DOI https://doi.org/10.30525/978-9934-26-570-9-29

СТРАТЕГІЇ УПРАВЛІННЯ КІБЕР-РИЗИКАМИ У БІРЖОВІЙ ДІЯЛЬНОСТІ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ У ПЕРІОД ВІЙСЬКОВИХ ДІЙ

Кустов В. П.

ВСТУП

У сучасному світі кібербезпека стає критично важливим аспектом для будь-якої діяльності, і біржова діяльність не є винятком. Біржі, як ключові елементи фінансових ринків, мають справу з величезними обсягами електронних операцій, які здійснюються за допомогою складних технологій. Зростання залежності від цифрових технологій і автоматизованих систем підвищує вразливість бірж до різноманітних кіберзагроз, таких як хакерські атаки, маніпуляції з торговими системами, шахрайство, витоки конфіденційної інформації.

В умовах цифрової трансформації фінансового ринку та військових дій кібербезпека стає одним із ключових викликів для біржової діяльності. Значні обсяги електронної торгівлі, активне використання алгоритмічного трейдингу та штучного інтелекту створюють нові можливості для учасників ринку, але водночас підвищують рівень кіберризиків. У період військових конфліктів загрози кібербезпеці значно зростають через цілеспрямовані хакерські атаки, кібершпигунство та саботаж фінансової інфраструктури. Витоки даних, маніпуляції з торговими системами та збої в роботі біржових платформ можуть призвести до значних фінансових втрат, дестабілізації ринку та зниження довіри інвесторів.

Тому управління кіберризиками на біржі в умовах цифрової трансформації та військових дій потребує комплексного підходу, що включає впровадження новітніх методів моніторингу загроз, розробку стратегій оперативного реагування на кібератаки та дотримання міжнародних стандартів кібербезпеки. Військові конфлікти значно посилюють рівень кіберзагроз, оскільки біржова інфраструктура може стати мішенню як для державних, так і для злочинних хакерських угруповань. З огляду на стрімкий розвиток технологій та зростання кількості атак, дослідження ефективних стратегій управління кіберризиками у біржовій діяльності під час військових дій є вкрай актуальним.

Метою наукового дослідження є аналіз ключових кіберризиків, з якими стикаються біржі в умовах цифрової трансформації та військових дій, а також дослідження ефективних стратегій управління цими

ризиками. Особлива увага приділяється впливу сучасних технологічних викликів та кібератак, що спричинені геополітичними конфліктами, на фінансову інфраструктуру бірж.

1. Теоретичні засади кібер-ризиків у біржовій діяльності в умовах цифрової трансформації

Цифрова трансформація значно змінила ландшафт фінансових ринків, відкривши нові можливості для учасників, але водночас створила додаткові ризики. Зростання використання автоматизованих систем торгівлі, алгоритмічного трейдингу, штучного інтелекту та великої кількості фінансових технологій збільшили швидкість і масштабність операцій на біржах. Такі технології дозволили операторам ринку досягати високої ефективності, знижуючи витрати і збільшуючи ліквідність. Однак це також призводить до ускладнення контролю за поточними процесами та створення нових можливостей для кіберзагроз. Наприклад, алгоритмічний трейдинг, хоча і забезпечує значну перевагу в обробці даних, водночас може стати мішенню для атак, спрямованих на маніпуляцію ринковими цінами. Інтеграція блокчейн-технологій, використання криптовалют, а також розширене застосування електронних платіжних систем додають нові рівні складності для захисту фінансових активів. Таким чином, цифрова трансформація не лише сприяє розвитку фінансових ринків, але й вимагає нових підходів до управління ризиками та забезпечення кібербезпеки.

Період військових конфліктів має безпосередній вплив на рівень кіберзагроз, зокрема для фінансової інфраструктури. Біржові платформи та фінансові системи стають стратегічними цілями для державних та недержавних акторів, включаючи хакерські групи, які можуть діяти за замовленням урядів чи терористичних організацій. В умовах війни кіберзагрози набувають нових форм, таких як кібершпигунство, саботаж, дестабілізація ринкових механізмів або навіть прямі кібератаки на критичну інфраструктуру бірж. Одним з найбільших ризиків є втручання у роботу алгоритмів трейдингу, що може призвести до значних фінансових втрат та криз. Крім того, у разі військового конфлікту може зрости кількість так званих «дісінформаційних» атак, які мають на меті посіяти паніку серед інвесторів, знизити довіру до ринку або спровокувати хаос на фінансових платформах. У таких умовах традиційні методи захисту від кіберзагроз можуть бути недостатніми, і необхідно розробляти нові стратегії, що враховують специфіку військових дій та загрози, пов’язані з гібридними атаками.

Кібер-ризик є динамічним ризиком, в основі якого лежить втручання та порушення цілісності інформаційного забезпечення. Кібер-ризик найчастіше проявляється через кібератаки, наслідки яких можуть бути як прямі, так і опосередковані, що значно ускладнює процес оцінки фінансових втрат. Крім того, фінансові втрати від реалізації кібер-ризиків не обмежені в часі, тобто можуть проявитись набагато пізніше після ліквідації шкоди[1].

Кібер-ризик (англ. Cyber risk) − це операційний ризик, який полягає в отриманні прямих чи побічних збитків економічними суб'єктами внаслідок їх функціонування у кіберпросторі. Поняття «кібер-ризики» трактується як потенційні загрози інформаційній безпеці, які можуть призвести до фінансових збитків, витоку конфіденційної інформації або порушення роботи біржових систем[2].

Вчені під поняттям «кібер-ризик» розуміють ризик, який:

− пов'язаний з накопиченням, зберіганням і використанням особистих персональних даних;

− стосується потенційної шкоди або втрат внаслідок порушення безпеки цифрових систем, мереж або даних;

− представляє ймовірність і вплив несприятливих подій, що відбуваються в цифровій сфері;

− охоплює різні загрози, пов'язані з комп'ютерним обладнанням та програмним забезпеченням, включаючи локальні та глобальні інтернет-мережі, платіжні системи, платформи електронної комерції та системи управління промисловістю[3][4].

Отже, кібер-ризики охоплюють широкий спектр загроз у цифровій сфері. Зокрема, у контексті біржової діяльності вони мають свою специфіку. У вузькому значенні кібер-ризики у біржовій діяльності пов'язані з операційними загрозами для інформаційних та технологічних активів, що можуть негативно впливати на конфіденційність, доступність і цілісність біржової інформації та торгових систем.

У широкому значенні кібер-ризики охоплюють потенційні загрози для цифрових торгових мереж, що використовуються для передавання,

---

[1] Волосович С., Клапків Л. Детермінанти виникнення та реалізації кіберризиків. *Зовнішня торгівля: економіка, фінанси, право.* 2018. № 3. С. 101–115.

