Наприклад, результати дослідження про дитину повідомляються батькам (це лише необхідна інформація, де обов'язково наголошується на компенсаторних можливостях і позитивних якостях). Якщо діагностичні висновки анонсуються через третю особу, то необхідно оцінити її здатність не тільки декодувати їх, але й достовірно передати (не варто повідомляти телефоном або через некомпетентних осіб; ймовірно важливо утриматися, якщо такі дані лише частково висвітлюють проблематику, є відповідні сумніви про їхній зміст тощо).

*Висновки:* 1. Об'єктивна інтерпретація теоретико-емпіричної інформації про досліджуване явище є вирішальною умовою розроблення його структурно-функціонального змісту. 2. Дотримання етичних норм, повага до людини, доказовий (валідний, перевірений, результативний) дослідницький інструментарій і аналогічна інтерпретація постають у психолога-діагноста одними з головних (маркерних) показників професійної компетентності.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ


1. Гарець Н. О. Психодіагностика : навчальний посібник / Н. О. Гарець. Дніпро : ДГУ, 2025. 144 с.
2. Панчук Н. Психологічна діагностика професійної придатності фахівця / Н. Панчук. К. : SBA Print, 2026. 142 с.
3. Поліщук В. М. Віковий кризовий розвиток людини від дня народження до дорослості / В. М. Поліщук. Суми : ПФ «Видавництво «Університетська книга», 2025. 459 с.
4. Поліщук С. А. Методичний довідник з психодіагностики / С. А. Поліщук. Суми : Університетська книга, 2026. 454 с.
5. Шванцара Й. і колектив авторів. Діагностика психічного розвитку / Й. Шванцара і колектив авторів. Прага : Авіценум, 1978. 387 с.



**УДК 159.9:004.056**



**Примак Юлія Володимирівна,**
кандидатка психологічних наук, доцентка, доцентка кафедри загальної, вікової та соціальної психології Національного університету «Чернігівський колегіум» імені Т. Г. Шевченка, м. Чернігів;

**Примак Валерія Вячеславівна**,
здобувачка спеціальності «Кібербезпека та захист інформації» Національного університету «Чернігівська Політехніка», м. Чернігів

# ДОВІРА ЯК ПСИХОЛОГІЧНИЙ ЧИННИК КІБЕРБЕЗПЕЧНОЇ ПОВЕДІНКИ ОСОБИСТОСТІ

Довіра – значущий психологічний чинник кібербезпечної поведінки особистості в умовах сучасного цифрового середовища. Нині особливо важливо змістити акцент із переважно технічного розуміння кібербезпеки на психологічний аналіз поведінки людини, оскільки значна частина кіберзагроз реалізується через маніпулювання когнітивними, емоційними та соціальними механізмами особистості. Саме довіра увиразнюється в її особливій ролі у сприйманні віртуального простору, оцінюванні інформації, прийнятті рішень та формуванні безпечної або ризикованої кіберповедінки. Сьогодні дедалі частіше спостерігається феномен надмірної довіри до цифрових технологій, так званих авторитетних джерел, знайомих комунікаторів та автоматизованих систем. Водночас довіра може мати амбівалентний характер: з одного боку, вона забезпечує комфортну взаємодію людини з цифровим середовищем, а з іншого – за недостатньої критичності може підвищувати вразливість до фішингу, соціальної інженерії, шахрайства та інших форм кіберманіпуляції.

Стрімка цифровізація суспільства спричинила істотне розширення простору повсякденної взаємодії людини з цифровими технологіями. Спілкування, навчання, професійна діяльність, фінансові операції, отримання адміністративних та медичних послуг дедалі частіше відбуваються саме у діджитал-просторі. Водночас розширення цифрових можливостей супроводжується зростанням кількості та складності кіберзагроз, серед яких особливе місце посідають ті, що безпосередньо спрямовані на психологічні механізми регуляції поведінки людини.

