

DOI: 10.18372/2310-5461.71.21432

УДК 004.056:336.7

В. В. Дністровський,

аспірант кафедри кібербезпеки

Національний технічний університет

«Харківський політехнічний інститут»

orcid.org/0009-0006-2115-6380

e-mail: v.dnistrovskiy@khpi.edu.ua

МОДЕЛЮВАННЯ ВПЛИВУ КІБЕРЗАГРОЗ НА ПРИЙНЯТТЯ ІНВЕСТИЦІЙНИХ РІШЕНЬ

Вступ

Глобальний фінансовий простір останніх років зазнає масштабної цифрової трансформації, що докорінно змінює архітектуру надання інвестиційних послуг. Інтеграція хмарних технологій, розгортання високочастотних алгоритмічних систем (HFT), застосування моделей машинного навчання та штучного інтелекту для управління великими масивами даних дозволили суттєво знизити транзакційні витрати та підвищити ліквідність ринків. Інституційні інвестори та індивідуальні трейдери отримали безпрецедентний інструментарій автоматизації стратегій. Водночас, така тотальна технологізація сформувала принципово нові системні виклики, ризики та вразливості, перетворивши фінансову інфраструктуру на одну з головних мішень для кіберзлочинців у всьому світі.

Масштабування інфраструктурних рішень у межах діджиталізації (зокрема, використання децентралізованих фінансів DeFi, відкритих інтерфейсів прикладного програмування API та автоматизованих смарт-контрактів) призвело до розмивання традиційного захисного периметра організацій. У сучасних умовах інформаційна безпека перестає бути відокремленою сервісною функцією технічних підрозділів. Будь-яка критична вразливість програмного або апаратного забезпечення здатна майже миттєво призвести до незворотної експропріації або тривалого блокування інвестиційних активів, що вимагає розробки нових фундаментальних підходів до оцінки фінансових інструментів. Системний фінансовий аналіз ускладнюється тим, що кібератак носять асиметричний характер, де затрати зловмисника набагато менші за потенційні збитки фінансової інституції.

Зростаюча інтеграція різномірних інформаційних платформ створює умови для каскадного переносу ризиків. Збій в одному елементі ланцюжка постачання ПЗ чи компрометація окремого вузла зв'язку здатні паралізувати діяльність десятків взаємопов'язаних фондів та операторів ринку.

У таких обставинах виникає об'єктивна наукова необхідність перегляду класичних канонів управління портфелем капіталу з метою трансформації технічних параметрів експлуатації вразливостей в ендогенні змінні економічної доцільності, які були б зрозумілі фінансовому менеджменту.

Формулювання проблеми в загальному вигляді та її зв'язок з важливими науковими чи практичними завданнями

Стрімке зростання кількості інцидентів шкідливого впливу (Ransomware), експлуатації zero-day вразливостей у смарт-контрактах та скоординованих атак на ланцюжки постачання програмного забезпечення підтверджує, що кібербезпека більше не є суто технічним питанням IT-підрозділів організації. Вона трансформувалася в ендогенний макроекономічний фактор, який напряду впливає на загальну капіталізацію, операційну стійкість та довгострокову фінансову стабільність інструментів інвестування. Важливе практичне і наукове завдання полягає в необхідності інтегрувати технічні параметри кіберризиків в класичні моделі управління портфелем активів для захисту інституційного капіталу в умовах нестабільного і агресивного цифрового середовища.

Оцінка ризиків потребує нових безрозмірних детермінант, оскільки абстрактні грошові виміри збитків не відображають специфіку вразливості конкретного інструменту. Більше того, за відсутності стандартизованих відносних метрик інвестори позбавлені можливості здійснювати крос-секційне порівняння активів, які функціонують у різних правових та технологічних юрисдикціях. Безпосередній зв'язок цієї проблеми із державними завданнями цифрової трансформації економіки та захисту критичної інформаційної інфраструктури обумовлює необхідність перегляду базових принципів класичного портфельного менеджменту.

