

УДК 005.334:005.934
JEL: D81; D91; G34; M10
DOI: <https://doi.org/10.32983/2222-4459-2026-8-474-486>

ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ У VUCA СЕРЕДОВИЩІ ЯК ОБ'ЄКТ ПРОАКТИВНОЇ КОРПОРАТИВНОЇ БЕЗПЕКИ: КОНЦЕПТУАЛЬНА МОДЕЛЬ PRISM ЗАПОБІГАННЯ КОРПОРАТИВНОМУ ШАХРАЙСТВУ

© 2026 ГАЙДУКОВ В. І., ГАЙДУКОВ І. В.

УДК 005.334:005.934
JEL: D81; D91; G34; M10

**Гайдуков В. І., Гайдуков І. В. Прийняття управлінських рішень у VUCA середовищі
як об'єкт проактивної корпоративної безпеки: концептуальна модель PRISM запобігання
корпоративному шахрайству**

Статтю присвячено розробленню концептуального підходу до забезпечення проактивної корпоративної безпеки в умовах динамічного, високо-ризикового та неоднозначного VUCA-середовища. На відміну від традиційних моделей Fraud Risk Management та комплаєнс-контролю, які концентруються переважно на виявленні зовнішніх / внутрішніх факторів корпоративного шахрайства та реактивному реагуванні на вже реалізовані загрози, у дослідженні запропоновано розглядати безпосередній процес прийняття управлінських рішень як самостійний об'єкт і «поверхню атаки» для корпоративної безпеки. Обґрунтовано, що високий рівень невизначеності, інформаційного шуму та часового тиску істотно змінює природу управлінських ризиків, деформуючи раціональні моделі вибору та формуючи специфічні когнітивні вразливості (систематичні упередження, евристики, ефекти перевантаження). Доведено, що ці вразливості створюють підґрунтя для цілеспрямованого психологічного й інформаційного впливу, соціальної інженерії та маніпуляцій, які призводять до прихованого викривлення управлінських рішень і реалізації корпоративного шахрайства. На основі міждисциплінарного синтезу концепцій когнітивної психології, поведінкової економіки, динамічних спроможностей (Dynamic Capabilities) та ERM-систем розроблено авторську концептуальну модель PRISM (Proactive Risk Identification through Structural Monitoring). Модель являє собою шестирівневу архітектуру ранньої ідентифікації когнітивних, інформаційних та організаційних спотворень через безперервний структурний моніторинг контексту й процедур прийняття рішень. Ключова відмінність моделі полягає у зміщенні фокусу з контролю дій чи наслідків на систематичну виправну фільтрацію передумов, за яких рішення стає вразливим до зловживань. Запропонований підхід розширює теоретико-методологічні засади проактивного ризик-менеджменту, обґрунтовує необхідність інтеграції когнітивних запобіжників у корпоративне управління та слугує практичним інструментарієм для побудови сучасних комплексних систем запобігання корпоративному шахрайству.

Ключові слова: VUCA; прийняття управлінських рішень; корпоративна безпека; корпоративне шахрайство; Fraud Risk Management; Enterprise Risk Management; когнітивні ризики; PRISM.

Табл.: 1. **Бібл.:** 19.

Гайдуков Володимир Ігорьович – здобувач, Центральнотехнічний національний технічний університет (просп. Університетський, 8, Кропивницький, 25006, Україна)

E-mail: academic.haidukov@gmail.com

ORCID: <https://orcid.org/0009-0002-3495-186X>

Гайдуков Ігор Валентинович – здобувач, Центральнотехнічний національний технічний університет (просп. Університетський, 8, Кропивницький, 25006, Україна)

E-mail: igor.gaidukov@gmail.com

ORCID: <https://orcid.org/0009-0001-8103-5728>

UDC 005.334:005.934
JEL: D81; D91; G34; M10

**Haidukov V. I., Haidukov I. V. Making Managerial Decisions in a VUCA Environment As an Object of Proactive Corporate Security:
The PRISM Conceptual Model For Preventing Corporate Fraud**

The article is devoted to the development of a conceptual approach to ensuring proactive corporate security in a dynamic, high-risk, and ambiguous VUCA environment. Unlike traditional Fraud Risk Management models and compliance frameworks, which primarily focus on identifying external/internal fraud factors and reactively responding to already realized threats, this study proposes considering the managerial decision-making process itself as an independent object and «attack surface» for corporate security. It is substantiated that high levels of uncertainty, information noise, and time pressure significantly alter the nature of managerial risks, distorting rational choice models and forming specific cognitive vulnerabilities (systematic biases, heuristics, cognitive overload effects). It is proved that these vulnerabilities create a foundation for targeted psychological and informational influence, social engineering, and manipulation, leading to the covert distortion of managerial decisions and the execution of corporate fraud. Based on an interdisciplinary synthesis of conceptions from cognitive psychology, behavioral economics, Dynamic Capabilities, and ERM systems, the authors have developed the PRISM (Proactive Risk Identification through Structural Monitoring) conceptual framework. The model presents a six-level architecture for the early identification of cognitive, informational, and organizational distortions through continuous structural monitoring of the decision-making context and procedures. The key difference of this model lies in shifting the focus from controlling actions or outcomes to systematic corrective filtering of the prerequisites under which a decision becomes vulnerable to abuse. The proposed approach expands the theoretical and methodological foundations of proactive risk management, substantiates the necessity of

integrating cognitive safeguards into corporate governance, and serves as a practical toolkit for building modern comprehensive corporate fraud prevention systems.

Keywords: VUCA; managerial decision-making; corporate security; corporate fraud; Fraud Risk Management; Enterprise Risk Management; cognitive risks; PRISM.

Tabl.: 1. Bibl.: 19.

Haidukov Volodymyr I. – Applicant, Central Ukrainian National Technical University (8 Universytetskyi Ave., Kropyvnytskyi, 25006, Ukraine)

E-mail: academic.haidukov@gmail.com

ORCID: <https://orcid.org/0009-0002-3495-186X>

Haidukov Ihor V. – Applicant, Central Ukrainian National Technical University (8 Universytetskyi Ave., Kropyvnytskyi, 25006, Ukraine)

E-mail: igor.gaidukov@gmail.com

ORCID: <https://orcid.org/0009-0001-8103-5728>

ВСТУП

Протягом останнього десятиліття концепція VUCA (Volatility, Uncertainty, Complexity, Ambiguity) остаточно закріпилася як одна з провідних парадигм для опису сучасного бізнес-середовища. Якщо спочатку вона використовувалася переважно для характеристики військово-політичних процесів, то сьогодні активно застосовується в дослідженнях стратегічного менеджменту, організаційної поведінки, управління ризиками та корпоративного управління [2; 15].

Для підприємств функціонування в умовах VUCA означає не лише збільшення кількості зовнішніх ризиків, а й якісну трансформацію самого процесу управління. Скорочення життєвих циклів продукції, цифровізація бізнес-процесів, нестабільність глобальних ланцюгів постачання, розвиток штучного інтелекту та зростання обсягів доступної інформації суттєво підвищують вимоги до швидкості та якості прийняття управлінських рішень. За цих умов саме управлінське рішення дедалі частіше визначає конкурентоспроможність організації значно більшою мірою, ніж окремі виробничі чи фінансові ресурси [16; 18].

