

Систематизація загроз на всіх етапах життєвого циклу засобів IoT забезпечує основу для створення стійких до кібератак проєктних рішень. Такий підхід дозволяє розробникам впроваджувати превентивні механізми захисту, мінімізуючи вразливості ще до фізичного виходу пристрою на ринок та початку його експлуатації. Попередній аналіз ризиків спрощує інтеграцію засобів моніторингу, підвищує загальну надійність та безпеку використання різноманітних мережевих засобів. Впровадження стандартів кібербезпеки у виробничий цикл гарантує відповідність сучасним вимогам захисту конфіденційної інформації користувачів. Це суттєво зменшує ризики безпеки експлуатації, забезпечуючи тривалу та стабільну експлуатацію засобів IoT у динамічному цифровому середовищі. Таким чином, комплексне визначення ризиків є необхідною умовою безпечного використання масштабованих та надійних технологій IoT та забезпечує перспективи подальшого розвитку відповідних засобів.

Список використаних джерел

1. Anastasia Grishina (2026) *IoT Device Management: Understanding the IoT Lifecycle and Its Stages*. <https://softteco.com/blog/iot-device-management-lifecycle>
2. Brian Russell & Drew Van Duren (2016) *Practical Internet of Things Security*. O'Reilly. Packt Publishing. Birmingham-Mumbai.
3. Gabor Soos & Daniel Kozma & Ferenc Nandor Janky & Pal Varga (2018) *IoT Device Lifecycle – a Generic Model and a use case for Cellular Mobile Networks*. IEEE 6th International Conference on Future Internet of Things and Cloud. Barcelona, Spain.
4. Leila Fatmasari Rahman & Tanir Ozcelebi & Johan Lukkien & Steve McConnel (2018) *Understanding IoT Systems: A Life Cycle Approach*. The 8th International Symposium on Internet of Ubiquitous and Pervasive Things. Procedia Computer Science. pp. 1057–1062.

Романов М.М.,
аспірант спеціальності «С1 Економіка та міжнародні економічні відносини»,
КНЕУ ім. В. Гетьмана, м. Київ, Україна

ОСОБЛИВОСТІ ФОРМУВАННЯ ПОРТФЕЛЯ КІБЕРБЕЗПЕКОВИХ ПРОЄКТІВ ДЛЯ МАЛИХ ТА СЕРЕДНІХ ПІДПРИЄМСТВ

Основні напрями еволюції сучасної портфельної теорії – це вдосконалення вимірювання ризику, введення реалістичних обмежень, багатостадійні постановки, факторна інтеграція та використання алгоритмів для підвищення стабільності, масштабованості й інтерпретованості рішень. У контексті малих та середніх підприємств (МСП) інвестиції в кіберзахист – не ізольовані витрати на окремі засоби, а як портфель взаємопов'язаних проєктів. Їхній «дохід» має специфічну природу: це очікуване зменшення втрат від інцидентів, скорочення простоїв, підвищення відповідності вимогам клієнтів і регуляторів, збереження контрактів та зниження операційної невизначеності. Тому оцінювання інвестиційної привабливості має поєднувати класичну портфельну логіку risk-return із downside-risk, факторним оцінюванням і динамічним переглядом портфеля [1, 2, 6].

Для МСП практично доцільною є гібридна схема: факторна оцінка очікуваної цінності проєкту, сценарний розподіл можливих втрат, оптимізація за критерієм mean-CVaR, обмеження на концентрацію, квартальне або покрокове ребалансування. Така схема враховує обмежений бюджет, дефіцит даних і нестачу фахівців, але не зводить рішення до простого ранжування ініціатив.