Поточні стандарти управління інвестиційною діяльністю здебільшого розглядають операційні ризики як фіксовані величини, що покриваються

резервними фондами або капіталом кіберстрахування. Проте динамічна природа технологічного простору унеможливорює статичне резервування, оскільки масштаб кумулятивного деструктивного ефекту може перевищувати ліквідні запаси фонду в кілька разів. Таким чином, формалізація кіберризиків як невід'ємного елемента ринкової оцінки ефективності розподілу активів є вагомим науковим завданням, що має глибоке прикладне значення для інституційних учасників ринку.

Аналіз останніх досліджень та публікацій

Традиційні підходи до управління інвестиційними ризиками, що базуються на фундаментальному та технічному аналізі, орієнтовані переважно на коливання ринкової кон'юнктури, макроекономічні індикатори, ліквідність та кредитну спроможність емітентів. У межах класичної інвестиційної теорії традиційні підходи до оцінки ризиків фокусуються виключно на їх розподілі на систематичні (ринкові) та несистематичні ризики, як це передбачено Сучасною портфельною теорією (MPT) Г. Марковіца та Моделлю оцінки капітальних активів (CAPM) В. Шарпа. У межах цих концепцій загальний ризик ототожнюється виключно з волатильністю ринкових цін. Проте сучасні дослідження доводять, що цифрова трансформація фінансового сектору вимагає розширення фундаментальних параметрів аналізу за рахунок технологічних чинників [1; 3].

Аналіз сучасних аналітичних праць свідчить про зростання уваги наукової спільноти та регуляторів до проблеми системних кіберризиків. Зокрема, у дослідженнях Positive Technologies обґрунтовано прогноз кіберзагроз для фінансового сектору та виявлено критичне зростання атак на інфраструктурні API і смарт-контракти [1]. Моніторинг кіберризиків у контексті забезпечення фінансової стабільності інвестиційних фондів детально висвітлено у дослідницькому меморандумі Грошово-кредитного управління Гонконгу (HKMA) [2]. Кількісна оцінка багатовимірного впливу кібератак на цифрові фінансові послуги проведена у систематичному огляді MDPI [3].

Питання корпоративного управління, моніторингу та оцінки кіберризиків у банківському та інвестиційному секторах детально розкрито у праці G. Birindelli та A. P. Iannuzzi [4]. Оцінку системних ризиків у глобальних фінансових системах наведено у звіті Всесвітнього економічного форуму (WEF) [5], а практичний аналіз економічних збитків від компрометації даних надано в дослідженнях IBM Security [6]. Проблематику актуальних загрозоутворюючих факторів та прогнози щодо кібербезпеки у сфері фінансових послуг висвітлено фахівцями BDO Global [7]. Водночас

методологічні засади кіберстрахування та управління ризиками ІКТ в інвестиційних фірмах сформовано в роботах F. Cramer та у керівних документах Європейського банківського управління (EBA) [8; 9]. Крім того, специфіку нормативно-правового комплаєнсу та захисту критичної інфраструктури досліджено у праці М. В. Красової [10].

Варто відзначити, що більшість існуючих робіт у сфері економіки кібербезпеки зосереджені на внутрішній оптимізації витрат окремого підприємства на захист периметра. Вони дають відповідь на питання, скільки коштів слід виділити на IT-інфраструктуру для мінімізації потенційних збитків. Однак зовнішній інвестор, який здійснює вибір між різнорідними інвестиційними інструментами на відкритому ринку капіталу, не має безпосереднього доступу до таких корпоративних моделей. Йому необхідний універсальний аналітичний інструмент, здатний перетворити непрямі ознаки надійності емітента на інтегрований коефіцієнт ризик-ефективності.

В умовах цифрової економіки класичні моделі «дохідність-ризик» виявляються обмеженими, оскільки вони повністю ігнорують загрозу раптової втрати або блокування капіталу внаслідок технічних збоїв чи цілеспрямованих кібератак. Основними недоліками традиційних підходів є: припущення про лінійність та нормальний розподіл ризиків (кіберінциденти є подіями класу fat-tailed, де ймовірність низька, але збитки катастрофічні) [7]; ігнорування інфраструктурного фактора (моделі передбачають безперебійне функціонування ринків, що повністю нівелюється під час DDoS-атак) [5]; фокус на історичних даних ряду цін, які неспроможні передбачити раптовий злам системи (zero-day вразливості) або інсайдерський саботаж [6].