Водночас сучасні дослідження свідчать, що прийняття управлінських рішень у ситуаціях високої невизначеності супроводжується істотним зростанням когнітивного навантаження. Обмеженість часу, інформаційна асиметрія, необхідність одночасного аналізу великої кількості взаємопов'язаних факторів та складність прогнозування наслідків призводять до підвищення ймовірності використання евристичних стратегій, формування когнітивних викривлень і погіршення якості управлінських рішень [8; 14].

Паралельно із цим змінюється характер корпоративних загроз. Якщо традиційні моделі корпоративної безпеки концентрувалися переважно на фізичному захисті активів, внутрішньому контролі або виявленні вже вчинених випадків корпоративного шахрайства, то сучасне середовище створює

передумови для використання значно складніших механізмів впливу. Дедалі більшого поширення набувають інформаційні операції, соціальна інженерія, маніпулятивні технології, навмисне викривлення інформаційних потоків та інші способи психологічного впливу, кінцевою метою яких є не безпосереднє викрадення ресурсів, а формування помилкового управлінського рішення [5; 9].

Попри значну кількість досліджень у сфері стратегічного менеджменту, корпоративної безпеки та ризик-менеджменту, взаємозв'язок між прийняттям управлінських рішень у VUCA-середовищі та забезпеченням проактивної корпоративної безпеки досі залишається недостатньо вивченим. Більшість сучасних моделей Enterprise Risk Management розглядає ризики як зовнішні або внутрішні фактори, що можуть вплинути на досягнення стратегічних цілей організації [3; 11]. Водночас когнітивні характеристики самого процесу прийняття управлінських рішень фактично залишаються поза межами системного аналізу.

Подібна ситуація спостерігається й у сфері досліджень корпоративного шахрайства. Класичні моделі, включаючи Fraud Triangle, Fraud Diamond та сучасні концепції Fraud Risk Management, зосереджуються насамперед на мотивації правопорушника, можливостях здійснення шахрайства або організаційних передумовах його реалізації [3; 4]. Проте вони практично не аналізують механізми, через які викривлення процесу прийняття управлінських рішень створюють умови для реалізації шахрайських схем.

На нашу думку, саме процес прийняття управлінських рішень слід розглядати як новий об'єкт проактивної корпоративної безпеки. У VUCA-середовищі він стає своєрідною «поверхнею атаки», на яку можуть спрямувати інформаційні, організаційні та психологічні впливи. У такому випадку корпоративне шахрайство постає не як первинна проблема, а як наслідок попередньої деформації процесу управлінського вибору.

Метою статті є розроблення концептуальної моделі проактивної корпоративної безпеки, що інтегрує механізми захисту процесу прийняття управлінських рішень у VUCA-середовищі та спрямована на запобігання корпоративному шахрайству.

Для досягнення поставленої мети визначено такі завдання:

- ✦ проаналізувати сучасні наукові підходи до прийняття управлінських рішень у VUCA-середовищі;
- ✦ узагальнити сучасні дослідження когнітивних чинників прийняття рішень в умовах невизначеності;
- ✦ дослідити роль психологічного та інформаційного впливу у викривленні управлінських рішень;
- ✦ визначити місце процесу прийняття рішень у системі проактивної корпоративної безпеки;
- ✦ розробити авторську концептуальну модель PRISM, орієнтовану на раннє виявлення структурних вразливостей процесу прийняття управлінських рішень як інструменту запобігання корпоративному шахрайству.

Теоретичні засади прийняття управлінських рішень у VUCA-середовищі

Сучасний розвиток теорії менеджменту характеризується поступовим переходом від дослідження організаційних структур до аналізу процесів, що забезпечують здатність підприємств адаптуватися до швидких змін у зовнішньому середовищі. Якщо в класичних концепціях менеджменту центральними об'єктами дослідження були планування, організація, мотивація та контроль, то сьогодні дедалі більша увага приділяється якості процесу прийняття управлінських рішень як ключовій передумові стратегічної стійкості організації [16].

Подібна трансформація значною мірою пов'язана з поширенням концепції VUCA, яка використовується для характеристики бізнес-середовища, що одночасно характеризується високою мінливістю (Volatility), невизначеністю (Uncertainty), складністю (Complexity) та неоднозначністю (Ambiguity) [2]. Незважаючи на широке використання цієї концепції в сучасній управлінській літературі, її значення нерідко спрощується до загальної характеристики нестабільності. Проте сучасні дослідження демонструють, що кожен із компонентів VUCA по-різному впливає на процес управління, створюючи специфічні виклики для прийняття управлінських рішень [15].

Перший компонент (мінливість (Volatility)) характеризується високою швидкістю змін зовнішнього середовища. Для менеджменту це означає суттєве скорочення часу, доступного для аналізу ситуації та вибору управлінських альтернатив. У результаті менеджери дедалі частіше змушені приймати рішення в умовах дефіциту часу, що підвищує залежність від інтуїтивних суджень та евристичних стратегій. Дослідження стратегічного менеджменту свідчать, що саме часовий тиск є одним із ключових факторів зниження якості стратегічних рішень, особливо в ситуаціях, коли організація одночасно стикається зі швидкими змінами ринкових умов та високою інформаційною невизначеністю [16].

Другий компонент (невизначеність (Uncertainty)) пов'язаний не стільки з відсутністю інформації, скільки з неможливістю достовірно прогнозувати наслідки ухвалених рішень. У сучасних організаціях навіть значні масиви даних не гарантують можливості точного прогнозування майбутніх подій. Як зазначає D. Teece, за умов високої невизначеності, конкурентні переваги дедалі більше визначаються не обсягом інформації, а здатністю керівників правильно її інтерпретувати та швидко адаптувати свої рішення до змін у середовищі [17].

Особливого значення в цьому контексті набуває концепція dynamic capabilities, відповідно до якої стратегічна ефективність підприємства визначається його здатністю інтегрувати, перебудовувати та переорієнтовувати власні ресурси відповідно до змін у зовнішньому середовищі [18]. Важливо, що в межах цієї концепції процес прийняття рішень фактично розглядається як центральний механізм організаційної адаптації. Ця теза підтверджується й новітніми систематичними оглядами: синтез 71 дослідження, присвячений динамічним здібностям підприємств, демонструє, що саме здатність до випереджувального розпізнавання загроз і проактивного управління ризиками, поряд із схильністю до реагування на порушення та гнучкістю ресурсів, визначає здатність організацій підтримувати стійкість у VUCA-середовищі [12]. Це означає, що якість управлінських рішень безпосередньо впливає на здатність підприємства підтримувати конкурентоспроможність у VUCA-середовищі.

Третій компонент (складність (Complexity)) характеризується різким збільшенням кількості взаємозалежних факторів, які необхідно враховувати під час управлінського аналізу. Цифровізація бізнесу, глобалізація ланцюгів постачання, міжгалузева інтеграція та розвиток платформної економіки істотно збільшують кількість взаємозв'язків

між окремими бізнес-процесами. За таких умов навіть локальні управлінські рішення можуть мати непрогнозовані наслідки для всієї організації. Саме складність середовища, а не лише обсяг доступної інформації, формує передумови для когнітивного перевантаження керівників. Дослідження у сфері менеджменту дедалі частіше підтверджують, що надлишок інформації може негативно впливати на якість прийняття рішень не менше, ніж її дефіцит. Зростання кількості показників, альтернатив та сценаріїв розвитку подій ускладнює процес виділення дійсно значущої інформації, що, своєю чергою, підвищує ймовірність помилкових управлінських висновків [14].