[2] Гриценко К. Кібербезпека в боротьбі з банківськими шахрайствами: захист споживачів фінансових послуг та зростання фінансово-економічної безпеки України. 2020. URL: https://www.academia.edu/95297712/ utm_source= chatgpt.com.

[3] Прокоф'єва О.В., Беспалова Ю. Кібер-ризики та управління ними в умовах глобалізації та цифрової трансформації. *Ефективна економіка*. 2024. № 5. URL: https://www.nayka.com.ua/index.php/ee/article/ view/3822/3857/

[4] Братюк В.П. Сутність кіберризиків та страховий захист від кіберризиків в Україні. *Актуальні проблеми економіки*. 2015. № 9 (171). С. 421–427.

обробки та зберігання біржових даних, а також для виконання фінансових операцій у кіберпросторі.

Кібер-ризик у біржовій діяльності можна визначити як загрозу, пов'язану з онлайн-торгівлею, електронними торговими платформами, алгоритмічним трейдингом, фінансовими технологіями та зберіганням персональних і корпоративних даних.

Варто назвати основні типи кібер-ризиків у біржовій діяльності, які включають:

- атаки на торгові платформи (DDoS, злом алгоритмів трейдингу);
- фінансове шахрайство (маніпуляції з транзакціями, підробка даних);
- витоки конфіденційної інформації (хакерські атаки, інсайдерські загрози);
- соціальна інженерія (фішингові атаки, компрометація акаунтів).

Ефективніше оцінювати загрози та розробляти стратегії захисту дозволяє класифікація кібер-ризиків у біржовій діяльності за різними критеріями, яка може ґрунтуватися на різних підходах залежно від джерела загрози, способу реалізації, наслідків тощо (рис. 1).

Таким чином, класифікація кібер-ризиків у біржовій діяльності допомагає визначити їхній вплив на функціонування біржових платформ і допомагає розробити ефективні заходи для їхнього попередження й мінімізації. Отже, розуміння та систематизація кібер-ризиків є важливим кроком для забезпечення стабільності біржових платформ. Водночас, відсутність належних механізмів управління кіберризиками, особливо в умовах цифрової трансформації та військових дій, може спричинити серйозні наслідки, зокрема:

- значних фінансових втрат через цілеспрямовані кібератаки, спрямовані на біржову інфраструктуру;
- зниження довіри інвесторів через нестабільність торгових платформ та витоки даних;
- дестабілізації ринку через технічні збої, викликані хакерськими атаками або кібердиверсіями;
- регуляторних санкцій та юридичної відповідальності біржових операторів за неналежний рівень кіберзахисту.

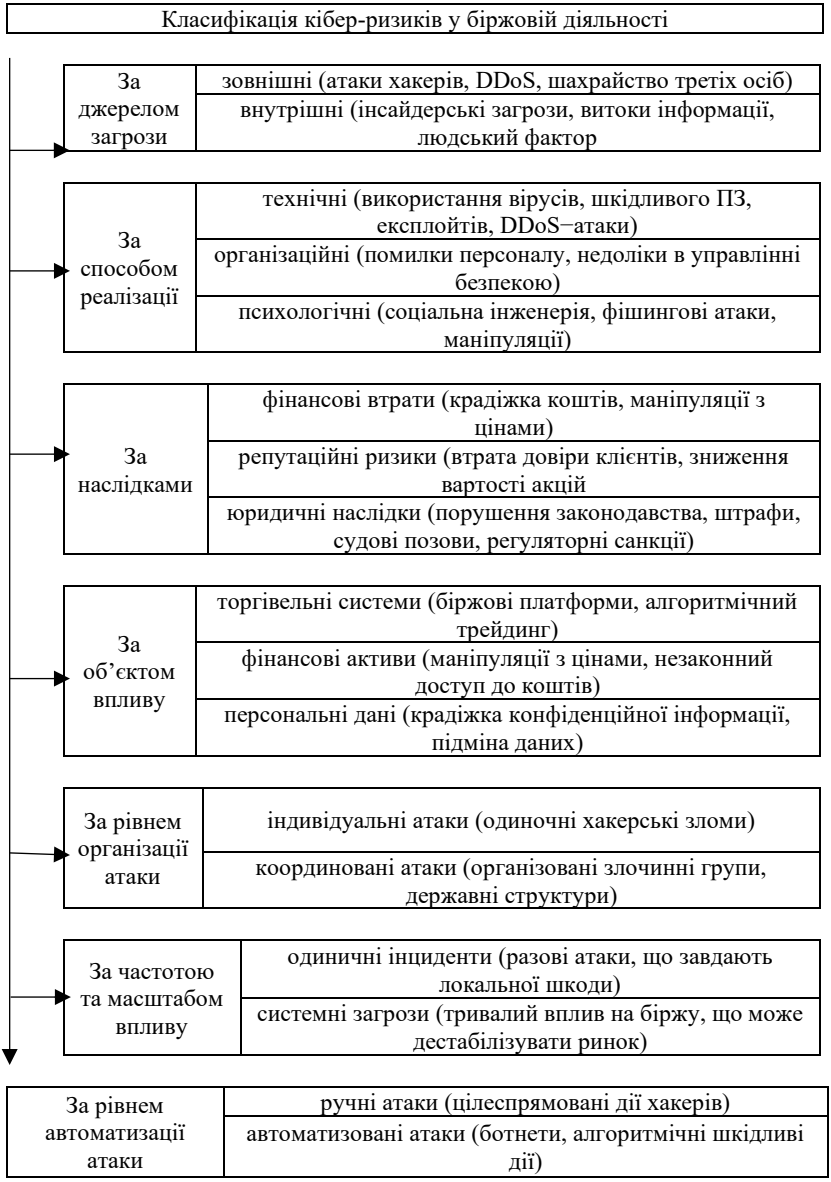

Рис. 1. Класифікація кібер-ризиків у біржовій діяльності

Джерело: власна розробка

2. Основні технологічні рішення для зниження кібер-ризиків

З огляду на потенційні загрози та їхні наслідки, виникає необхідність у розробці й реалізації дієвих стратегій захисту. Управління кібер-ризиками у біржовій діяльності в умовах цифрової трансформації потребує системного підходу, що включає моніторинг загроз, впровадження передових технологій кібербезпеки та страхування ризиків як фінансовий механізм захисту[5]. Для ефективного управління кібер-ризиками біржі повинні впроваджувати такі заходи:

− використання багаторівневої автентифікації та шифрування даних для запобігання несанкціонованому доступу;

− регулярний аудит безпеки та тестування на проникнення з урахуванням нових тактик кібератак у період війни;

− розвиток системи виявлення загроз (SIEM) та механізмів швидкого реагування на кіберінциденти;

− навчання персоналу основам кібербезпеки та протидії соціальній інженерії, що часто використовується під час військових конфліктів.