Попередні дослідження не враховували одночасно відносний коефіцієнт ефективності захисту, питомі витрати на безпеку та рівень інформаційної асиметрії для інвестора, а оперування виключно абсолютними показниками (в USD) не дозволяло порівнювати фонди різного масштабу. Існуючі моделі здебільшого розглядають кіберризик як екзогенний шок, що не пов'язаний із внутрішніми бізнес-процесами або структурою витрат компанії-емітента активів. Це унеможливує проведення глибокого стратегічного аналізу ефективності інвестицій у системи виявлення та запобігання кібератакам. Невирішеною залишається проблема розробки безрозмірного критерію, який би враховував специфічний ризик простою та інформаційну непрозорість високотехнологічних фондів.

Порівняно з розглянутими підходами наукова новизна запропонованої моделі полягає у таких принципових відмінностях. По-перше, класичні

моделі МРТ Г. Марковіца та САРМ В. Шарпа [1] ототожнюють ризик виключно з ринковою волатильністю та не містять жодної технологічної складової. По-друге, аналітичні звіти Positive Technologies [1], НКМА [2] та WEF [5] мають описово-статистичний характер і фіксують масштаб кіберзагроз, однак не пропонують формалізованого розрахункового апарату для перенесення цих даних у показники дохідності конкретного інвестиційного інструменту. По-третє, роботи з корпоративного управління кіберризиками [4; 8] орієнтовані на внутрішню оптимізацію витрат емітента на захист периметра і, на відміну від запропонованої моделі, не придатні для використання зовнішнім інвестором, який не має доступу до внутрішньої звітності компанії. На противагу цьому, розроблений коефіцієнт Scyber_pro є першим інструментом, що: 1) виражає всі параметри кіберризиків виключно у відносних (безрозмірних) величинах, що уможливорює кроссекційне порівняння інструментів різного масштабу капіталізації; 2) безпосередньо інтегрує коефіцієнти k_{ale} , k_{sec} та α_{asym} у структуру класичного коефіцієнта Шарпа як його невід'ємні складові, а не розглядає кіберризик як окремий паралельний показник; 3) орієнтований саме на зовнішнього інвестора, який оцінює емітента лише за непрямими, публічно доступними ознаками надійності, а не на внутрішнього ризик-менеджера компанії.

Мета статті

Метою статті є формування комплексного науково-методичного підходу до оцінки кіберризиків як повноцінної складової процесу прийняття інвестиційних рішень шляхом розробки багатофакторної математичної моделі з повністю відносними (безрозмірними) значеннями, яка дозволяє формалізувати фінансові збитки з урахуванням розширених технологічних параметрів безпеки і скоригувати класичні метрики ризик-адаптованої ефективності для портфелів будь-якого масштабу.

Виклад основного матеріалу дослідження

Для глибокого розуміння природи деструктивного впливу технологічних чинників на інвестиційну діяльність необхідна суворая систематизація загрозоутворюючих факторів за контуром їх виникнення на дві ключові категорії: зовнішні (екзогенні) та внутрішні (ендогенні) [4; 5]. Зовнішні кіберзагрози генеруються суб'єктами поза операційним та правовим контролем структури (DDoS-атаки на API, фішинг, експлуатація вразливостей смарт-контрактів, Ransomware). Внутрішні кіберзагрози формуються в межах організації та походять від осіб, які мають легітимні права доступу (крадіжка пропрієтарного коду, саботаж баз даних, витік інсайдерської інформації) [6]. Детальний порівняльний аналіз архітектури кіберзагроз наведено в таблиці 1.