Четвертий компонент (неоднозначність (Ambiguity)) є найскладнішим для управлінського аналізу. На відміну від невизначеності, де проблема полягає в недостатності інформації, неоднозначність виникає тоді, коли одна й та сама інформація допускає декілька рівноцінних інтерпретацій. Саме ця особливість сучасного бізнес-середовища істотно підвищує значення управлінського досвіду, професійного судження та колективного аналізу альтернатив. У сучасній літературі з менеджменту дедалі більшого поширення набуває концепція *managerial cognition*, відповідно до якої якість стратегічних рішень визначається не лише доступністю інформації, а й тим, як керівники її сприймають, інтерпретують та інтегрують у власні ментальні моделі [10]. Хоча ця концепція виникла значно раніше, останні дослідження демонструють суттєве зростання її актуальності саме в умовах VUCA, коли процес осмислення інформації стає не менш важливим, ніж її накопичення.

Водночас аналіз сучасної літератури свідчить про наявність певної теоретичної прогалини. Більшість досліджень розглядає прийняття управлінських рішень як індивідуальний когнітивний процес або як елемент стратегічного менеджменту. Значно менше уваги приділяється питанню, яким чином характеристики VUCA-середовища створюють системні когнітивні вразливості в самому процесі прийняття рішень, які потенційно можуть бути використані як інструмент для реалізації корпоративних ризиків.

На нашу думку, саме ця прогалина є принциповою для сучасної теорії менеджменту. Якщо організація функціонує в умовах постійної мінливості, інформаційного перевантаження та високої невизначеності, то процес прийняття управлінських рішень поступово перетворюється на один із найбільш критичних бізнес-процесів підприємства. Відповідно, забезпечення його стійкості має розглядатися не лише як управлінське завдання,

а й як самостійний напрям у забезпеченні корпоративної безпеки.

Саме ця теза є відправною точкою подальшого дослідження. У наступному розділі буде проаналізовано, яким чином когнітивні особливості прийняття рішень у VUCA-середовищі формують нові управлінські ризики та створюють передумови для психологічного впливу й корпоративного шахрайства. Це дозволить перейти від загальної теорії стратегічного менеджменту до побудови авторської концепції проактивної корпоративної безпеки.

Когнітивні ризики прийняття управлінських рішень у VUCA-середовищі як передумова корпоративних загроз

Аналіз сучасних досліджень у сфері стратегічного менеджменту свідчить, що ключовим наслідком функціонування організацій у VUCA-середовищі є не лише підвищення рівня зовнішньої невизначеності, а й істотна трансформація самого процесу прийняття управлінських рішень. Якщо традиційні підходи до ризик-менеджменту концентрувалися переважно на оцінюванні фінансових, операційних або ринкових ризиків, то сучасні дослідження дедалі частіше акцентують увагу на ризиках, пов'язаних із якістю управлінського судження [7; 14].

У цьому контексті доцільно розмежувати поняття когнітивних викривлень (*cognitive biases*) та когнітивних ризиків управлінського процесу. Перше поняття традиційно використовується в психології та поведінковій економіці для позначення систематичних помилок мислення окремої людини [13]. Натомість друге, на нашу думку, має розглядатися як характеристика самого процесу прийняття управлінських рішень, яка виникає внаслідок взаємодії особливостей організаційного середовища, інформаційної архітектури підприємства та когнітивних можливостей осіб, що приймають рішення.

Подібне розмежування є принципово важливим для менеджменту. Організація не здатна повністю усунути індивідуальні когнітивні викривлення своїх працівників. Водночас вона може змінювати архітектуру процесу прийняття рішень, знижуючи ймовірність того, що окремі когнітивні помилки трансформуються в стратегічно значущі управлінські рішення. Показово, що навіть новітні інтегративні огляди організаційної поведінки визнають: попри загальноновизнаний вплив когнітивних викривлень на якість рішень, практичні механізми їх пом'якшення на рівні організацій (а не окремих осіб) залишаються слабко систематизованими й рідко інтегрованими безпосередньо в архі-

тектуру ухвалення рішень [6]. Це підтверджує актуальність розмежування, запропонованого в цій статті.

Саме тому в подальшому під когнітивними ризиками управлінського процесу пропонується розуміти сукупність організаційних, інформаційних та поведінкових факторів, які підвищують імовірність прийняття необґрунтованих або викривлених управлінських рішень в умовах VUCA.

VUCA як джерело когнітивних ризиків

Кожен із компонентів VUCA створює специфічний тип когнітивного навантаження на систему управління.

Volatility (мінливість) скорочує часовий горизонт прийняття рішень. Керівники змушені реагувати швидше, ніж завершуються процедури повноцінного аналізу. У таких умовах організації дедалі частіше використовують спрощені алгоритми прийняття рішень, що дозволяють підтримувати оперативність, але одночасно підвищують ризик поверхневого аналізу альтернатив. Дослідження стратегічного менеджменту демонструють, що саме дефіцит часу є одним із найсуттєвіших чинників погіршення якості управлінських рішень, особливо в кризових ситуаціях [16].

Uncertainty (невизначеність) призводить до інформаційної асиметрії. Керівники змушені приймати рішення за відсутності повної інформації, що закономірно збільшує роль експертних оцінок. Проте саме в цей момент виникає новий управлінський ризик – надмірна залежність від окремих носіїв інформації. Якщо критично важливі дані концентруються в руках обмеженого кола співробітників або зовнішніх консультантів, організація стає більш вразливою до навмисного чи ненавмисного викривлення інформації.

Complexity (складність) характеризується збільшенням кількості взаємозалежних факторів. Для сучасних підприємств це означає, що навіть локальне управлінське рішення може впливати одночасно на виробництво, фінанси, логістику, комплаєнс, інформаційну безпеку та репутацію. За таких умов жоден керівник не здатний самостійно охопити весь масив необхідної інформації. Як наслідок, процес прийняття рішень дедалі більше залежить від якості внутрішніх комунікацій, міжфункціональної взаємодії та інтеграції знань різних підрозділів [17].

Ambiguity (неоднозначність) створює, можливо, найбільш складний виклик для менеджменту. Одна й та сама інформація може мати декілька логічно обґрунтованих інтерпретацій, кожна

з яких здатна привести до різних управлінських рішень. У таких ситуаціях вирішального значення набуває не лише якість інформації, але й спосіб її представлення. Саме тому сучасні дослідження дедалі активніше використовують поняття framing effects, демонструючи, що форма подання інформації може істотно впливати на стратегічний вибір керівників навіть за незмінного фактичного змісту повідомлення [14].

Архітектура процесу прийняття рішень як фактор корпоративної безпеки

Традиційно архітектура процесу прийняття управлінських рішень розглядається як питання організаційного дизайну. Вона визначає порядок підготовки інформації, розподіл відповідальності, процедури погодження та механізми контролю за виконанням рішень. Однак у контексті корпоративної безпеки цей процес набуває принципово іншого значення.