Ключовим інструментом забезпечення фінансової стабільності компаній, що працюють у сфері біржової діяльності та стикаються з ризиками цифрової епохи є розвиток кіберстрахування як складової глобального страхового ринку[6]. На часі, кібер-страхування вже стало критично важливим елементом управління ризиками у цифровій економіці, особливо в період військових дій, коли зростає кількість кібератак на фінансові інституції та біржові системи[7].

Також поряд із розвитком кіберстрахування, критично важливою залишається реалізація комплексних заходів кібербезпеки, що сприяють зниженню ризиків для біржових платформ. Використання сучасних методів захисту, зокрема багаторівневої аутентифікації, шифрування даних та моніторингу кіберзагроз у режимі реального часу, дозволяє мінімізувати потенційні втрати від атак. Крім того, впровадження міжнародних стандартів інформаційної безпеки, таких як ISO/IEC 27001 та NIST Cybersecurity Framework, сприяє підвищенню стійкості фінансових систем до зовнішніх загроз.

Однак, незважаючи на активний розвиток кіберстрахування та впровадження передових технологій кіберзахисту, біржові компанії все ще стикаються з викликами у сфері регулювання та правового забезпечення. Відсутність єдиних міжнародних норм, що регулюють

[5] Кожедуб Ю. Аналіз документів з керування ризиком кібербезпеки. *Information Technology and Security.* 2017. Vol. 5. № 1. С. 82–95.

[6] Селіверстова Л.С., Трухан Д.А. Підходи до розвитку кіберстрахування як сегменту глобального страхового ринку. *Економіка та держава.* 2020. № 1. С. 23 – 26.

[7] Приказюк Н.В., Гуменюк Л.С. Кібер-страхування як важливий інструмент захисту підприємств в умовах цифровізації економіки. *Ефективна економіка*. 2020. № 4. URL: http://www.economy.nayka. com.ua/pdf/4_2020/8.pdf.

страхування кіберризиків, створює певну невизначеність для учасників ринку. У цьому аспекті важливою є співпраця між державними органами, фінансовими регуляторами та страховими компаніями для розробки ефективних механізмів управління ризиками, що дозволять створити надійну систему захисту біржових платформ від кіберзагроз.

У цьому контексті особливу роль відіграє застосування міжнародних стандартів, таких як ISO/IEC 27001, NIST Cybersecurity Framework, GDPR, а також адаптація до умов гібридної війни, що дозволяють біржам підвищувати рівень кіберзахисту та мінімізувати фінансові ризики.

Водночас, хоча кіберстрахування та впровадження передових методів кібербезпеки є ключовими елементами захисту біржових платформ, вони не можуть повністю усунути всі виклики. Одним із найбільших бар'єрів залишається відсутність єдиного міжнародного правового регулювання у сфері страхування кіберризиків, що створює невизначеність для учасників ринку. У цьому контексті необхідна тісна взаємодія між державними органами, фінансовими регуляторами та страховими компаніями, що дозволить сформувати ефективну систему управління ризиками та забезпечити стабільність біржової діяльності в умовах зростаючих кіберзагроз.

З огляду на зростаючі загрози у сфері кібербезпеки, біржі мають активно впроваджувати сучасні технології для мінімізації кібер-ризиків. Інноваційні підходи, зокрема використання штучного інтелекту, блокчейну та квантової криптографії, відіграють ключову роль у підвищенні стійкості біржових платформ. У цьому контексті розглянемо основні технологічні рішення для зниження кіберризиків: використання Big Data у кібербезпеці; блокчейн та його роль у захисті біржових операцій; автоматизовані системи моніторингу та виявлення загроз; інтеграція кібербезпеки у біржові фінансові технології; використання квантової криптографії для захисту біржових транзакцій (рис. 2).

Рис. 2. Основні технологічні рішення для зниження кіберризиків

Джерело: власна розробка

Використання Big Data у кібербезпеці, у свою чергу, забезпечує аналіз величезних обсягів інформації, що зберігається в різноманітних джерелах − від транзакцій на біржі до інформації про поточний стан мережі. Збір та обробка таких даних дозволяють ідентифікувати зразки поведінки, які можуть свідчити про початок кібернападу, навіть якщо він є складним або новим. Для бірж важливо мати можливість не тільки аналізувати транзакції, але й розуміти контекст подій на ринку, що досягається за допомогою Big Data. Інтеграція Big Data дозволяє створити комплексну систему кібербезпеки, яка здатна виявляти загрози ще до їх повного розгортання.

Окрім використання Big Data, важливу роль у забезпеченні кібербезпеки біржових платформ відіграє технологія блокчейн. Її унікальні властивості, такі як децентралізація, прозорість і незмінність даних, роблять її ефективним інструментом для захисту біржових операцій. Блокчейн є технологією, яка відома своїми можливостями забезпечити прозорість, безпеку та незмінність даних. Завдяки своїй дистрибутивній природі, блокчейн здатний змінити підхід до захисту біржових операцій, забезпечуючи більшу стійкість до маніпуляцій, зловмисних атак та шахрайства.

У контексті біржової діяльності блокчейн може бути використаний для таких цілей:

− прозорість та незмінність записів, зокрема завдяки своїй архітектурі, блокчейн забезпечує, щоб всі транзакції та операції були незмінними і доступними для перевірки, що робить складними будь-які маніпуляції з інформацією або зміну історії транзакцій. Для бірж, де важливо забезпечити довіру між учасниками ринку, ця властивість є надзвичайно цінною;

− захист від шахрайства та маніпуляцій. Блокчейн, використовуючи криптографію для захисту даних, ефективно запобігає шахрайству та маніпуляціям, зокрема підробці інформації та штучному впливу на ціни. Особливо важливо в умовах використання алгоритмічного трейдингу та автоматизованих систем, де несанкціоноване втручання може призвести до серйозних фінансових втрат;

− децентралізація та стійкість до атак. Блокчейн є дистрибутивною технологією, що означає, що копії даних зберігаються на численних незалежних вузлах, що робить блокчейн стійким до атак на окремі сервери або бази даних. Для бірж це особливо важливо, оскільки централізовані системи можуть бути вразливими до кібератак, спрямованих на знищення або викрадення даних;

− ідентифікація та авторизація користувачів, зокрема за допомогою блокчейн-технологій можна створювати безпечні, незмінні механізми ідентифікації та автентифікації користувачів, що дозволяє уникнути проблем з незаконним доступом до облікових записів або маніпуляцією з рахунками;

− покращення безпеки смарт-контрактів. Біржові платформи можуть використовувати смарт-контракти на базі блокчейну для автоматизації виконання угод, що значно знижує ризик людських помилок або зловмисного втручання. Смарт-контракти виконуються лише за настання певних умов, і не можуть бути змінені після їх запуску, що робить їх ефективним інструментом для забезпечення захисту угод.