Таблиця 1

Порівняльний аналіз архітектури кіберзагроз для інвестиційних інструментів

Критерій порівняння	Зовнішні кіберзагрози (External Threats)	Внутрішні кіберзагрози (Insider Threats)
Етіологія та суб'єкти	Суб'єкти поза контуром захисту (хакерські угруповання, державні кіберструктури, недобросовісні конкуренти) [4]	Суб'єкти з легітимним доступом (діючий або звільнений персонал, топменеджмент, IT-підрядники) [6]
Канали реалізації	DDoS-атаки на API торговельних платформ, фішинг, експлуатація вразливостей смарт-контрактів, Ransomware [5]	Крадіжка пропрієтарного коду торгових роботів, саботаж баз даних, витік інсайдерської інформації, недбалість
Вектор деструктивного впливу	Порушення доступності сервісів та ліквідності; пряма експропріація активів	Порушення конфіденційності торгових стратегій; маніпулювання ринком «зсередини»
Специфіка детекції	Висока інтенсивність на початковій стадії; фіксуються системами IDS/IPS та екранами захисту периметра	Латентний характер; дії маскуються під стандартні бізнес-процеси, що ускладнює виявлення
Регуляторні наслідки	Репутаційні втрати, часові лаги при виконанні клієнтських ордерів	Санкції з боку фінансових регуляторів (SEC, BaFin тощо) за порушення комплаєнсу та витік даних [4]

*Джерело: розроблено автором

Для адекватного перенесення технічних параметрів загроз в економічну площу пропонується багатофакторна розширена модель, що базується на відносних безрозмірних величинах. Замість абсолютного показника річних втрат (Annual Loss Expectancy – ALE) ми вводимо коефіцієнт очікуваних річних кібервтратах (k_{ale}), який виражає відносні збитки як частку від загального капіталу під управлінням (Asset Value – AV). Показник k_{ale} доповнюється коефіцієнтом ефективності кіберзахисту ($CP \in [0, 1]$), де $CP = 1$ означає абсолютний захист, а $CP = 0$ – його повну відсутність:

$$k_{ale} = ALE / AV = [SLE \cdot ARO \cdot (1 - CP)] / AV, \quad (1)$$

де SLE (Single Loss Expectancy) – фінансові збитки від одного інциденту; ARO (Annualized Rate of Occurrence) – середньорічна частота виникнення загрози. Оскільки абсолютні базові збитки визначаються через коефіцієнт вразливості (Exposure Factor – EF) як $SLE = AV \cdot EF$, після підстановки параметр AV скорочується, і ми отримуємо чисту безрозмірну формулу відносних річних втрат:

$$k_{ale} = EF \cdot ARO \cdot (1 - CP). \quad (2)$$

Аналогічно, замість абсолютних грошових витрат на підтримку ІТ-безпеки (C_{sec}) ми вводимо коефіцієнт питомих витрат на кіберзахист (k_{sec}),

який показує відсоток бюджету безпеки відносно загального обсягу залучених управлінських активів: $k_{sec} = C_{sec} / AV$. Для урахування фактора непрозорості архітектури системи вводиться індекс інформаційної асиметрії ($\alpha_{asym} \geq 1$) за концепцією Акерлофа [11]. Що складніша система для аудиту інвестором, то вищий коефіцієнт α_{asym} , який штучно посилює очікувану волатильність. Авторська модифікація коефіцієнта Шарпа з відносними значеннями (S_{cyber_pro}) набуває такого вигляду:

$$S_{cyber_pro} = (R_p - R_f - k_{ale} - k_{sec}) / [\sigma_p + (\sigma_{cyber} \cdot \alpha_{asym})], \quad (3)$$

де R_p – базова номінальна дохідність інструменту; R_f – безризикова ставка дохідності; σ_p – ринкова складова волатильності; σ_{cyber} – додаткова волатильність дохідності, спричинена технічними зупинками і простоями інфраструктури від атак. Усі параметри чисельника та знаменника вимірюються у відсотках (частках) річних, що забезпечує методологічну строгість моделі.

Взаємодію вказаних параметрів, логічні зв'язки та етапність розрахунку індексу ризик-адаптованої ефективності на основі безрозмірних коефіцієнтів формалізовано на структурній схемі (рис. 1).