На нашу думку, саме архітектура процесу прийняття рішень визначає ступінь стійкості організації до зовнішніх і внутрішніх маніпулятивних впливів. Якщо процес побудований таким чином, що критично важлива інформація не проходить незалежної перевірки, альтернативні сценарії не аналізуються, а рішення концентруються в руках однієї особи чи вузької групи, то навіть відсутність очевидних порушень системи внутрішнього контролю не гарантує безпеки організації.

У цьому контексті доцільно говорити про когнітивну архітектуру управлінського процесу як про сукупність процедур, механізмів і організаційних практик, що визначають, яким чином інформація перетворюється на управлінське рішення. Саме ця архітектура, на нашу думку, має стати новим об'єктом дослідження в системі проактивної корпоративної безпеки. І саме її стан має безперервно відстежуватися за допомогою структурних індикаторів, а не оцінюватися лише за фактом уже реалізованого порушення.

Від когнітивного ризику до корпоративного шахрайства

Одним із принципових положень цієї статті є твердження, що когнітивний ризик сам по собі ще не означає виникнення корпоративного шахрайства. Він лише створює сприятливі умови для реалізації маніпулятивного впливу.

На відміну від класичних моделей, зокрема Fraud Triangle чи Fraud Diamond, які пояснюють причини виникнення шахрайської поведінки через мотивацію, можливість або раціоналізацію [4], запропонований підхід зміщує фокус аналізу на попередній етап. Питання полягає не лише в тому,

чому людина вчиняє шахрайство, а й у тому, чому організація створює умови, за яких викривлене управлінське рішення стає можливим.

Іншими словами, корпоративне шахрайство часто є завершальним етапом значно довшого процесу. Спочатку формується когнітивна вразливість системи прийняття рішень, потім вона використовується шляхом інформаційного або психологічного впливу, після чого приймається управлінське рішення, що відкриває можливість реалізації шахрайської схеми.

Саме тому сучасна проактивна корпоративна безпека повинна змістити акцент із виявлення вже скоєних порушень на ранню ідентифікацію когнітивних ризиків, що виникають у процесі прийняття управлінських рішень. Такий підхід дозволяє перейти від реактивного управління наслідками до управління причинами виникнення корпоративних загроз.

У наступному розділі буде розглянуто, яким чином психологічний та інформаційний вплив використовує зазначені когнітивні ризики, а також чому саме VUCA-середовище суттєво підвищує ефективність подібних маніпулятивних механізмів. Це стане теоретичною основою для розроблення авторської моделі PRISM, яка інтегрує раннє виявлення вразливостей у процес ухвалення управлінських рішень у системі проактивної корпоративної безпеки.

Психологічний та інформаційний вплив як механізм експлуатації когнітивних вразливостей процесу прийняття управлінських рішень

Проведений аналіз сучасних досліджень дозволяє стверджувати, що самі по собі когнітивні ризики не призводять до корпоративного шахрайства. Вони лише формують середовище, у якому управлінські рішення стають більш чутливими до зовнішнього та внутрішнього впливу. Саме тому наступним логічним етапом дослідження є аналіз механізмів, за допомогою яких ці вразливості можуть бути використані для викривлення процесу прийняття управлінських рішень.

У сучасній науковій літературі дедалі частіше підкреслюється, що інформація перетворилася на один із ключових стратегічних ресурсів організації. Проте не менш важливим є інше положення: об'єктом впливу стає вже не сама інформація, а спосіб її інтерпретації особами, які ухвалюють рішення. За умов VUCA-середовища керівники змушені швидко інтегрувати великі обсяги неоднорідної інформації, що об'єктивно збільшує залежність від когнітивних скорочень, експертних оцінок та організаційної довіри [14].

У результаті психологічний вплив набуває принципово нового значення. Якщо традиційно його розглядали переважно як інструмент міжособистісної взаємодії, то в сучасному менеджменті він дедалі більше використовується як засіб цілеспрямованого викривлення процесу управлінського вибору. При цьому ключовою особливістю є те, що об'єктом впливу є не окрема людина, а весь процес підготовки управлінського рішення.

Від соціальної інженерії до маніпуляції управлінськими рішеннями

Одним із найбільш показових прикладів такого підходу є розвиток технологій соціальної інженерії. Останні дослідження у сфері інформаційної безпеки демонструють, що переважна більшість успішних атак на організації починається не з подолання технічних засобів захисту, а з використання психологічних особливостей людської поведінки [9].

За даними ENISA (2023) [5], людський фактор залишається одним із найсуттєвіших джерел кіберризиків для сучасних організацій. При цьому дедалі більшого поширення набувають комбіновані атаки, у яких психологічний вплив поєднується з інформаційними технологіями та організаційними слабкостями підприємства. Аналогічні висновки містяться і у щорічних звітах Verizon Data Breach Investigations Report, які протягом останніх років стабільно фіксують домінування соціальної інженерії серед початкових векторів компрометації корпоративних систем [19].

Однак у контексті менеджменту особливий інтерес становлять не лише кіберінциденти. Значно важливішим є те, що аналогічні принципи можуть використовуватися для впливу на процес прийняття управлінських рішень навіть без здійснення технічної атаки.

Наприклад, навмисне приховування частини інформації, зміна порядку подання альтернатив, акцентування уваги лише на окремих ризиках або використання авторитету окремих експертів можуть істотно впливати на кінцевий управлінський вибір. Формально при цьому всі процедури корпоративного управління можуть залишатися дотриманими, однак якість самого рішення вже буде визначатися не об'єктивним аналізом, а штучно сформованою інформаційною картиною.

VUCA як каталізатор ефективності психологічного впливу

Важливо підкреслити, що ефективність психологічного впливу істотно залежить від характеристик середовища, у якому приймається рішення. Саме тому VUCA не лише створює когнітивні ри-

зики, а й значно підсилює результативність маніпулятивних технологій.

Умови високої мінливості (Volatility) скорочують час перевірки інформації. Якщо рішення необхідно приймати негайно, керівники об'єктивно рідше використовують процедури незалежної верифікації та частіше покладаються на наявні джерела інформації.

Невизначеність (Uncertainty) підвищує роль експертного знання. За відсутності достатньої інформації керівники змушені більше довіряти спеціалістам, консультантам або керівникам функціональних підрозділів. Водночас саме концентрація критично важливої інформації в окремих учасників процесу створює потенційну можливість її навмисного викривлення.

Складність (Complexity) обмежує можливості комплексного аналізу. Чим більше взаємозалежних факторів необхідно врахувати, тим важче своєчасно виявити суперечності або неповноту інформації. Це суттєво підвищує ризик того, що окремі маніпулятивні дії залишаться непоміченими.

Нарешті, неоднозначність (Ambiguity) створює сприятливі умови для використання інформаційного фреймінгу. Якщо одна й та сама ситуація допускає декілька інтерпретацій, спосіб представлення інформації починає відігравати не меншу роль, ніж її фактичний зміст. Саме тому маніпуляція контекстом, акцентами або критеріями оцінювання здатна суттєво впливати на остаточний управлінський вибір навіть без викривлення фактичних даних.

Таким чином, VUCA-середовище не створює психологічного впливу, але істотно підвищує його потенційну ефективність.