Таким чином, блокчейн є потужним інструментом для підвищення рівня кібербезпеки на біржах. Його використання дозволяє значно знизити рівень ризиків, пов'язаних з маніпуляціями, шахрайством та несанкціонованим доступом, тим самим підвищуючи довіру учасників ринку до фінансових операцій.

У сучасних умовах кібербезпеки на фінансових ринках важливу роль відіграють автоматизовані системи моніторингу та виявлення загроз. Біржі та фінансові установи стикаються з великим обсягом даних і складними кіберзагрозами, що постійно змінюються. Традиційні методи контролю можуть бути недостатньо ефективними через швидкість та масштабність атак. Тому автоматизовані системи, які використовують передові технології, є критично важливими для ефективного забезпечення безпеки.

Автоматизовані системи моніторингу засновані на використанні алгоритмів машинного навчання та штучного інтелекту, що дозволяє відстежувати активність на біржах в реальному часі та оперативно виявляти аномалії, що можуть бути не тільки спроби несанкціонованого доступу до системи або маніпуляції з даними, але й детектування незвичних торгових патернів, що можуть свідчити про шахрайство чи спроби маніпулювання ринком. Такі системи здатні аналізувати величезні обсяги інформації, що надходить з різних джерел, виявляти закономірності та автоматично повідомляти про потенційні загрози.

Крім того, автоматизовані системи можуть бути інтегровані з іншими інструментами безпеки, такими як системи запобігання вторгненням (IPS), що забезпечують негайне реагування на загрози, а також з системами управління інцидентами для належного документування та швидкого реагування.

Завдяки високій швидкості обробки даних та самонавчанню алгоритмів, такі системи можуть значно знизити час на виявлення кіберзагроз та підвищити ефективність заходів реагування.

Необхідною для забезпечення безпеки операцій, особливо в умовах цифрової трансформації є інтеграція кібербезпеки у біржові фінансові технології. Оскільки біржі активно використовують новітні технології, такі як алгоритмічний трейдинг, платформи для торгівлі криптовалютами та інші інновації, важливо, щоб всі ці системи були захищені на кожному етапі їхньої роботи.

Одним з ключових аспектів інтеграції є впровадження безпеки вже на етапі проектування та розробки фінансових технологій, що означає, що системи повинні враховувати захист від потенційних кіберзагроз з самого початку: від захисту персональних даних до забезпечення прозорості торгових операцій та запобігання шахрайству.

Важливою частиною цього процесу є використання безпечних протоколів передачі даних, таких як TLS (Transport Layer Security), для забезпечення конфіденційності та цілісності інформації під час її передавання. Також варто впроваджувати механізми багатофакторної аутентифікації та шифрування даних, що дозволяє зменшити ризики несанкціонованого доступу до платформи.

Інтеграція кібербезпеки в фінансові технології повинна також передбачати постійний моніторинг та аудит систем, щоб оперативно виявляти та усувати вразливості, що включає як регулярні перевірки безпеки, так і адаптацію до нових кіберзагроз і технологічних змін.

Для захисту біржових транзакцій варто використовувати квантову криптографію, яка є технологією, що базується на принципах квантової механіки, і вона має великий потенціал для забезпечення безпеки фінансових транзакцій на біржах у майбутньому. Оскільки традиційні методи шифрування, такі як RSA або алгоритм ECDSA, можуть стати вразливими до атак з використанням квантових обчислювальних потужностей, квантова криптографія пропонує альтернативні рішення, що здатні значно підвищити рівень безпеки.

Одним з основних принципів квантової криптографії є квантова розподілена передача ключів (Quantum Key Distribution, QKD), яка дозволяє безпечно передавати криптографічні ключі, навіть в умовах, коли зловмисник може контролювати канали зв’язку. За допомогою QKD інформація про ключ передається таким чином, що будь-яка спроба перехоплення або маніпуляції з даними буде одразу помічена, оскільки квантова механіка забезпечує зміну стану часток при їх вимірюванні.

У біржових фінансових транзакціях це може значно підвищити захист від кіберзагроз, таких як перехоплення чутливих даних чи спроби маніпулювання з транзакціями. Використання квантових алгоритмів для шифрування забезпечить підвищену стійкість до

потенційних квантових атак, що можуть здійснити майбутні квантові комп'ютери.

Таким чином, квантова криптографія пропонує значні переваги для захисту біржових транзакцій, створюючи більш надійні механізми безпеки, які здатні витримати навіть найпотужніші атаки. Проте впровадження цих технологій наразі залишається предметом активних досліджень і експериментів, оскільки їх масове використання на фінансових ринках ще потребує подальшого розвитку та тестування.

Аналізуючи сучасні технології кібербезпеки, можна дійти висновку, що їхнє ефективне впровадження значно підвищує стійкість біржових платформ до кіберзагроз. Досвід провідних бірж показує, що комплексний підхід до управління кіберризиками дозволяє:

− по-перше, знизити ймовірність успішних атак, навіть у період зростання загроз під час війни;

− по-друге, мінімізувати наслідки потенційних загроз завдяки автоматизованим системам реагування;

− по-третє, підвищити рівень довіри інвесторів та забезпечити стабільність фінансових ринків у складних умовах.

В умовах зростаючих кіберзагроз біржі повинні не лише впроваджувати сучасні технології захисту, а й адаптувати свої стратегії управління ризиками до нових викликів. Особливо це актуально в періоди військових конфліктів, коли кібератаки стають потужним інструментом гібридної війни. У цьому контексті розглянемо стратегії управління кіберризиками на біржі в умовах війни, а саме:

− багаторівневі механізми захисту біржової інфраструктури;

− роль міжнародних стандартів у забезпеченні кібербезпеки (ISO/IEC 27001, NIST);

− розробка планів реагування на кіберінциденти;

− моделювання сценаріїв кібератак та тестування безпеки;

− досвід країн та міжнародних бірж у боротьбі з кібератаками.

3. Особливості багаторівневої кібербезпеки біржової інфраструктури

Біржова інфраструктура є однією з найбільш критичних складових фінансової системи, тому її захист від кіберзагроз вимагає застосування багаторівневих механізмів безпеки. Такий підхід дозволяє створити кілька захисних бар'єрів, що забезпечують надійний захист від різноманітних атак, включаючи хакерські вторгнення, спроби маніпуляцій з даними, а також фізичні та логічні загрози.

Один із основних елементів багаторівневого захисту біржової інфраструктури є безпека на рівні мережі. Використання фаєрволів, систем виявлення та запобігання вторгненням (IDS/IPS), а також

мережевих проксі-серверів допомагає фільтрувати та контролювати мережевий трафік, що дозволяє виявляти аномалії та блокувати шкідливі з'єднання ще до того, як вони досягнуть важливих систем. Крім того, застосування сегментації мережі допомагає зменшити вплив можливих атак, обмежуючи доступ до критичних ресурсів тільки авторизованим користувачам.