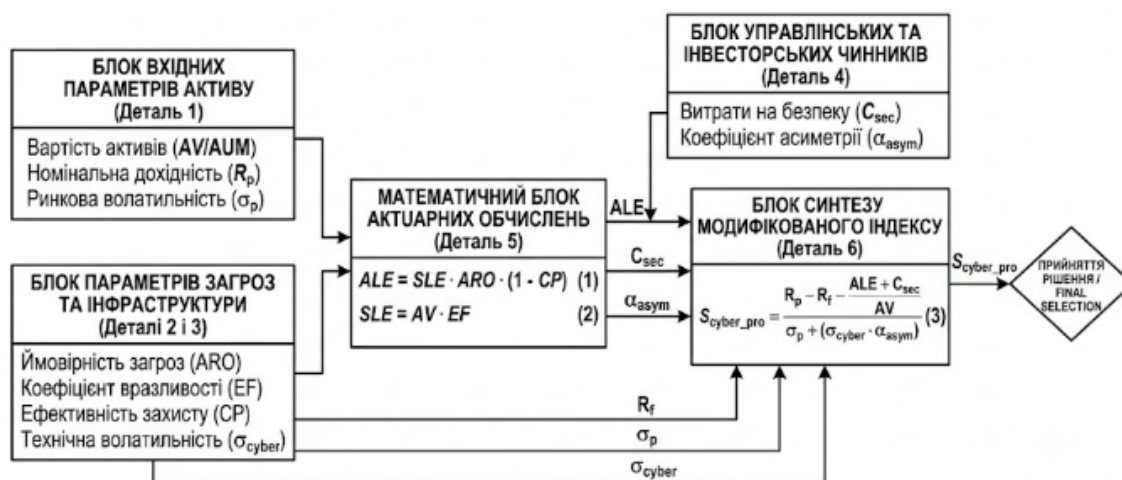


Рис. 1. Структурно-логічна схема взаємодії технологічних та фінансових детермінант відносної моделі

Відповідно до рис. 1, елементи моделі декомпоновано на окремі функціональні вузли: деталь 1 відображає базові фінансові відсоткові метрики інструменту; деталь 2 характеризує ймовірнісні параметри кіберзагроз; деталь 3 задає показники стійкості ІТ-архітектури організації; деталь 4 визначає питомі управлінські витрати та суб'єктивне ставлення до прозорості алгоритмів; деталь 5 репрезентує актуарний блок обчислення відносного коефіцієнта річних втрат k_{ale} , а деталь 6 є фінальною ланкою математичного синтезу та прийняття рішення інвестором.

Важливість переходу до повністю безрозмірного апарату обумовлена стохастичною природою сучасного цифрового фінансового ринку. Використання абсолютних сум створює методологічні викривлення, оскільки великі транснаціональні інвестиційні інститути здатні абсорбувати значні обсяги збитків без істотної втрати фінансової стійкості, тоді як для дрібних венчурних проєктів аналогічна сума втрат є катастрофічною. Застосування безрозмірних індексів дозволяє нівелювати масштабний фактор і сфокусувати увагу аналітиків суто на внутрішній технологічній надійності та системній стійкості активу.

Наукова новизна такого підходу полягає також у можливості динамічного моніторингу ефективності витрат на безпеку. Вводячи відносні змінні, інвестиційний менеджер отримує чітку математичну залежність: на скільки одиниць має зрости ефективність захисту CP при збільшенні питомих витрат k_{sec} на один відсоток, щоб значення підсумкового індексу S_{cyber_pro} не зменшилось. Таким чином, модель перетворюється з пасивного інструменту оцінки на активну систему підтримки прийняття рішень.