Маніпуляція як управлінський ризик

У більшості сучасних досліджень психологічний вплив аналізується переважно як проблема індивідуальної поведінки або міжособистісної взаємодії. На нашу думку, для менеджменту більш продуктивним є інший підхід. Доцільно розглядати маніпулятивний вплив як управлінський ризик, здатний порушувати якість функціонування процесу прийняття рішень незалежно від особистісних характеристик окремих керівників.

За такого підходу ключовим питанням стає не те, чи можна повністю усунути психологічний вплив, а те, яким чином необхідно організувати процес прийняття управлінських рішень і систему його моніторингу, щоб мінімізувати наслідки цього впливу. Саме це положення, на нашу думку, принципово відрізняє проактивну корпоративну безпеку від традиційних моделей вну-

трішнього контролю. Якщо класичні системи орієнтовані переважно на виявлення порушень після їх виникнення, то проактивний підхід передбачає безперервне структурне спостереження за архітектурою управлінського процесу, у межах якого можливість успішної маніпуляції ідентифікується ще до прийняття рішення.

Таким чином, психологічний вплив не є самостійною причиною корпоративного шахрайства. Його ефективність визначається рівнем когнітивної стійкості процесу прийняття управлінських рішень. Саме тому наступним логічним етапом дослідження є розроблення концептуальної моделі, яка інтегрує механізми раннього виявлення таких вразливостей у систему корпоративного управління. У наступному розділі пропонується авторська модель PRISM (Proactive Risk Identification through Structural Monitoring), що розглядає процес прийняття управлінських рішень як центральний об'єкт проактивної корпоративної безпеки в умовах VUCA-середовища.

Концептуальна модель PRISM як інструмент забезпечення проактивної корпоративної безпеки в умовах VUCA

Проведений аналіз сучасних досліджень свідчить, що в умовах VUCA-середовища корпоративна безпека поступово виходить за межі традиційної функції контролю та дедалі більше інтегрується в систему стратегічного управління підприємством. Якщо класичні моделі безпеки були орієнтовані переважно на захист матеріальних активів, інформаційних ресурсів або фінансових потоків, то сучасна організація потребує захисту значно складнішого об'єкта - процесу прийняття управлінських рішень.

Подібне зміщення акцентів є закономірним. Саме управлінські рішення визначають розподіл ресурсів, вибір стратегічних пріоритетів, формування організаційної структури, взаємодію із зовнішніми партнерами та систему корпоративного контролю. Помилкове або навмисно викривлене рішення здатне породити ризики, масштаб яких значно перевищує наслідки окремого порушення внутрішніх процедур. У зв'язку з цим, забезпечення стійкості процесу прийняття управлінських рішень має розглядатися як самостійний напрям розвитку сучасної корпоративної безпеки.

Логіка побудови моделі PRISM

На основі проведеного аналізу пропонується концептуальна модель PRISM – Proactive Risk Identification through Structural Monitoring (проактивна ідентифікація ризиків через структурний моніторинг).

У межах даного дослідження PRISM визнається як інтегрована система проактивної корпоративної безпеки, спрямована на раннє виявлення когнітивних, інформаційних та організаційних вразливостей процесу прийняття управлінських рішень шляхом безперервного структурного моніторингу архітектури цього процесу, на протидію періодичній постфактумній перевірки вже прийнятих рішень.

На відміну від традиційних моделей Fraud Risk Management, запропонована концепція змінює сам об'єкт управління. Якщо класичні підходи концентруються переважно на виявленні факторів шахрайства або контролі окремих бізнес-процесів

[1; 3], то модель PRISM виходить із припущення, що корпоративне шахрайство є кінцевою фазою значно складнішого процесу, який починається з викривлення управлінського рішення, а отже, підлягає ідентифікації набагато раніше, ніж виникає сам шахрайський епізод.

Відповідно, первинним об'єктом моніторингу має стати не саме шахрайство, а архітектура прийняття управлінських рішень.

Архітектура моделі

Концептуально модель PRISM складається із шести взаємопов'язаних рівнів, кожен з яких є самостійною точкою структурного моніторингу (табл. 1).

Таблиця 1

Шестирівнева архітектура моделі PRISM

Рівень	Назва	Зміст	Об'єкт моніторингу
1	Контекст прийняття рішень	Характеристики VUCA-середовища: мінливість, невизначеність, складність, неоднозначність	Рівень зовнішнього когнітивного навантаження на систему управління
2	Архітектура процесу прийняття рішень	Порядок збору інформації, механізми міжфункціональної взаємодії, процедури погодження, централізація управління, делегування повноважень	Структурні індикатори організації процесу (концентрація повноважень, наявність альтернативних каналів інформації)
3	Когнітивні вразливості процесу	Інформаційна асиметрія, концентрація експертного знання, відсутність незалежної верифікації, дефіцит альтернативних сценаріїв, часовий тиск, міжфункціональна ізольованість	Індикатори «щільності» вразливостей у конкретному рішенні або підрозділі
4	Механізми психологічного та інформаційного впливу	Фреймінг, вибіркове подання інформації, використання авторитету, маніпуляція черговістю альтернатив	Поведінкові та комунікаційні аномалії в процесі підготовки рішення
5	Викривлення управлінського рішення	Зміна критеріїв вибору, порядку інтерпретації інформації, оцінювання альтернатив	Розбіжність між формальною процедурою та фактичною обґрунтованістю рішення
6	Наслідки викривленого рішення	Корпоративне шахрайство, помилкові інвестиційні рішення, неефективний розподіл ресурсів, репутаційні втрати	Постфактумна верифікація (контрольний, а не первинний контур)

Джерело: розроблено авторами.

Перший рівень формує контекст прийняття рішень. Його визначають характеристики VUCA-середовища: мінливість, невизначеність, складність та неоднозначність. Саме вони створюють початкове когнітивне навантаження на систему управління та визначають рівень організаційної стійкості до зовнішніх викликів.

Другий рівень представлений архітектурою процесу прийняття управлінських рішень. До нього належать порядок збору інформації, механізми міжфункціональної взаємодії, процедури погодження, рівень централізації управління, система делегування повноважень та організація інфор-

маційних потоків. Саме на цьому рівні PRISM відстежує перші структурні індикатори вразливості, зокрема, надмірну концентрацію повноважень або відсутність альтернативних каналів надходження інформації.

Третій рівень охоплює когнітивні вразливості процесу прийняття рішень. На відміну від психологічних досліджень, які аналізують індивідуальні особливості особистості, у межах запропонованої моделі оцінюються характеристики самого процесу управління. До них належать інформаційна асиметрія, надмірна концентрація експертного знання, відсутність незалежної верифікації критичної

інформації, дефіцит альтернативних сценаріїв, часовий тиск та міжфункціональна ізолюваність окремих структурних підрозділів.

Четвертий рівень представлений механізмами психологічного та інформаційного впливу. Важливо підкреслити, що модель PRISM не розглядає маніпуляцію як самостійну причину корпоративного шахрайства. Її ефективність визначається виключно наявністю когнітивних вразливостей, сформованих на попередньому рівні. Саме тому однакові маніпулятивні дії можуть мати принципово різні наслідки для різних організацій.