Для захисту даних, що передаються між користувачами та біржею, важливим є використання сучасних протоколів шифрування, таких як TLS/SSL для захисту каналу зв'язку та алгоритмів AES для шифрування даних на сервері, що запобігає несанкціонованому доступу до інформації, включаючи особисті дані користувачів та фінансові операції. Шифрування також забезпечує захист від атак «людина посередині», де зловмисник може перехопити дані між учасниками біржової торгівлі.

Забезпечення належного рівня аутентифікації є важливою складовою багаторівневого захисту. Важливо використовувати багатофакторну аутентифікацію (MFA), що комбінує кілька різних методів підтвердження особи, наприклад, паролі, біометричні дані або апаратні токени. Це знижує ризик несанкціонованого доступу навіть у разі компрометації одного з рівнів аутентифікації.

Успішний захист біржової інфраструктури неможливий без постійного моніторингу її діяльності. Використання автоматизованих систем виявлення аномалій та кіберзагроз дозволяє оперативно реагувати на потенційні атаки, навіть якщо вони відбуваються у реальному часі. Крім того, необхідно мати налагоджені процедури реагування на інциденти, що включають швидке блокування загроз, ізоляцію уражених систем і проведення розслідувань.

Незважаючи на те, що основні кіберзагрози зосереджені на програмному забезпеченні, фізична безпека інфраструктури також має важливе значення. Це включає захист серверних кімнат, дата−центрів і інших критичних об'єктів від несанкціонованого доступу, природних катастроф або фізичних атак. Крім того, необхідно забезпечити надійне резервне копіювання даних і відновлення після аварій.

Міжнародні стандарти відіграють важливу роль у забезпеченні кібербезпеки на фінансових ринках, зокрема в біржовій діяльності. Вони створюють єдині підходи до управління ризиками та забезпечення безпеки інформації, що є критично важливим у середовищі, де обробляються великі обсяги фінансових і персональних даних. Два основних міжнародних стандартів, які регулюють кібербезпеку в багатьох галузях, зокрема й у фінансових, це ISO/IEC 27001 та NIST.

ISO/IEC 27001 є міжнародним стандартом для систем управління інформаційною безпекою (ISMS), який визначає вимоги до створення,

впровадження, підтримки та постійного вдосконалення системи управління безпекою інформації в організаціях. Він дозволяє організаціям, що працюють в умовах високих кіберризиків, розробляти та реалізовувати стратегії, які знижують ймовірність інцидентів безпеки та захищають критично важливу інформацію. Основні елементи стандарту включають:

− оцінку ризиків і уразливостей, що допомагає виявляти можливі загрози для інформаційної безпеки;

− визначення політик безпеки, які повинні регламентувати доступ до інформації, управління інцидентами та інших аспектів безпеки;

− розробку процедур для безпечного обміну інформацією та надійного шифрування даних;

− забезпечення постійного моніторингу, аналізу і вдосконалення заходів безпеки.

NIST (Національний інститут стандартів і технологій) надає набір настанов і стандартів для кібербезпеки, який широко використовується не тільки в США, але й у міжнародній практиці. Одна з основних публікацій NIST − це Cybersecurity Framework (NIST CSF), який складається з п'яти основних функцій: ідентифікація, захист, виявлення, реагування і відновлення, що дозволяє організаціям створити комплексну стратегію кібербезпеки, що охоплює всі етапи від профілактики до відновлення після інциденту.

Стандарти NIST також зосереджуються на таких напрямах, як:

− ризик-менеджмент у сфері кібербезпеки;

− захист даних і забезпечення конфіденційності;

− виявлення загроз, використовуючи передові технології для моніторингу та аналізу;

− оцінка вразливостей та впровадження заходів для їх усунення.

Наслідуючи такі стандарти, фінансові установи можуть створити більш безпечну інфраструктуру, що дозволяє ефективно захищати біржові операції від різноманітних кіберзагроз і забезпечувати стабільність фінансових ринків. Адже, міжнародні стандарти є основою для довіри клієнтів і партнерів до біржових платформ, забезпечуючи високий рівень безпеки, а також відповідність вимогам законодавства і нормативним актам в різних юрисдикціях.

У цьому контексті розробка ефективних планів реагування на кіберінциденти є критично важливою частиною стратегії кібербезпеки для біржових організацій.

Розробка ефективних планів реагування на кіберінциденти є критично важливою частиною стратегії кібербезпеки для біржових організацій. Такі плани дозволяють забезпечити швидку та організовану

відповідь на інциденти, знижуючи їхній вплив на інфраструктуру та фінансові операції.

Основні елементи плану реагування на кіберінциденти:

− першим кроком у реагуванні є своєчасне виявлення інциденту, зокрема його ідентифікація та оцінка. Для цього необхідно мати систему моніторингу, яка дозволяє швидко виявляти аномалії в роботі біржової платформи, такі як невідомі підключення, спроби зловмисного доступу або маніпуляції з торговими даними. Оцінка масштабу інциденту дозволяє визначити пріоритети реагування та визначити ресурсні потреби;

− другим кроком є мобілізація команди реагування. План має чітко визначати роль і обов'язки кожного члена команди реагування, що саме може включати системних адміністраторів, фахівців з кібербезпеки, менеджерів з реагування на інциденти, а також комунікаційні підрозділи для взаємодії з користувачами та регуляторами. Важливо, щоб кожен член команди мав чітке розуміння своєї ролі і знав алгоритм дій у разі інциденту;

− третім кроком є контроль доступу та ізоляція інциденту. Після ідентифікації інциденту важливо забезпечити швидке ізолювання вражених систем, щоб мінімізувати подальше поширення атак, що може включати обмеження доступу до заражених серверів або даних, припинення вразливих з'єднань і обмеження доступу користувачів до важливих торгових платформ;

− четвертим кроком є аналіз причин та відновлення. Після того, як інцидент локалізовано, важливо провести ретельний аналіз причин його виникнення, щоб зрозуміти, яким чином зловмисники змогли проникнути в систему або атакувати її, що дозволяє усунути вразливості та запобігти подібним інцидентам у майбутньому. Відновлення нормальної роботи біржі також є важливим етапом плану, що включає відновлення втрачених даних, перевірку цілісності інформації та забезпечення безперервності фінансових операцій.

− пятим кроком є комунікація та звітність. Під час і після інциденту важливо забезпечити прозору комунікацію з усіма зацікавленими сторонами: користувачами платформи, регуляторами, аудиторами та іншими органами. Випуск офіційних повідомлень про інцидент, опис заходів, що були вжиті для його нейтралізації, і запобігання подібним ситуаціям у майбутньому допомагає зберегти довіру до біржі та забезпечити відповідність вимогам нормативних органів;

− шостим кроком є навчання та тестування. Регулярне тестування та оновлення планів реагування на кіберінциденти є необхідною частиною стратегічного підходу до кібербезпеки, що включає

тренування персоналу, розігрування сценаріїв кіберінцидентів, що дозволяє персоналу краще реагувати в умовах реальної загрози.