Практичне застосування моделі зовнішнім інвестором потребує окремого пояснення джерел вхідних параметрів. Показники R_p , R_f та σ_p є загальнодоступними і визначаються за біржовими котируваннями, проспектами емісії та звітами фонду про дохідність за попередні періоди. Значення ARO (частота кіберінцидентів) та EF (коефіцієнт вразливості) інвестор може оцінити опосередковано – на основі галузевої статистики спеціалізованих аналітичних звітів (Positive Technologies [1], IBM Security [6], НКМА [2], WEF [5]), які регулярно публікують усереднені показники частоти та масштабу кібератак для фінансового сектору в цілому або за окремими його сегментами (банки, DeFi-платформи, брокери). Коефіцієнт ефективності захисту CP та питомі витрати на безпеку k_{sec} є найскладнішими для об'єктивної оцінки, оскільки більшість емітентів не розкривають деталізовану інформацію про архітектуру власного кіберзахисту з міркувань безпеки. Для їх непрямої оцінки інвестор може використовувати публічні сертифікати відповідності (ISO/IEC 27001, SOC 2), рейтинги кібербезпеки спеціалізованих скорингових агентств (наприклад, Security Scorecard, BitSight), а також частку витрат на IT-безпеку, яку публічні емітенти розкривають у річний фінансовий звітності. Індекс інформаційної асиметрії α_{asym} за своєю природою є експертною оцінкою і може формуватися методом структурованого опитування (метод Дельфі) або за якісною шкалою прозорості коду й архітектури (відкритий blockchain-код отримує мінімальне значення, закрита пропрієтарна система – максимальне). Слід відверто зазначити, що складність та часткова суб'єктивність отримання показників CP , k_{sec} і α_{asym} є об'єктивним обмеженням моделі на поточному етапі й потребує подальшої розробки стандартизованих методик їх кількісного оцінювання, зокрема на основі агрегованих баз даних кіберінцидентів.

З метою практичного підтвердження пропонуваного підходу проведено симуляційне моделювання розподілу капіталу за безризикової ставки ринку $R_f = 4,0\%$. Інвестор порівнює два альтернативні об'єкти з кардинально різними профілями відносних значень (результати зведено у таблиці 2):

1. Інструмент А (Крипто-арбітражний фонд). Характеризується відкритою DeFi-інфраструктурою, високою дохідністю, але слабким рівнем стримування екзогенних атак. Вхідні параметри: $R_{pA} = 25,0\%$, $\sigma_{pA} = 18,0\%$, $ARO_A = 0,20$ (успішний злам раз на 5 років), $EF_A = 0,40$ (втрата 40 % портфеля), $\sigma_{cyber_A} = 5,0\%$, $CP_A = 0,30$ (низький захист), питомі витрати $k_{sec_A} = 1,0\%$, коефіцієнт інформаційної асиметрії $\alpha_{asym_A} = 1,05$ (висока прозорість блокчейн-коду).

2. Інструмент Б (Квантовий фонд акцій). Базується на закритих пропрієтарних високошвидкісних стратегіях. Вхідні параметри: $R_{pB} = 12,0\%$, $\sigma_{pB} = 8,0\%$, $ARO_B = 0,05$ (злам раз на 20 років), $EF_B = 0,10$ (втрата 10 % активів), $\sigma_{cyber_B} = 1,0\%$, $CP_B = 0,80$ (висока ефективність систем виявлення), питомі витрати на безпеку та комплаєнс $k_{sec_B} = 2,5\%$, коефіцієнт асиметрії $\alpha_{asym_B} = 1,50$ (архітектура типу «чорна скринька» для зовнішнього інвестора).

Математичне обчислення коефіцієнтів уточнених кіберзбитків за формулою (2) дає такі результати: для фонду А: $k_{ale_A} = 0,40 \cdot 0,20 \cdot (1 - 0,30) = 0,056$ або 5,6 % річних втрат капіталу; для фонду Б: $k_{ale_B} = 0,10 \cdot 0,05 \cdot (1 - 0,80) = 0,001$ або 0,1 % річних втрат портфеля. Класичний розрахунок коефіцієнта Шарпа без урахування чинників кібербезпеки демонструє явну, але помилкову перевагу першого варіанта: $S_A = (25,0 - 4,0) / 18,0 = 1,167$; $S_B = (12,0 - 4,0) / 8,0 = 1,000$.

Проте інтеграція розробленого відносного апарату за формулою (3) кардинально уточнює оцінку ризик-адаптованої ефективності. Чисельник для варіанта А становить $25,0\% - 4,0\% - 5,6\% - 1,0\% = 14,4\%$, знаменник дорівнює $18,0\% + (5,0\% \cdot 1,05) = 23,25\%$, що дає фінальний індекс $S_{cyber_pro_A} \approx 0,619$. Для варіанта Б чисельник дорівнює $12,0\% - 4,0\% - 0,1\% - 2,5\% = 5,4\%$, знаменник – $8,0\% + (1,0\% \cdot 1,50) = 9,5\%$, що формує індекс $S_{cyber_pro_B} \approx 0,568$.