П'ятий рівень пов'язаний із викривленням управлінського рішення. Якщо попередні рівні не були виявлені та компенсовані, інформаційний або психологічний вплив може змінити процес оцінювання альтернатив, структуру критеріїв вибору чи порядок інтерпретації інформації. У результаті організація формально дотримується всіх процедур управління, однак прийняте рішення вже не відповідає її реальним стратегічним інтересам.

Шостий рівень охоплює наслідки викривленого управлінського рішення, серед яких корпоративне шахрайство розглядається лише як один із можливих сценаріїв розвитку подій. Аналогічними наслідками можуть бути помилкові інвестиційні рішення, неефективний розподіл ресурсів, реалізація збиткових проектів, стратегічні помилки або суттєві втрати репутації. Цей рівень у моделі PRISM виконує контрольну, а не первинну функцію: якщо система моніторингу спрацювала на рівнях 2–5, наслідки шостого рівня в ідеалі взагалі не повинні реалізуватися.

Ілюстративний приклад застосування логіки моделі

Логіку послідовного спрацювання рівнів моделі можна проілюструвати узагальненим (гіпотетичним) сценарієм. Підприємство ухвалює рішення щодо вибору постачальника в умовах стислих термінів (рівень 1 – Volatility). Уся інформація про альтернативних постачальників проходить через одного менеджера із закупівель, а процедура незалежної перевірки цінових пропозицій відсутня (рівень 2 – концентрація інформаційних повноважень).

Керівництво, обмежене в часі, не залучає альтернативного експерта та не вимагає порівняльного аналізу (рівень 3 – дефіцит альтернативних сценаріїв і часовий тиск). Менеджер із закупівель подає єдину пропозицію як «єдино можливу за таких термінів», акцентуючи ризики відмови від неї (рівень 4 – фреймінг і вибіркове подання інформації). Керівництво затверджує рі-

шення, формально дотримуючись процедури погодження, однак фактично без порівняння альтернатив (рівень 5 – викривлення рішення). Лише за результатами подальшого аудиту з'ясується, що обраний постачальник пов'язаний із менеджером через афілійовану структуру (рівень 6 – реалізований корпоративний ризик). У межах моделі PRISM подія на шостому рівні є не точкою виявлення проблеми, а точкою, якої можна було уникнути: структурні індикатори рівнів 2–4 (одноосібна концентрація закупівельної інформації, відсутність альтернативного порівняння, риторика «єдиного можливого рішення») за умови їх безперервного моніторингу давали підстави для втручання задовго до затвердження рішення.

Принципи функціонування PRISM

Практична реалізація запропонованої моделі базується на кількох взаємопов'язаних принципах.

Перший принцип – проактивність. Основною метою системи є не виявлення вже вчинених порушень, а раннє визначення умов, за яких процес прийняття рішень стає вразливим до викривлення. Це повністю відповідає сучасній концепції Enterprise Risk Management, відповідно до якої ризики мають управлятися до моменту їх реалізації [3].

Другий принцип – інтегрованість. Моніторинг процесу прийняття рішень не може бути функцією виключно служби корпоративної безпеки. До нього мають бути інтегровані механізми стратегічного менеджменту, ризик-менеджменту, внутрішнього аудиту, комплаєнсу, інформаційної безпеки та управління персоналом. Лише міжфункціональна взаємодія забезпечує достатній рівень стійкості організації в умовах VUCA.

Третій принцип – структурна індикація. Кожен із рівнів 2–4 моделі повинен мати власний набір спостережуваних структурних індикаторів (концентрація повноважень, відсутність альтернативних джерел інформації, частота використання риторики «єдиного рішення» тощо), а не лише узагальнену експертну оцінку. Практичними інструментами такої індикації можуть виступати незалежний аналіз альтернатив, процедури decision challenge, залучення міжфункціональних експертних груп та перевірка джерел критично важливої інформації [14].

Четвертий принцип – організаційна адаптивність. Оскільки VUCA-середовище постійно змінюється, система корпоративної безпеки також має бути динамічною. Це означає регулярний перегляд переліку структурних індикаторів, оновлення процедур прийняття рішень та накопичення організаційного досвіду щодо протидії новим типам інформаційного впливу.

Наукова новизна запропонованої моделі

Запропонована концепція PRISM, на нашу думку, має кілька принципових відмінностей від наявних підходів.

Перш за все, вона переносить центр уваги із суб'єкта шахрайства на процес прийняття управлінських рішень як на об'єкт структурного моніторингу.

Далі, модель інтегрує положення стратегічного менеджменту, когнітивної психології, Enterprise Risk Management та Fraud Risk Management у єдину концептуальну систему.

Третьою відмінністю є те, що корпоративне шахрайство розглядається не як ізольований вид корпоративного ризику, а як один із можливих наслідків невиявленого вчасно порушення цілісності процесу прийняття управлінських рішень.

Четверта відмінність - VUCA-середовище у межах запропонованої моделі виступає не лише зовнішнім контекстом діяльності організації, а фактором, який безпосередньо змінює характеристики управлінського процесу та формує нові об'єкти для структурного моніторингу.

Саме така логіка, на нашу думку, дозволяє розглядати проактивну корпоративну безпеку як невід'ємний елемент сучасного стратегічного менеджменту, а не лише як допоміжну функцію контролю чи реагування на вже реалізовані загрози.

ОБГОВОРЕННЯ РЕЗУЛЬТАТІВ

Запропонована концептуальна модель PRISM розвиває сучасні підходи до управління корпоративними ризиками, пропонуючи зміну самого об'єкта управління в системі корпоративної безпеки: замість контролю фінансових операцій чи виявлення ознак уже здійсненого шахрайства [1; 3] – раннє структурне виявлення вразливостей процесу прийняття рішень. Це узгоджується із сучасними дослідженнями динамічних здібностей підприємства, згідно з якими довгострокова конкурентоспроможність визначається здатністю організації своєчасно розпізнавати зміни зовнішнього середовища (sensing), приймати стратегічні рішення (seizing) та трансформувати власні ресурси відповідно до нових умов (transforming) [12; 18] – усі три компоненти в запропонованій моделі безпосередньо залежать від стійкості процесу прийняття управлінських рішень.

Отримані результати дають змогу сформулювати три положення, що розширюють сучасні уявлення про корпоративну безпеку. *По-перше*, когнітивні ризики доцільно розглядати не лише як індивідуально-психологічне явище, а як властивість організаційного процесу прийняття рішень, що дозволяє інтегрувати результати когнітивної

психології у сферу стратегічного менеджменту, не зводячи проблему до особистісних особливостей керівників. *По-друге*, психологічний вплив у моделі PRISM є не самостійним фактором ризику, а вторинним механізмом, ефективність якого визначається наявністю вже сформованих когнітивних вразливостей. *По-третє*, корпоративне шахрайство доцільно аналізувати як фінальний, контрольний рівень послідовного процесу, а отже, основні зусилля безпеки варто зосереджувати на рівнях 2–4, а не на рівні 6.