Сучасна людина дедалі виразніше розглядається не лише як користувач захищеної системи, а й як активний суб’єкт, поведінка якого може як

підвищувати, так і знижувати рівень безпеки. Систематичний огляд досліджень людської кіберповедінки показав, що основними предметами такого аналізу ставали поведінкові наміри та власне кібербезпечна поведінка, а серед теоретичних основ особливе місце – теорія запланованої поведінки та теорія мотивації захисту (I. Ajzen, M. Fishbein, R. W. Rogers) [2]. Особливої актуальності в цьому контексті набув феномен довіри. У повсякденному житті вона є необхідною умовою соціальної взаємодії, оскільки дозволяє людині зменшувати когнітивне навантаження, швидше приймати рішення та взаємодіяти з іншими без постійної перевірки кожного повідомлення чи дії. Однак у цифровому середовищі саме ця психологічна властивість може ставати об’єктом цілеспрямованого маніпулятивного впливу.

Соціальна інженерія, фішинг та інші форми кібершахрайства часто ґрунтуються не на подоланні технічного захисту, а на створенні у людини хибного відчуття достовірності, безпеки або авторитетності джерела. Дослідження психології фішингових повідомлень (A. Acquisti, R. Dhamija, M. Hearst, P. J. Hills, P. Kumaraguru, J. McAlaney, J. D. Tygar), зокрема, демонструють значення характеристики як-от сприймання надійності повідомлення, терміновість, загрозливе формулювання та інші особливості, що впливають на процес його когнітивної обробки.

Довіра не є тотожною безумовній впевненості. Вона передбачає певний рівень невизначеності та готовність особистості діяти за відсутності повної інформації. Саме ця властивість робить довіру принципово важливою для цифрового середовища. Користувач практично ніколи не володіє повною інформацією про реального автора повідомлення, справжність вебресурсу, безпечність цифрового сервісу або алгоритм функціонування автоматизованої системи. Тому значна частина цифрової поведінки ґрунтується на психологічних припущеннях. У цьому сенсі довіра виконує адаптивну функцію. Вона дозволяє економити когнітивні ресурси, спрощує прийняття рішень і робить можливим ефективне користування складними цифровими системами. Проблема виникає тоді, коли рівень довіри не

відповідає реальному рівню надійності об’єкта. Отже, для психології кібербезпеки принциповим є розмежування обґрунтованої та надмірної довіри.

Одним із стрижневих механізмів зв’язку між довірою та кібербезпекою може бути сприймання ризику. Людина, яка довіряє певному цифровому ресурсу або комунікатору, може суб’єктивно оцінювати ситуацію як менш небезпечну. Відповідно, зменшується потреба в додатковій перевірці інформації. Відтак довіра потенційно впливає на кібербезпеку не безпосередньо, а через суб’єктивну оцінку ситуації та вибір поведінкової стратегії (йдеться про зниження сприймання загрози на суб’єктивному рівні, зменшення критичної перевеліки, швидке прийняття рішення).

Водночас цей механізм не слід трактувати однозначно. Високий рівень довіри до надійних джерел може навпаки засвідчити кібербезпечну поведінку, оскільки людина швидше користується рекомендаціями фахівців, дотримується правил захисту та використовує перевірені цифрові ресурси. Відтак важливим психологічним індикатором є не просто рівень довіри, а адекватність її прояву в певній ситуації. Так, надмірна довіра може поставати як психологічна вразливість. Зокрема може йтися про електронні повідомлення від нібито знайомих осіб; сайтів, що мають ознаки офіційності; цифрових сервісів; автоматизованих систем захисту; рекомендацій алгоритмів; повідомлень із використанням авторитетної символіки; контенту, створеного завдяки штучному інтелекту. Саме останній дозволив генерувати дедалі переконливіші тексти, зображення, голосові повідомлення та відео [1]. Сучасні психологічні дослідження (Glikson, Woolley; Kaplan et al.; Li et al.; Everett et al.) довіри до штучного інтелекту наголошують на необхідності розмежування довіри, сприйнятої надійності та власне довірливої поведінки.

