онлайн-курси, співпрацю з закладами освіти та приватним сектором. На міжнародному рівні вже діють подібні ініціативи, наприклад, «Cyber Aware» у Великій Британії чи кампанії Європейського агентства з кібербезпеки (ENISA), які можуть бути адаптовані в українських реаліях.

Таким чином, ефективна протидія соціальній інженерії можлива лише за умови гармонійного поєднання технічних рішень із розвитком поведінкової компетентності користувачів. Кібергігієна перестає бути суто технічною дисципліною – вона набуває психологічного й соціального виміру, охоплюючи знання, навички, мотивацію та культуру безпеки. Тільки системний підхід до цифрової освіти, що враховує особливості сприйняття інформації, емоційні реакції та звички людей, дозволить зменшити вразливість до соціоінженерних атак і забезпечити стійкість як окремих користувачів, так і суспільства загалом у новому цифровому середовищі.

Список використаних джерел

1. What is social engineering?. URL: <https://www.ibm.com/think/topics/social-engineering> (дата звернення: 12.04.2025)
2. Proofpoint State of the Phish 2022 Report Released. URL: <https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-2022-state-phish-report-reveals-email-based-attacks-dominated> (дата звернення: 12.04.2025)
3. 7 Types of Social Engineering Attacks Targeting You. URL: <https://www.securityhq.com/blog/7-types-of-social-engineering-attacks-targeting-you/> (дата звернення: 12.04.2025)

Ключові слова: соціальна інженерія, кібергігієна, фішинг, кіберзагрози, інформаційна безпека.

Key words: social engineering, cyber hygiene, phishing, cyber threats, information security.