УДК 316.614:004.9

СПРИЙНЯТТЯ РИЗИКУ В ОНЛАЙН-СЕРЕДОВИЩІ ТА ЙОГО ВПЛИВ НА БЕЗПЕЧНУ ПОВЕДІНКУ КОРИСТУВАЧІВ

Леонова А.О.
e-mail: anna.leonova@nure.ua
Харківський національний університет радіоелектроніки, каф. СГН
м. Харків, Україна

The digital environment has become a natural space for communication, learning and everyday activities. However, the way users perceive risk online often differs from their perception of danger in real life. Understanding this difference is essential for explaining why people sometimes behave less cautiously in cyberspace. Risk perception in the digital environment is influenced not only by knowledge about cybersecurity but also by psychological factors such as trust, habits and previous online experience. As a result, users may underestimate potential threats or perceive them as unlikely to affect them personally.

У сучасному суспільстві використання інтернету стало звичною частиною повсякденного життя. Більшість користувачів щодня взаємодіє з онлайн-платформами, соціальними мережами та цифровими сервісами, не завжди замислюючись над потенційними ризиками. Проте, саме спосіб, у який люди сприймають небезпеку в інтернеті, значною мірою визначає їхню поведінку. У багатьох випадках проблема полягає не в нестачі інформації про кіберзагрози, а в особливостях психологічного сприйняття цих загроз. Дослідження в галузі кіберпсихології показують, що люди оцінюють ризики в цифровому середовищі інакше, ніж у реальному світі [1]. Онлайн-простір створює відчуття певної дистанції між користувачем і потенційною небезпекою. Багато дій у мережі здаються безпечними лише тому, що вони не мають безпосередніх негативних наслідків у момент їх виконання. Саме ця відкладеність наслідків формує ілюзію безпеки. У результаті користувач може легко поділитися особистими даними, перейти за невідомим посиланням або довіритися сумнівному джерелу інформації.

Зазвичай користувачі усвідомлюють існування кіберризиків, але сприймають їх досить абстрактно. Дослідження свідчать, що багато людей визнають небезпеку певних онлайн-активностей, однак не пов’язують ці ризики зі своєю власною поведінкою [2]. Така психологічна дистанція призводить до своєрідного парадоксу: користувач може знати про кіберзагрози, але все одно діяти необережно. Це свідчить про те, що сам факт інформування про небезпеку не завжди змінює поведінку людини.

Важливу роль у цьому процесі відіграють звички користування інтернетом. Чим частіше людина виконує певні дії онлайн, тим менш ризикованими вони починають їй здаватися. Наприклад, регулярна взаємодія з цифровими сервісами формує відчуття впевненості у власній

компетентності. Дослідження показують, що надмірна впевненість у власних цифрових навичках може навіть збільшувати вразливість користувачів до онлайн-шахрайства [3, 4]. Людина починає вважати себе достатньо обізнаною і перестає перевіряти інформацію або оцінювати потенційні ризики.

З точки зору аналізу поведінки, це явище можна пояснити тим, що інтернет створює середовище швидких рішень. Користувачі постійно взаємодіють із великою кількістю інформації, повідомлень та цифрових стимулів. У таких умовах рішення часто приймаються автоматично, без глибокого аналізу. Саме цим активно користуються кіберзлочинці, створюючи ситуації, які викликають довіру, поспіх або емоційний тиск. У результаті поведінка користувачів визначається не стільки раціональним оцінюванням ризику, скільки психологічними реакціями.

Наслідки такого сприйняття ризику можуть бути досить серйозними. Небезпечна поведінка в інтернеті може призводити до втрати персональних даних, фінансових збитків або інших негативних наслідків. Проте, більш важливим є те, що подібні ситуації часто формують нові поведінкові моделі. Користувачі або починають більш обережно ставитися до цифрового середовища, або навпаки продовжують ризиковану поведінку, якщо негативні наслідки не є очевидними.

Отже, сприйняття ризику в онлайн-середовищі є складним психологічним процесом, який безпосередньо впливає на поведінку користувачів. Аналіз цього явища показує, що підвищення цифрової безпеки потребує не лише технічних знань, але й розуміння психологічних механізмів, що визначають прийняття рішень у мережі. Саме поєднання технологічних і психологічних підходів може сприяти формуванню більш усвідомленої та безпечної поведінки користувачів у цифровому середовищі.

Список використаних джерел:

1. Attrill-Smith A., Fullwood C., Keep M., Kuss D. J. (ред.). The Oxford Handbook of Cyberpsychology. Oxford: Oxford University Press, 2019.
2. Carcelén-García S., Díaz-Bustamante Ventisca M., Galmes-Cerezo M. Young People's Perception of the Danger of Risky Online Activities: Behaviours, Emotions and Attitudes Associated with Their Digital Vulnerability. Social Sciences. 2023. Vol. 12(3). DOI: 10.3390/socsci12030164.
3. Balakrishnan V., Ahhmed U., Basheer F. Personal, Environmental and Behavioral Predictors Associated with Online Fraud Victimization among Adults. PLOS ONE. 2025. DOI: 10.1371/journal.pone.0317232.
4. Дашенкова Н.М., Коробкіна Т.В., Митцева О.С. Когнітивна відкритість і педагогіка гідності: освіта поза межами тоталітаризму // Суспільство та національні інтереси. № 5 (13). 2025. С.100-110. DOI 10.52058/3041-1572-2025-5(13)-100-110