Також виразно психологічне значення довіри проявилося у соціальній інженерії. Остання передбачає використання психологічних механізмів для того, щоб спонукати людину до дії, яка підвищує ризик для її інформаційної або цифрової безпеки. У цьому разі зловмисник намагається не так «зламати»

систему, як сформувати необхідну психологічну ситуацію, в якій сама людина виконає потрібну дію. У цьому процесі можуть використовуватися: авторитет, соціальна подібність, знайомство, почуття терміновості, страх, винагорода, інтерес, дефіцит часу, емоційне напруження. Отож психологічна вразливість до соціальної інженерії може бути пов'язана з тим, наскільки швидко людина переходить від сприймання повідомлення до довіри й дії. Важливо, що така поведінка не обов'язково свідчить про низький рівень інтелекту або недостатню цифрову грамотність. Навпаки, навіть компетентна людина може прийняти небезпечне рішення в ситуації високого емоційного навантаження, виснаження, дефіциту часу або сильного авторитетного впливу.

Психологічний аналіз кібербезпечної поведінки потребує і врахування когнітивних механізмів прийняття рішень. Ідеться про ситуації, в яких людина не перевіряє кожен цифровий сигнал шляхом повного раціонального аналізу. У повсякденному житті вона використовує когнітивні скорочення – евристики, що дозволяють швидко оцінювати інформацію. Такі механізми є адаптивними, однак можуть використовуватися зловмисниками. Саме тому психологічний захист від кіберзагроз має передбачати не лише інформування про існування фішингу чи шахрайства, а й формування навичок уповільнення автоматичного рішення, перевірки джерела та усвідомлення власних емоційних реакцій. Водночас на кожному етапі можуть діяти модератори: цифрова грамотність, критичне мислення, досвід попереднього користування цифровими сервісами, емоційний стан, тривожність, психологічна стійкість, схильність до ризику та попередній досвід кіберінцидентів. Тому перспективною є не лінійна модель «довіра → небезпечна поведінка», а складніша модель, у якій довіра взаємодіє з певними психологічними характеристиками особистості. Зокрема психологічна стійкість здатна підвищувати здатність особистості призупиняти автоматичну довірливу реакцію в умовах кіберзагрози.

Отже, проблема кібербезпеки особистості не може бути повною мірою розкрита лише в межах технічного підходу. Людина є активним суб'єктом цифрової взаємодії, а її психологічні характеристики значною мірою окреслюють характер реагування на кіберзагрози. Довіра є одним із важливих психологічних феноменів, що визначають взаємодію особистості з цифровим середовищем. Вона виконує адаптивну функцію, полегшуючи орієнтацію в умовах інформаційної складності та невизначеності. Заразом надмірність або некритичність довіри може ставати психологічною вразливістю, яка використовується у фішингу, соціальній інженерії, цифровому шахрайстві та маніпулятивній комунікації. Тому надважливим завданням стає формування кібербезпечної поведінки: здоровий скептицизм (перехід до презумпції недовіри у віртуальному просторі), критична перевірка (звичка перевіряти адреси сайтів, каналів зв'язку та не піддаватися на штучну терміновість), цифрова гігієна (регулярне навчання та усвідомлення психологічних тригерів, які використовують кіберзлочинці).

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Everett J. A. C., Claessens S., Knöchel T.-D., et al. Principles for understanding trust in artificial intelligence. *Nature Reviews Psychology*. 2026. №5. P. 388–401.

2. Fabrykant M. S. Psychological Factors of Cybersecurity and Trust in Fake News in Internet Communication: Review of Contemporary Foreign Studies. *Journal of Modern Foreign Psychology*. 2024. № 13(4). P. 163–171.

**УДК 373.2**

**Пугачова Марія Олександрівна,**
здобувачка першого (бакалаврського) рівня вищої освіти спеціальності А2 Дошкільна освіта Глухівського НПУ імені Олександра Довженка, м. Глухів;
***Науковий керівник:***
**Тітаренко Світлана Анатоліївна,**
кандидат педагогічних наук, доцент кафедри дошкільної педагогіки і психології Глухівського національного педагогічного університету імені Олександра Довженка, м. Глухів