Одним із ключових аспектів таких планів є визначення основних елементів реагування на кіберінциденти, зокрема моделювання сценаріїв кібератак та тестування безпеки. Адже, моделювання сценаріїв кібератак та тестування безпеки є важливим компонентом стратегії кібербезпеки для біржових платформ. Отже, всі ці заходи дозволяють оцінити ефективність наявних засобів захисту та підготувати організацію до реальних загроз.

У свою чергу, моделювання кібератак передбачає створення сценаріїв, що симулюють реальні кібератаки на інфраструктуру біржі, що дозволяє перевірити реакцію систем на потенційні загрози і виявити слабкі місця в захисті. Основні типи атак, які можна моделювати:

− атаки типу DDoS (розподілені атаки на відмову в обслуговуванні мають на меті перевантажити сервери біржі, порушивши доступ до торгової платформи;

− фішинг та соціальна інженерія, зокрема моделювання атак, що спрямовані на отримання конфіденційної інформації через підроблені веб-сайти або обман у листах електронної пошти, може допомогти виявити вразливості в системах доступу;

− атаки на внутрішні ресурси, зокрема симуляція атаки на сервери біржі з боку внутрішніх користувачів або через зловмисний код, що дозволяє перевірити, наскільки ефективно система безпеки обмежує доступ до чутливих даних;

− враховуючи поширеність мобільних додатків для торгівлі на біржі, важливо моделювати атаки, націлені на мобільні платформи, щоб перевірити їхню стійкість до різних загроз.

Ефективне моделювання таких атак дозволяє не лише оцінити потенційні загрози, а й підготувати систему до їхньої нейтралізації. Однак для забезпечення належного рівня захисту біржі важливо також регулярно проводити тестування безпеки, яке охоплює всі елементи її інфраструктури.

До основних методів тестування відносяться:

− пенетестація (penetration testing) як метод включає в себе імітацію реальних атак на систему з метою виявлення уразливостей. Пенетестація дозволяє знаходити слабкі місця в системах, що можуть бути використані зловмисниками;

− аудит безпеки допомагає оцінити відповідність біржової інфраструктури міжнародним стандартам і виявити потенційні недоліки в політиках безпеки;

− тестування на проникнення в код націлене на перевірку безпеки програмного коду біржових платформ, виявлення вразливостей, таких як SQL-ін'єкції або XSS-атаки;

− тестування на стійкість до атак до DDoS-атак, перевірка здатності системи підтримувати високі навантаження під час атаки. Важливо також перевіряти здатність відновлення після таких інцидентів.

Моделювання сценаріїв та тестування безпеки дозволяють біржовим організаціям виявити потенційні слабкі місця у своїх системах і забезпечити своєчасне усунення вразливостей до того, як вони можуть бути використані для здійснення реальної атаки, що не лише зміцнює загальний рівень кібербезпеки, але й дозволяє побудувати більш стійку інфраструктуру, готову до реагування на різноманітні загрози.

Таким чином, у сучасному світі кіберзагрози стають одними з найбільших викликів для біржової діяльності. Оскільки фінансові ринки все більше залежать від цифрових технологій, кіберзагрози здатні суттєво вплинути на їх функціонування, стабільність та довіру учасників ринку. Важливо зрозуміти, які конкретно загрози можуть виникати в умовах швидкого розвитку інформаційних технологій, а також які наслідки це може мати для майбутнього біржових операцій.

Один із найбільших ризиків для бірж полягає в можливості атак хакерів на торгові системи. Такі атаки можуть призвести до маніпулювання курсами активів, незаконних операцій або навіть до повної зупинки біржових платформ. Отже, всі ці загрози можуть значно знизити довіру до ринку, особливо якщо такі інциденти стануть регулярними.

Атаки типу DDoS, коли ресурси біржі або фінансової установи перевантажуються великим обсягом трафіку з численних джерел, можуть призвести до тимчасової недоступності торгових платформ, що може викликати не лише фінансові втрати для учасників ринку, а й посіяти паніку серед інвесторів, що знизить стабільність ринку.

Кіберзагрози також можуть включати використання підроблених даних або злом баз даних для маніпулювання цінами активів. Зловмисники можуть здійснювати атаки для створення неправдивих сигналів на ринку, маніпулюючи цінами акцій або валют, що може призвести до штучного спотворення ринкової ситуації та великого рівня невизначеності.

Оскільки біржова діяльність базується на великій кількості чутливої фінансової інформації, одна з найбільших кіберзагроз – це крадіжка особистих даних трейдерів або інвесторів, що може призвести до витоку фінансових даних та незаконних операцій. Крім того, такі інциденти можуть підривають довіру до системи в цілому.

Не менш серйозними є загрози, що виникають від співробітників біржі або торгових платформ. Внутрішні зловмисники можуть маніпулювати даними, знімати інформацію про угоди чи навіть підривати цілісність торгових систем. Така загроза може бути важко виявлена, і її наслідки часто є не менш катастрофічними, ніж зовнішні атаки.

У світі швидких технологічних змін багато країн не встигають оновлювати законодавство, що стосується кібербезпеки та фінансових операцій. У майбутньому це може стати великою проблемою для бірж, оскільки існуючі регуляції не завжди здатні адекватно реагувати на нові типи кіберзагроз.

Загрози, що зростають, призводять до того, що біржі та інші фінансові установи змушені витрачати значні кошти на забезпечення кібербезпеки, розробку стратегій захисту та відновлення після атак. Витрати на безпеку можуть збільшити операційні витрати, що відобразиться на кінцевому результаті біржової діяльності.

Зважаючи на зростання кіберзагроз і необхідність значних інвестицій у захист, постає питання про довгостроковий вплив цих викликів на майбутнє біржової діяльності, а саме:

− зниження довіри інвесторів через кіберзагрози і як наслідок підрив довіри до фінансових ринків. Інвестори потребують впевненості в тому, що їхні кошти будуть в безпеці, а біржі працюватимуть стабільно. Регулярні кіберінциденти можуть знизити цей рівень довіри і змусити учасників ринку шукати більш захищені альтернативи;

− можливе посилення регулювання як відповідь на зростаючі кіберзагрози, уряди та міжнародні організації можуть впровадити нові жорсткіші регулювання щодо кібербезпеки. Біржі будуть змушені витрачати більше ресурсів на відповідність новим стандартам, що може вплинути на їхній фінансовий стан і конкурентоспроможність;

− інновації в області технологій кібербезпеки. Біржі та фінансові інститути змушені будуть інвестувати в новітні технології для забезпечення безпеки, такі як штучний інтелект, машинне навчання, блокчейн для прозорості та криптографічні методи захисту даних, що може призвести до суттєвих змін у структурі фінансових ринків;

− ризики для автоматизованих торгових систем. Автоматизовані торгові системи, алгоритми та штучний інтелект, які використовуються для здійснення торгівлі, можуть стати мішенню для кіберзагроз. Злом таких систем може призвести до непередбачуваних торгових помилок, що потенційно зруйнує ринок.