Практична цінність моделі PRISM полягає в можливості її інтеграції в існуючі системи корпоративного управління без створення окремої служби чи нових організаційних структур. На відміну від внутрішнього аудиту чи комплаєнсу, які фіксують порушення постфактум, PRISM забезпечує безперервний моніторинг структурних індикаторів на рівні підготовки рішення. Практична реалізація моделі може включати: інтегрування оцінювання когнітивних ризиків у процедури Enterprise Risk Management; використання процедур незалежної експертизи стратегічних рішень (decision challenge); обов'язкову перевірку критично важливої інформації із незалежних джерел; моніторинг концентрації інформаційних повноважень у межах окремих структурних підрозділів; формування системи поведінкових індикаторів можливого викривлення процесу прийняття рішень. Особливої актуальності підхід набуває для підприємств з високим рівнем регуляторних, фінансових або операційних ризиків, де навіть окреме управлінське рішення може мати довгострокові наслідки для фінансової стійкості й репутації.

Дослідження має три основні обмеження. Перш за все, модель PRISM має теоретичний характер і не пройшла емпіричної перевірки на вибірці українських чи міжнародних підприємств: сформульовані положення потребують подальшої операціоналізації та статистичної верифікації. Іншим обмеженням є те, що стаття зосереджена на корпоративному шахрайстві як одному з можливих наслідків викривлення рішень, тоді як аналогічна логіка потенційно застосовна до ширшого кола управлінських ризиків (стратегічні помилки, невдалі інвестиції, кризове управління). Третім обмеженням можна вважати те, що запропонована модель поки не містить кількісного інструментарію оцінювання структурних індикаторів. Розроблення відповідної системи показників є окремим напрямом подальших досліджень.

Подальший розвиток концепції доцільно здійснювати за трьома напрямками: розроблення методики кількісного оцінювання структурних ін-

дикаторів рівнів 2–4 моделі; емпірична перевірка PRISM на підприємствах різних галузей для встановлення зв'язку між характеристиками процесу прийняття рішень і показниками корпоративної безпеки; інтеграція моделі із цифровими системами підтримки управлінських рішень, Business Intelligence та штучним інтелектом для автоматизованого виявлення інформаційних аномалій і поведінкових патернів.

ВИСНОВКИ

Функціонування сучасних підприємств в умовах VUCA-середовища суттєво змінює традиційні підходи до забезпечення корпоративної безпеки. Якщо раніше основна увага приділялася захисту матеріальних, фінансових та інформаційних активів, то сучасні виклики свідчать про необхідність розширення об'єкта корпоративної безпеки шляхом включення процесу прийняття управлінських рішень. Саме якість управлінських рішень дедалі більше визначає здатність організації адаптуватися до мінливості зовнішнього середовища, ефективно управляти ризиками та забезпечувати довгострокову конкурентоспроможність.

Проведений аналіз сучасної наукової літератури з менеджменту, когнітивної психології, Enterprise Risk Management та Fraud Risk Management дозволив встановити, що наявні концепції здебільшого розглядають когнітивні процеси, управлінські рішення та корпоративну безпеку як відносно самостійні напрями досліджень. Водночас їхній взаємозв'язок у контексті функціонування підприємств у VUCA-середовищі залишається недостатньо вивченим.

У статті обґрунтовано, що кожен із компонентів VUCA (Volatility, Uncertainty, Complexity, Ambiguity) формує специфічні когнітивні ризики для процесу прийняття управлінських рішень. Мінливість скорочує час на аналіз альтернатив; невизначеність підвищує залежність від неповної інформації та експертних оцінок; складність збільшує когнітивне навантаження на осіб, які приймають рішення; неоднозначність створює можливості для множинного трактування одних і тих самих даних. Сукупний вплив цих факторів знижує стійкість управлінського процесу до інформаційних та психологічних впливів.

На відміну від поширених у психологічній літературі підходів, у дослідженні запропоновано розглядати когнітивні ризики не лише як індивідуальні особливості окремих керівників, а як властивість архітектури процесу прийняття управлінських рішень. Такий підхід дозволяє перенести акцент із особистісних характеристик управлінців на

організаційні механізми, які можуть як підвищувати, так і знижувати стійкість системи управління до викривлення управлінського вибору.

Обґрунтовано, що психологічний та інформаційний вплив не є самостійною причиною корпоративного шахрайства. Його ефективність значною мірою визначається наявністю когнітивних вразливостей процесу прийняття рішень. Таким чином, корпоративне шахрайство доцільно розглядати як один із можливих наслідків порушення цілісності управлінського процесу, а не виключно як результат неправомірної поведінки окремих працівників.

Основним результатом дослідження стало розроблення концептуальної моделі PRISM (Proactive Risk Identification through Structural Monitoring), яка інтегрує положення стратегічного менеджменту, когнітивної психології, Enterprise Risk Management і корпоративної безпеки в єдину систему. На відміну від традиційних моделей Fraud Risk Management, PRISM пропонує змінити об'єкт управління: замість реагування на вже реалізовані шахрайські дії основна увага приділяється безперервному структурному моніторингу процесу прийняття управлінських рішень на рівні його архітектури, когнітивних вразливостей та ознак впливу задовго до того, як рішення буде фактично викривлене.

Наукова новизна запропонованого підходу полягає в тому, що процес прийняття управлінських рішень розглядається як самостійний об'єкт проактивної корпоративної безпеки в умовах VUCA-середовища, а структурний моніторинг – як механізм, що дозволяє ідентифікувати ризик на крок раніше, ніж виникає сам шахрайський епізод. Практичне значення моделі полягає в можливості її інтеграції в наявні системи корпоративного управління без суттєвого перегляду організаційної структури підприємства.

Подальші дослідження доцільно спрямувати на операціоналізацію моделі PRISM, розроблення системи кількісних показників оцінювання структурних індикаторів, емпіричну перевірку запропонованої концепції на підприємствах різних галузей економіки, а також інтеграцію моделі із сучасними цифровими технологіями підтримки управлінських рішень та системами штучного інтелекту. ■

БІБЛІОГРАФІЯ

1. Association of Certified Fraud Examiners. *Occupational Fraud 2024: A Report to the Nations*. Austin : ACFE, 2024. 96 p. URL: <https://www.acfe>.