Введення відносних параметрів дозволило виявити прихований деструктивний вплив інформаційної асиметрії квантового фонду та його високих постійних питомих витрат на утримання систем захисту. У результаті, попри вищі прямі кіберзбитки, Інструмент А за рахунок капіталізації надвисокої ринкової маржі та прозорості архітектури залишається більш привабливим для раціонального інвестора. Це підтверджує гіпотезу про те, що інвестиції у надмірно закриті високотехнологічні системи безпеки можуть створювати негативний ефект для кінцевої ризик-ефективності капіталу через феномен «чорної скриньки». Порівняльний аналіз результатів моделі наведений у таблиці 2.

Таблиця 2

Зведена відомість порівняльного моделювання з урахуванням розширених відносних параметрів

Фінансово-технологічний індикатор (у % або частках)	Інструмент А (Крипто-арбітраж)	Інструмент Б (Квантовий фонд)	Вектор переваги інвестора
Номинальна доходність (R_p)	25,0 %	12,0 %	Інструмент А (+13,0 %)
Коефіцієнт річних збитків (k_{ale})	5,6 %	0,1 %	Інструмент Б (мінімізація ризику)
Коефіцієнт питомих витрат (k_{sec})	1,0 %	2,5 %	Інструмент А (нижчі витрати)
Традиційний коефіцієнт Шарпа (S)	1,167	1,000	Інструмент А (хибна перевага)
Розширений відносний коефіцієнт S_{cyber_pro}	0,619	0,568	Інструмент А (обґрунтований вибір)

*Джерело: розроблено автором

Висновки цього дослідження та перспективи подальших досліджень

Проведене дослідження наочно доводить, що в умовах цифрової трансформації фінансових ринків ігнорування технологічних загроз веде до критичних методологічних помилок. Запропонований розширений безрозмірний коефіцієнт S_{cyber_pro} успішно переводить абстрактні технічні параметри в єдину фінансову площину відносних часток капіталу. Модель дозволяє збалансувати оцінку ефективності інструментів через одночасну інтеграцію індексів інформаційної асиметрії, питомих витрат на комплаєнс та коефіцієнта ефективності захисту периметра.

Перспективи подальших досліджень у цьому напрямку полягають у розробці динамічних стохастичних моделей кіберризиків із застосуванням апарату марковських процесів для прогнозування коливань інтенсивності атак у реальному часі. Окремим науковим вектором є дослідження впливу геополітичних чинників та макроекономічної волатильності на зміну середнього показника вразливості фінансових інструментів критичної інфраструктури.

ЛІТЕРАТУРА

- [1] Positive Technologies. (2025). Cyberthreats to the financial sector: forecast for 2025–2026. *Global Research & Analytics Report*. URL: <https://global.ptsecurity.com/en/research/analytics/cyberthreats-to-the-financial-sector--forecast-for-2025-2026/>
- [2] Hong Kong Monetary Authority (HKMA). (2025). Assessing Cyber Risks for Financial Stability: Evidence from Investment Funds. *Research Memorandum RM12-2025*. URL: <https://www.hkma.gov.hk/media/eng/publication-and-research/research/research-memorandums/2025/RM12-2025.pdf>
- [3] MDPI. (2025). Quantifying the Multidimensional Impact of Cyber Attacks in Digital Financial Services: A Systematic Literature Review. *Sensors*, 25(14), 4345. <https://doi.org/10.3390/s25144345>
- [4] Birindelli, G., & Iannuzzi, A. P. (2024). Cyber Risk in the Banking and Financial Sector: Monitoring, Measurement, and Governance. *Financial and Credit Activity: Problems of Theory and Practice*, 2(55), 112–126.
- [5] World Economic Forum (WEF). (2025). Global Cybersecurity Outlook 2025: Navigating Systemic Risks in Financial Systems. *Geneva: WEF Report*. URL: <https://www.weforum.org/publications/global-cybersecurity-outlook-2025/>
- [6] IBM Security. (2024). Cost of a Data Breach Report 2024. *IBM Institute for Business Value*. URL: <https://www.ibm.com/reports/data-breach>
- [7] BDO Global. (2024/2025). Top Cybersecurity Threats and Predictions for 2025 in Financial Services. *BDO Insights Report*.
- [8] Cremer F., Sheehan B., Fortmann M., Kia A. N., Mullins M., Murphy F., & Materne S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance – Issues and Practice*, 47(3), 698–736. <https://doi.org/10.1057/s41288-022-00266-6>
- [9] European Banking Authority (EBA). (2024). Guidelines on ICT and Security Risk Management in Investment Firms and Asset Managers. *EBA/GL/2024/03*. URL: <https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management>
- [10] Краснова М. В. Договори в екологічному та інформаційному праві України : монографія. Київ : Алерта, 2012. 216 с.
- [11] Akerlof, G. A. (1970). The Market for “Lemons”: Quality Uncertainty and the Market Mechanism. *Quarterly Journal of Economics*, 84(3), 488–500. <https://doi.org/10.2307/1879431>

