СЕКЦІЯ
«Психологія бізнесу та управління в динамічному просторі сучасності»

УДК 159.9

ПСИХОЛОГІЧНІ ЧИННИКИ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ В УМОВАХ КІБЕРРИЗИКІВ ТА ЦИФРОВОЇ НЕВИЗНАЧЕНОСТІ

Василь ВИШНЬОВСЬКИЙ **Володимир ВИШНЬОВСЬКИЙ**
Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, Україна

У сучасному цифровому середовищі управлінські рішення дедалі більше залежать від людських чинників, які визначають якість реагування на кіберінциденти, стратегії забезпечення кіберзахисту та вибудовування системи управління ризиками. Зростання складності цифрової інфраструктури, інтенсифікація кібератак, постійна поява нових векторів загроз і високий рівень невизначеності трансформують не лише технологічні, а й психологічні виміри управлінської діяльності. Прийняття рішень у таких умовах відбувається на перетині емоційних реакцій, когнітивних упереджень, організаційної культури та суб'єктивної оцінки ризику, що зумовлює необхідність глибшого вивчення психології управління в кіберсфері. Кіберризики суттєво відрізняються від традиційних, оскільки вони поєднують високий рівень прихованості, мінливості та асиметрії інформації. Керівники часто змушені ухвалювати рішення в умовах браку достовірних даних, неповної або суперечливої інформації про інцидент, одночасного тиску часу та значних потенційних наслідків. Відповідно, психологічні механізми, які зазвичай лише частково впливають на процес управління, у сфері кібербезпеки стають ключовими й можуть або посилювати ефективність реагування, або істотно погіршувати його. Значну роль відіграють когнітивні упередження, серед яких одним із найпоширеніших є упередження надмірної впевненості. Воно проявляється тоді, коли менеджер вважає системи захисту достатньо надійними, недооцінюючи потенційні слабкі місця інфраструктури. У поєднанні з ефектом доступності, коли рішення ґрунтуються на найбільш помітних або нещодавніх подіях, це може призводити до хибних управлінських стратегій, розподілу ресурсів і неправильних пріоритетів. Ефект якоря також впливає на прийняття рішень, адже перше припущення чи гіпотеза щодо джерела атаки або її серйозності здатна визначити подальший хід реагування навіть після отримання нових даних. Такі закономірності описані у відомих працях Д. Канемана і А. Тверскі, а також підтверджені у пізніших дослідженнях психології ризику [5].

Важливою складовою процесу прийняття управлінських рішень у цифровому середовищі є емоційний чинник. Страх, напруга, невпевненість або, навпаки, надмірний оптимізм здатні суттєво змінювати поведінкові реакції керівників. У ситуаціях гострих кіберінцидентів емоційний стан часто визначає швидкість і обережність дій. Наприклад, під впливом тривоги може виникнути тенденція до надмірно консервативних рішень, таких як повне вимкнення критичної інфраструктури без належного аналізу. У той же час заниження рівня загрози може стати наслідком природного бажання мінімізувати стресові переживання. Дослідження емоційно-когнітивної взаємодії в управлінському процесі (Лернер, Валдесоло та ін.) демонструють, що емоції здатні викривляти сприйняття й моделювання ризиків навіть у досвідчених керівників [2]. Не менш суттєвим чинником є вплив соціального та організаційного середовища. Організаційна культура визначає рівень відкритості обміну інформацією, готовність визнавати

помилки, оперативність повідомлення про інциденти та якість взаємодії між підрозділами. За умов недостатньої психологічної безпеки, коли працівники бояться повідомляти про проблеми, навіть незначні кібератаки можуть перетворюватися на масштабні інциденти через затримки в комунікації. Феномен групового мислення, описаний І. Джерісом, створює ризик конформізму, коли колектив прагне уникати протиріч, що знижує ефективність аналізу та критичного мислення під час реагування на загрози [3; 4].

Цифрова невизначеність підсилюється нерівномірністю інформації всередині організації. Інформаційна асиметрія, коли різні підрозділи володіють лише фрагментами даних, ускладнює вибір найбільш раціонального рішення. У контексті кібербезпеки це проявляється у недостатньому обміні технічними деталями між ІТ-командою, менеджментом і суміжними департаментами, що може призвести до помилкових управлінських дій. У таких умовах концепція обмеженої раціональності Герберта Саймона набуває нового звучання, адже керівники змушені діяти швидко, спираючись на неповні дані, що збільшує ймовірність евристичних та інтуїтивних рішень [3; 4]. Управлінські рішення у сфері кіберризиків також значною мірою залежать від рівня довіри до технологій та технічних експертів. Менеджери з технічним бекґраундом частіше демонструють вищий рівень довіри до автоматизованих систем, іноді навіть надмірної, тоді як керівники іншого профілю можуть недооцінювати значення технічних деталей. Це створює додаткову психологічну напругу у процесі міждисциплінарної взаємодії, де важливо поєднувати технічну аналітику з людським фактором, зберігаючи баланс між автоматизацією та експертною оцінкою.

Українські дослідники також активно розвивають напрям психології управління в умовах цифровізації. Зокрема, О. Барановський, С. Пиріг, Н. Побережна, І. Козубцова, О. Криворучко та інші аналізують поведінкові аспекти кібербезпеки, питання довіри в цифровому середовищі, психологічну готовність персоналу до реагування на загрози. Їхні дослідження доповнюють міжнародні підходи, підкреслюючи важливість врахування культурних та організаційних особливостей українських інституцій [2].