Отже, підсумовуючи вищесказане, варто зазначити, що кіберзагрози мають великий потенціал вплинути на майбутнє біржової діяльності, адже вони ставлять під загрозу не тільки фінансову стабільність, а й

саму основу довіри до ринків. Для забезпечення безпеки необхідно активно впроваджувати новітні технології кібербезпеки, удосконалювати законодавчі ініціативи та посилювати співпрацю між фінансовими установами для боротьби з кіберзагрозами.

У зв'язку з розвитком технологій та зростанням цифрових загроз, кібербезпека стала критично важливою складовою для забезпечення безпеки фінансових та біржових операцій. Біржова діяльність, що значною мірою залежить від інформаційних технологій, зіштовхується з новими викликами, пов'язаними з кіберзагрозами. Для збереження стабільності та довіри до фінансових ринків необхідно впроваджувати стратегічні підходи до кібербезпеки, які забезпечують захист від сучасних кіберзагроз.

До основних пріоритетів розвитку стратегій кібербезпеки для біржової діяльності відносяться:

- забезпечення цілісності та конфіденційності даних;
- захист інфраструктури від кіберзагроз;
- інтеграція новітніх технологій для підвищення безпеки;
- створення резервних систем для відновлення після атак;
- навчання та підвищення кваліфікації персоналу;
- впровадження технологій блокчейн для забезпечення прозорості;
- співпраця з іншими організаціями і державними структурами;
- адаптація до нормативних вимог та стандартів (рис. 3).

Основною метою є захист даних, які передаються між учасниками біржового ринку, від несанкціонованого доступу та змін. Це включає впровадження ефективних методів шифрування, а також застосування багаторівневої перевірки автентичності користувачів для запобігання можливим атакам.

Рис. 3. Основні пріоритети розвитку стратегій кібербезпеки для біржової діяльності

Джерело: власна розробка

Інфраструктура бірж повинна бути захищена від різноманітних кіберзагроз, таких як атаки типу DDoS, маніпуляції з торговими системами або інші види зловмисних дій. Важливими напрямками є

удосконалення систем моніторингу та детекції загроз, а також оптимізація процесів реагування на інциденти.

Використання штучного інтелекту (AI) та машинного навчання для автоматичного виявлення аномальних або підозрілих дій може значно підвищити рівень безпеки. Такі технології дозволяють оперативно ідентифікувати потенційні загрози, зменшуючи час на реагування.

Підготовка до відновлення операцій після кібернападів є важливою частиною стратегії кібербезпеки. Потрібно розробляти плани відновлення після інцидентів, включаючи резервне зберігання даних та забезпечення швидкої відновлювальної здатності.

Людський фактор є одним з найбільших ризиків для кібербезпеки. Тому необхідно регулярно проводити тренінги для співробітників бірж, аби підвищити їх обізнаність щодо кіберзагроз, методів захисту та реагування на інциденти.

Використання блокчейн-технологій дозволяє підвищити прозорість та безпеку фінансових операцій, що може зменшити ймовірність шахрайства та маніпулювання даними, оскільки блокчейн забезпечує незмінність інформації.

Враховуючи постійне вдосконалення нормативних актів у сфері кібербезпеки, біржі повинні адаптувати свої стратегії до вимог міжнародних стандартів, таких як ISO/IEC 27001, а також до законодавчих вимог з кібербезпеки, які стають обов'язковими для фінансових установ.

Важливою складовою є співпраця з іншими фінансовими установами, державними органами та спеціалізованими компаніями з кібербезпеки для обміну інформацією про нові загрози та кращі практики захисту.

Забезпечення кібербезпеки в біржовій діяльності має бути комплексним процесом, що передбачає постійне вдосконалення та адаптацію до нових викликів та технологічних змін. Стійкість бірж до кіберзагроз є ключовим фактором для забезпечення довіри та стабільності фінансових ринків у майбутньому.

Одним із ключових аспектів забезпечення кіберстійкості бірж є налагодження ефективної співпраці між державними та приватними структурами, що дозволяє об'єднати ресурси та експертизу у боротьбі з кіберзагрозами.

Публічно-приватне партнерство (ППП) стає дедалі важливішим елементом у боротьбі з кіберзагрозами, адже кібербезпека вимагає зусиль з боку як державних органів, так і приватного сектору. Кіберзагрози носять глобальний характер і не обмежуються кордонами однієї країни чи галузі, тому ефективна боротьба з ними потребує скоординованих дій усіх зацікавлених сторін.

Однією з найбільших переваг публічно-приватного партнерства є можливість обміну інформацією між державними органами та приватними компаніями, що працюють у сфері кібербезпеки. В умовах швидкого розвитку нових кіберзагроз, важливо мати оперативний доступ до актуальної інформації, яка допомагає виявляти та запобігати атакам. Приватні компанії, як правило, мають доступ до реальних даних про кіберзагрози, з якими вони стикаються в процесі своєї діяльності, а державні органи можуть забезпечити підтримку на рівні законодавства та регулювання.

Боротьба з кіберзагрозами потребує швидкої та ефективної реакції. ППП дозволяє розробити спільні механізми реагування на інциденти, які можуть виникнути на рівні як окремих організацій, так і на рівні національної або міжнародної кіберінфраструктури. У разі великомасштабних атак важливо мати чіткий план дій, щоб мінімізувати можливі збитки та відновити нормальну роботу систем. Спільні ресурси та скоординовані дії державних і приватних структур можуть значно підвищити ефективність таких операцій.

Приватний сектор, зокрема компанії, що спеціалізуються на інформаційних технологіях та кібербезпеці, володіють передовими технологіями та інноваціями, які можуть бути використані для підвищення рівня безпеки. Державні органи можуть надати підтримку у вигляді правових ініціатив, що сприяють розвитку таких технологій та їх широкому впровадженню в різних сферах. Разом ці два сектори можуть забезпечити стійкість критичної інфраструктури країни до кіберзагроз.

Державні органи можуть сприяти приватному сектору в забезпеченні необхідного фінансування для розробки новітніх технологій захисту від кіберзагроз. Крім того, за допомогою державних ініціатив можна створювати механізми фінансових стимулів для приватних компаній, що займаються розробкою рішень для боротьби з кіберзагрозами, що може включати інвестиції в стартапи, що працюють у галузі кібербезпеки, або надання грантів для впровадження нових технологій.