- com/-/media/files/acfe/pdfs/rtnn/2024/2024-report-to-the-nations.pdf
2. Bennett N., Lemoine G. J. What VUCA really means for you. *Harvard Business Review*. 2014. Vol. 92. No. 1–2. P. 27–42. URL: <https://hbr.org/2014/01/what-vuca-really-means-for-you>
3. Committee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management – Integrating with Strategy and Performance*. COSO, 2017.
4. Dorminey J., Fleming A. S., Kranacher M.-J., Riley R. A. The evolution of fraud theory. *Issues in Accounting Education*. 2012. Vol. 27. No. 2. P. 555–579. DOI: <https://doi.org/10.2308/iace-50131>
5. European Union Agency for Cybersecurity. *ENISA Threat Landscape 2023*. ENISA, 2023. 136 p.
6. Fasolo B., Heard C., Scopelliti I. Mitigating cognitive bias to improve organizational decisions: an integrative review, framework, and research agenda. *Journal of Management*. 2025. DOI: <https://doi.org/10.1177/01492063241287188>
7. Frigo M. L., Anderson R. J. Strategic risk management: a foundation for improving enterprise risk management and governance. *Journal of Corporate Accounting & Finance*. 2022. Vol. 33. No. 2. P. 17–28. DOI: <https://doi.org/10.1002/jcaf.22534>
8. Gigerenzer G. *The Intelligence of Intuition*. Cambridge : Cambridge University Press, 2023. 312 p. DOI: <https://doi.org/10.1017/9781009304894>
9. Hadnagy C. *Human Hacking: Win Friends, Influence People, and Leave Them Better Off for Having Met You*. New York : Harper Business, 2021. 304 p.
10. Hodgkinson G. P., Healey M. P. Psychological foundations of dynamic capabilities: reflexion and reflection in strategic management. *Strategic Management Journal*. 2011. Vol. 32. No. 13. P. 1500–1516. DOI: <https://doi.org/10.1002/smj.964>
11. ISO 31000:2018. *Risk Management – Guidelines*. 2nd ed. Geneva : International Organization for Standardization, 2018. 16 p.
12. Jousset T. P., Kanbach D. K., Kraus S. Enabling strategic change toward resilience: a systematic review from a dynamic capabilities perspective. *Strategic Change*. 2024. Vol. 34. P. 373–405. DOI: <https://doi.org/10.1002/jsc.2626>
13. Kahneman D. *Thinking, Fast and Slow*. New York : Farrar, Straus and Giroux, 2011. 512 p.
14. Kahneman D., Sibony O., Sunstein C. R. *Noise: A Flaw in Human Judgment*. New York : Little, Brown Spark, 2021. 464 p.
15. Millar C. C. J. M., Groth O., Mahon J. F. Management innovation in a VUCA world: challenges and recommendations. *California Management Review*. 2018. Vol. 61. No. 1. P. 5–18. DOI: <https://doi.org/10.1177/0008125618805111>
16. Schoemaker P. J. H., Heaton S., Teece D. J. Innovation, dynamic capabilities, and leadership. *California Management Review*. 2018. Vol. 61. No. 1. P. 15–42. DOI: <https://doi.org/10.1177/0008125618790246>
17. Teece D. J. Business models and dynamic capabilities. *Long Range Planning*. 2018. Vol. 51. No. 1. P. 40–49. DOI: <https://doi.org/10.1016/j.lrp.2017.06.007>
18. Teece D. J., Peteraf M., Leih S. Dynamic capabilities and organizational agility: risk, uncertainty, and strategy in the innovation economy. *California Management Review*. 2016. Vol. 58. No. 4. P. 13–35. DOI: <https://doi.org/10.1525/cmr.2016.58.4.13>
19. Verizon. 2025 Data Breach Investigations Report. Verizon Enterprise, 2025. 108 p.

REFERENCES

- Association of Certified Fraud Examiners (2024). *Occupational Fraud 2024: A Report to the Nations*. Austin: ACFE. <https://www.acfe.com/-/media/files/acfe/pdfs/rtnn/2024/2024-report-to-the-nations.pdf>
- Bennett N. & Lemoine G. J. (2014). What VUCA really means for you. *Harvard Business Review*, 1–2(92), 27–42. <https://hbr.org/2014/01/what-vuca-really-means-for-you>
- Committee of Sponsoring Organizations of the Treadway Commission (2017). *Enterprise Risk Management – Integrating with Strategy and Performance*. COSO.
- Dorminey J., Fleming A. S., Kranacher M.-J. & Riley R. A. (2012). The evolution of fraud theory. *Issues in Accounting Education*, 2(27), 555–579. <https://doi.org/10.2308/iace-50131>
- European Union Agency for Cybersecurity (2023). *ENISA Threat Landscape 2023*. ENISA.
- Fasolo B., Heard C. & Scopelliti I. (2025). Mitigating cognitive bias to improve organizational decisions: an integrative review, framework, and research agenda. *Journal of Management*. <https://doi.org/10.1177/01492063241287188>
- Frigo M. L. & Anderson R. J. (2022). Strategic risk management: a foundation for improving enterprise risk management and governance. *Journal of Corporate Accounting & Finance*, 2(33), 17–28. <https://doi.org/10.1002/jcaf.22534>
- Gigerenzer G. (2023). *The Intelligence of Intuition*. Cambridge: Cambridge University Press. <https://doi.org/10.1017/9781009304894>
- Hadnagy C. (2021). *Human Hacking: Win Friends, Influence People, and Leave Them Better Off for Having Met You*. New York: Harper Business.
- Hodgkinson G. P. & Healey M. P. (2011). Psychological foundations of dynamic capabilities: reflexion and reflection in strategic management. *Strategic Management Journal*, 13(32), 1500–1516. <https://doi.org/10.1002/smj.964>
- International Organization for Standardization (2018). *ISO 31000:2018. Risk Management – Guidelines*. 2nd ed. Geneva: International Organization for Standardization.

- Joussen T. P., Kanbach D. K. & Kraus S. (2024). Enabling strategic change toward resilience: a systematic review from a dynamic capabilities perspective. *Strategic Change*, 34, 373–405. <https://doi.org/10.1002/jsc.2626>
- Kahneman D., Sibony O. & Sunstein C. R. (2021). *Noise: A Flaw in Human Judgment*. New York: Little, Brown Spark.
- Kahneman D. (2011). *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux.
- Millar C. C. J. M., Groth O. & Mahon J. F. (2018). Management innovation in a VUCA world: challenges and recommendations. *California Management Review*, 1(61), 5–18. <https://doi.org/10.1177/0008125618805111>
- Schoemaker P. J. H., Heaton S. & Teece D. J. (2018). Innovation, dynamic capabilities, and leadership. *California Management Review*, 1(61), 15–42. <https://doi.org/10.1177/0008125618790246>
- Teece D. J., Peteraf M. & Leih S. (2016). Dynamic capabilities and organizational agility: risk, uncertainty, and strategy in the innovation economy. *California Management Review*, 4(58), 13–35. <https://doi.org/10.1525/cmr.2016.58.4.13>
- Teece D. J. (2018). Business models and dynamic capabilities. *Long Range Planning*, 1(51), 40–49. <https://doi.org/10.1016/j.lrp.2017.06.007>

Verizon (2025). *2025 Data Breach Investigations Report*. Verizon Enterprise.

Дослідження не отримувало зовнішнього фінансування.

Автори заявляють про відсутність конфлікту інтересів.

Внесок авторів:

Гайдуков В.: систематизація теоретичних засад прийняття управлінських рішень у VUCA-середовищі, аналіз впливу когнітивних упереджень, евристик та когнітивного перевантаження на якість рішень під тиском невизначеності, розробка та моделювання практичного кейсу оцінки рішень за системою PRISM. Гайдуков І.: розробка концептуальної рамки проактивної корпоративної безпеки, обґрунтування розширення «поверхні атаки» корпоративного шахрайства на рівень управлінських рішень, формулювання шестирівневої архітектури концептуальної моделі PRISM як системи запобігання зловживанням і формування підсумкових висновків дослідження.

Під час підготовки цього рукопису автори використовували інструменти генеративного штучного інтелекту для технічного редагування, стилістичного коригування тексту та перевірки бібліографічного опису джерел на відповідність вимогам ДСТУ 8302:2015.

Стаття надійшла до редакції / Received: 14.07.2026

Статтю прийнято до публікації / Accepted: 01.08.2026

Оприлюднено / Published: 08.10.2026