Дністровський В. В.**МОДЕЛЮВАННЯ ВПЛИВУ КІБЕРЗАГРОЗ НА ПРИЙНЯТТЯ ІНВЕСТИЦІЙНИХ РІШЕНЬ**

Глобальний фінансовий простір останніх років зазнає масштабної цифрової трансформації, яка докорінно змінює архітектуру інвестиційних послуг, проте формує принципово нові виклики та вразливості, перетворюючи фінансову інфраструктуру на головну мішень для кібератак. Традиційні підходи до оцінки інвестиційних ризиків, що базуються на ринковій волатильності, повністю ігнорують ризик раптової втрати або блокування капіталу внаслідок кіберінцидентів, що веде до хибних управлінських рішень. У статті запропоновано авторський науково-методичний підхід до трансформації класичних портфельних теорій шляхом безпосередньої інтеграції відносних показників очікуваних кіберзбитків, питомих витрат на інформаційну безпеку та коефіцієнтів інформаційної асиметрії у критерії оцінки ризик-адаптованої ефективності капіталу. Розроблено математичну модель розширеного безрозмірного коефіцієнта Шарпа та проведено симуляційне моделювання розподілу активів між двома фондами з кардинально різними профілями ризику, що продемонструвало уточнення вектора інвестиційної привабливості на користь прозорих високовідокремлених стратегій. Доведено критичну доцільність урахування технологічних детермінант при диверсифікації портфеля інституційних та приватних інвесторів для забезпечення об'єктивного вибору фінансових інструментів.

Ключові слова: кіберзагрози; інвестиційні рішення; коефіцієнт Шарпа; очікувані збитки (ALE); алгоритмічна торгівля; фінансовий ризик; діджиталізація; управління активами.

Dnistrovskiy V.**MODELING THE IMPACT OF CYBER THREATS ON INVESTMENT DECISION-MAKING**

The global financial space of recent years is undergoing a massive digital transformation that fundamentally changes the architecture of investment services, however, it forms entirely new challenges and vulnerabilities, turning financial infrastructure into a major target for cyberattacks. Traditional approaches to investment risk assessment, based on market volatility, completely ignore the risk of sudden loss or blocking of capital due to cyber incidents, which leads to erroneous managerial decisions. The article proposes a scientific and methodical approach to the transformation of classical portfolio theories by directly integrating the relative annual loss expectancy, specific information security expenditures, and information asymmetry coefficients into the criteria for assessing risk-adjusted asset management efficiency. A mathematical model of the expanded dimensionless Sharpe ratio was developed, and a simulation modeling of capital allocation between two funds with fundamentally different risk profiles was conducted, demonstrating a precise adjustment of the investment attractiveness vector toward transparent, high-margin strategies. The critical expediency of taking technological determinants into account when diversifying the portfolio of institutional and private investors to ensure an objective choice of financial instruments is proved.

Keywords: cyber threats; investment decisions; Sharpe ratio; annual loss expectancy (ALE); algorithmic trading; financial risk; digitalization; asset management.

Дата першого надходження: 21.07.2026 р.

Дата прийняття до друку: 21.08.2026 р.

Дата публікації: 10.09.2026 р.