Для мінімізації впливу психологічних чинників важливо формувати сталі механізми підтримання якості управлінських рішень у кіберсфері. Значну роль відіграє розвиток сценарного мислення, проведення тренувальних навчань, моделювання кризових ситуацій та застосування практик червоних і синіх команд. Це сприяє формуванню інтуїтивних компетенцій, які особливо важливі під час динамічних кіберінцидентів. Досвід показує, що регулярні практичні вправи знижують рівень панічних реакцій, покращують злагодженість дій і зменшують вплив когнітивних викривлень. Також важливо створювати умови психологічної безпеки, у яких працівники можуть відкрито повідомляти про вразливості та інциденти без страху покарання. Це не лише сприяє своєчасному виявленню загроз, а й формує культуру довіри, необхідну для стійкого функціонування цифрової екосистеми. Культура взаємної підтримки й відкритості стає фундаментом ефективного управління ризиками [1].

Узагальнюючи, можна стверджувати, що психологічні чинники суттєво визначають якість управлінських рішень у цифровому середовищі. Їхнє ігнорування може призвести до системних помилок і посилення вразливостей організації, тоді як інтеграція психологічних підходів у стратегічне планування, побудову процесів кіберзахисту та управління ризиками підсилює кіберстійкість і забезпечує більш раціональні реакції в умовах невизначеності. Додатково, важливо підкреслити, що в умовах ескалації кіберризиків зростає значення управлінської рефлексії як здатності керівника здійснювати критичний аналіз власних дій, рішень та стратегічних припущень. Рефлексивна компетентність дозволяє керівникам своєчасно виявляти помилки, пов’язані з емоційним перенавантаженням, упередженістю або нестачею інформації. У

контексті кібербезпеки рефлексивне мислення виконує роль інструмента самокорекції, що допомагає адаптувати управлінські рішення під впливом нових даних про інцидент, зміну рівня загрози або появу невідомих раніше вразливостей. У цифровому середовищі, де швидкість поширення інформації є критичною, рефлексія сприяє запобіганню імпульсивним реакціям, водночас підсилюючи здатність керівника до стратегічного планування [4].

З іншого боку, вагоме значення має також розвиток цифрової емпатії – здатності розуміти психологічний стан співробітників, які працюють у стресових умовах кіберінцидентів. Постійні повідомлення про нові загрози, необхідність працювати у режимі підвищеної готовності та висока відповідальність за збереження даних можуть спричиняти емоційне виснаження. Менеджери, які враховують психологічний стан команди, здатні ефективніше розподіляти навантаження, запобігати професійному вигоранню та підтримувати стабільний рівень мотивації. Дослідження в українському науковому середовищі доводять, що емоційна підтримка колективу значною мірою визначає адаптивність організації, підвищує її здатність протистояти кіберризикам та сприяє формуванню культури довіри, без якої неможливе ефективне управління ризиками. Додаткову роль відіграють комунікативні механізми, які формують внутрішню інформаційну екосистему організації. Чіткі протоколи обміну інформацією, визначення рівнів доступу, налагоджені канали швидкого сповіщення та механізми зворотного зв'язку забезпечують оперативне реагування на інциденти, мінімізують помилки та знижують рівень невизначеності. Психологічні аспекти комунікації, такі як довіра між підрозділами, готовність ділитися інформацією та уникнення конфліктів, у поєднанні з високим рівнем цифрової грамотності персоналу, створюють синергетичний ефект, що посилює стійкість організації в умовах постійних загроз. У протилежному випадку, коли існує недовіра або страх покарання, комунікаційну систему паралізує приховування інцидентів, що веде до катастрофічних наслідків [3].

У сучасному бізнес-середовищі дедалі важливішими стають інструменти психологічної діагностики, що дозволяють виявляти індивідуальні схильності керівників та співробітників до ризику, стресостійкість, здатність працювати в умовах невизначеності та потенційні зони вразливості. Застосування психометричних методів, оцінювання емоційної регуляції, аналізу стилів мислення дає змогу структурувати управлінські процеси з урахуванням потреб та особливостей персоналу, що підсилює загальну ефективність кіберзахисту. В умовах високої цифрової залежності організацій такі підходи набувають стратегічного значення, оскільки дозволяють створити комплексну систему протидії кіберризикам, у якій людський фактор виступає не вразливістю, а ресурсом розвитку.

Список використаних джерел:

1. Донцов Л. В., Орбан-Лембрик Л. Є., Тищенко Л. В. Комунікації в організації та вплив на управлінські процеси: монографія. Харків: ХНУ, 2019. 368 с.
2. Камінський О. Є. Соціально-психологічна стійкість систем кібербезпеки. *Сучасні проблеми правового, економічного та соціального розвитку держави: матеріали міжнар. наук.-практ. конф.* Київ: НАВС, 2025. С. 45–53. Режим доступу: https://sit.nuou.org.ua/article/download/336863/326606/784723 (дата звернення: 17.11.2025).
3. Лучик С. Д., Бешлей А. В. Психологічні аспекти інформаційної та кібербезпеки. *Матеріали XIII Міжнар. наук.-практ. конф.* Вінниця: ХНУВС, 2024. С. 112–118.
4. Матласевич О. М. Психологічні особливості кібербезпеки: автореферат магістерської роботи. Острог: НаУ «Острозька академія», 2022. 42 с. Режим доступу: https://theses.oa.edu.ua (дата звернення: 17.11.2025).
5. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2023. Athens: ENISA, 2023. 164 p. Режим доступу: https://www.enisa.europa.eu (дата звернення: 17.11.2025).