ППП є важливим інструментом для створення ефективної нормативно-правової бази, що регулює питання кібербезпеки. Взаємодія між державними органами та приватними компаніями дозволяє розробляти закони та стандарти, які забезпечують захист не тільки державної інфраструктури, а й комерційних організацій. Приватний сектор може брати активну участь у створенні норм, які відповідають на вимоги сучасних загроз і технологічних інновацій.

У рамках ППП можливо створювати спільні дослідницькі ініціативи, що сприяють розвитку інновацій у сфері кібербезпеки. Приватний

сектор часто є джерелом технологічних новацій, а державні органи можуть виступати в ролі організаторів, координаторів і фінансистів таких ініціатив. Такі спільні зусилля можуть прискорити створення нових технологій для виявлення та нейтралізації кіберзагроз.

Кіберзагрози не знають кордонів, і тому боротьба з ними потребує міжнародної співпраці. ППП на міжнародному рівні дозволяє обмінюватися інформацією та досвідом між країнами, а також створювати глобальні ініціативи для боротьби з кіберзлочинністю, що може включати обмін інформацією про нові типи загроз, розробку глобальних стандартів безпеки та координацію дій щодо кіберінцидентів.

Таким чином, публічно-приватне партнерство є важливою складовою стратегії боротьби з кіберзагрозами. Тільки спільними зусиллями державних і приватних структур можна створити ефективні механізми для захисту від сучасних кіберризиків. Обмін інформацією, розвиток спільних технологій та підвищення кваліфікації кадрів, що включає лише частину можливостей, які надає ППП. Взаємодія між секторами забезпечить не тільки національну, а й глобальну кіберстабільність, що є необхідним для розвитку цифрової економіки та безпеки у всьому світі.

Регулятори мають важливу роль під час розробки і впровадження стандартів і нормативних актів, що стосуються кібербезпеки у фінансовому секторі. Такі нормативи допомагають фінансовим установам забезпечити належний рівень захисту інформації, що включає управління ризиками, захист даних та виявлення загроз та можуть включати: мінімальні вимоги до кібербезпеки; вимоги до реагування на інциденти; стандарти щодо безпеки даних; плани відновлення після кібератак.

Всі вищевказані нормативні акти сприяють зменшенню кіберризиків та забезпечують більш високий рівень стійкості фінансових установ до кіберзагроз.

ВИСНОВКИ

Таким чином, управління кіберризиками є критично важливим завданням для сучасних бірж, особливо в умовах військових конфліктів та зростання кібератак. Впровадження комплексних стратегій, що включають превентивні заходи, використання сучасних технологій кіберзахисту та дотримання міжнародних стандартів, дозволяє мінімізувати вплив кіберзагроз, захистити фінансову інфраструктуру від атак та забезпечити стабільність ринку навіть у кризових умовах. Критичну роль у підвищенні кіберстійкості фінансового сектору відіграють регулятори. Вони створюють нормативно-правову базу,

здійснюють контроль за виконанням вимог кібербезпеки, а також формують стратегії і політики для забезпечення захисту від кіберзагроз. Спільно з приватним сектором вони можуть забезпечити стабільність і надійність фінансових установ, що є важливою складовою для розвитку економіки і підтримки довіри до фінансових ринків.

Кібербезпека вимагає постійного вдосконалення навичок та знань фахівців. Публічно-приватне партнерство дозволяє створювати програми для навчання та сертифікації кадрів у галузі кібербезпеки, забезпечуючи тим самим кваліфікованих фахівців для ефективної боротьби з кіберзагрозами. Такі програми можуть включати як базові навчання для широкої аудиторії, так і спеціалізовані курси для експертів.

З огляду на глобальний характер кіберзагроз, регулятори повинні активно співпрацювати з іншими національними та міжнародними органами для обміну інформацією про кіберзагрози та кращі практики, що дозволяє швидше реагувати на нові виклики та запроваджувати глобальні стандарти, що підвищують рівень кіберстійкості у фінансовому секторі.

АНОТАЦІЯ

Досліджено проблематику управління кіберризиками у біржовій діяльності в умовах цифрової трансформації та військових дій. Встановлено, що біржові платформи стають вразливими до кібератак, зокрема DDoS-атак, фінансових шахрайств, маніпуляцій ринком, витоків конфіденційної інформації та внутрішніх загроз. Визначено, що особливо актуальними всі ці ризики стають під час військових конфліктів, коли зростає кількість цілеспрямованих атак на фінансову інфраструктуру. Охарактеризовано стратегії управління кіберризиками, серед яких – впровадження новітніх методів моніторингу загроз, розробка ефективних планів реагування, використання штучного інтелекту для виявлення аномалій та посилення міжнародної співпраці. Доведено важливість публічно-приватного партнерства у зміцненні кібербезпеки бірж. Запропоновано адаптивні моделі кіберзахисту, що поєднують регуляторні механізми та технологічні рішення. Результати дослідження можуть бути використані для розробки комплексних стратегій кібербезпеки у фінансовому секторі.

Література

1. Братюк В.П. Сутність кіберризиків та страховий захист від кіберризиків в Україні. *Актуальні проблеми економіки*. 2015. № 9 (171). С. 421–427.

2. Волосович С., Клапків Л. Детермінанти виникнення та реалізації кіберризиків. *Зовнішня торгівля: економіка, фінанси, право.* 2018. № 3. С. 101–115.

3. Гриценко К. Кібербезпека в боротьбі з банківськими шахрайствами: захист споживачів фінансових послуг та зростання фінансово-економічної безпеки України. 2020. URL: https://www.academia.edu/95297712/utm_source= chatgpt.com.

4. Кожедуб Ю. Аналіз документів з керування ризиком кібербезпеки. *Information Technology and Security*. 2017. Vol. 5. № 1. С. 82–95.

5. Приказюк Н.В., Гуменюк Л.С. Кібер-страхування як важливий інструмент захисту підприємств в умовах цифровізації економіки. *Ефективна економіка*. 2020. № 4. URL: http://www.economy.nayka.com.ua/pdf/4_2020/8.pdf.

6. Прокоф'єва О.В., Беспалова Ю. Кібер-ризики та управління ними в умовах глобалізації та цифрової трансформації. *Ефективна еконо*міка. 2024. № 5. URL: https://www.nayka.com.ua/index.php/ee/article/view/3822/3857

7. Селіверстова Л.С., Трухан Д.А. Підходи до розвитку кіберстрахування як сегменту глобального страхового ринку. *Економіка та держава.* 2020. № 1. С. 23–26.

Information about the author:
Kustov Vitaliy Petrovych,
PhD in Management (Specialty 073 «Management»),
Doctoral Student at the Department of Management and Marketing
Private Higher Education Establishment «European University»
16B, Akademika Vernadskoho Blvd, Kyiv, 03115, Ukraine