Risk-return та інвестиційна цінність кіберпроєктів. Підхід risk-return дає компроміс між очікуваним ефектом і невизначеністю результату. Нехай ω_i – частка бюджету або

імплементативної спроможності, спрямована на проєкт i , μ_i – очікувана нормалізована чиста цінність проєкту, R_p – дохідність портфелю кіберзахисних проєктів, σ_p – загальний ризик портфеля, а V – коваріаційна матриця проєктних результатів, тоді портфель описується через

$$E(R_p) = \omega^T \mu \text{ та } \sigma_p^2 = \omega^T V \omega$$

Для кіберпроєктів μ_i варто трактувати як очікувану чисту економічну вигоду на одиницю вкладення: зменшення очікуваних річних втрат, економія операційних витрат, уникнення штрафів і втрати контрактів мінус витрати на реалізацію:

$$\mu_i = \frac{E(\Delta ALE_i + \Delta OPEX_i + \Delta Revenue_i - Cost_i)}{Cost_i}$$

Слабке місце класичної теорії портфеля Марковіца – нестабільність очікуваних ефектів і поганий опис рідкісних катастрофічних подій. Тому сучасні дослідження посилюють її робастними обмеженнями, сценарним аналізом і CVaR-орієнтованими моделями [1, 2]. Для МСП *це означає, що проєкт з найвищим точковим ROI не повинен автоматично домінувати*, якщо він залежить від одного постачальника, одного бізнес-процесу або має високий ризик затримки.

Ефективність диверсифікації. Сутність диверсифікації в кіберпортфелі полягає у зменшенні концентрації між різними класами загроз, контрольними доменами, активами, постачальниками та бізнес-процесами. Портфель із кількох ініціатив, які всі залежать від одного постачальника або захищають лише один канал атаки, може виглядати різноманітним, але фактично залишатися концентрованим. Тому треба контролювати не лише бюджетні частки, а й внесок кожного проєкту або кластера у сукупний ризик. Для цього придатні внесок проєкту в сукупний ризик портфеля і коефіцієнт диверсифікації. Дослідження стратегій паритету ризику показують, що рівномірніший розподіл ризик-внесків часто стійкіший до помилок параметризації, ніж оптимізація лише за очікуваною дохідністю [3]. У практиці МСП *це перетворюється на прості правила: ліміти ваг одного проєкту, одного вендора або домену контролів, мінімальна кількість різних класів захисту і перевірка структурних залежностей між ініціативами.*

Динамічне ребалансування портфеля. Кіберпортфель не може бути статичним: змінюються загрози, вразливості, регуляторні вимоги, бюджет і стан реалізації проєктів. Динамічне ребалансування означає періодичний або покроковий перегляд ваг із урахуванням нової інформації та витрат на зміну курсу. Підходи прогнозного управління і ковзного горизонту оптимізації показують, що багатоперіодна логіка може бути ефективнішою за одноразовий розподіл ресурсів, особливо коли є трансакційні витрати та зміни режиму ризику [4].

Для МСП оптимальним є квартальний перегляд із покроковими тригерами: істотне зростання CVaR портфеля, критичний інцидент або подія, що ледь не призвела до інциденту, перевищення ліміту концентрації, затримка ключового проєкту понад 20% планового строку, поява нової регуляторної або контрактної вимоги. Ребалансування має враховувати штраф за зміни у структурі портфеля, адже зміна пріоритетів створює витрати на повторні закупівлі, перенавчання персоналу, затримку впровадження та управлінське навантаження.

VaR, CVaR і сценарне оцінювання втрат. VaR показує поріг втрат, який із певною довірою не буде перевищено, тоді як CVaR оцінює середні втрати у хвості розподілу. Для кіберризиків CVaR методологічно сильніший, оскільки кіберінциденти мають важкі хвости. VaR корисний для комунікації з керівництвом як пороговий індикатор, але CVaR краще підходить як критерій оптимізації портфеля [2, 6].

Практична постановка для МСП: *максимізувати очікувану чисту вигоду портфеля з урахуванням штрафу за CVaR₉₅ або CVaR₉₉ та штрафу за зміну ваг.* Достатній стартовий набір сценаріїв охоплює атаку програм-вимагачів, фішинг, компрометацію третьої сторони, невиконання регуляторної вимоги та провал або затримку критичного проєкту. Після кожного сценарію перераховуються CVaR, концентрація, найбільший внесок у ризик і залишковий розрив відновлюваності.

Побудова багатфакторних моделей. Багатфакторна модель потрібна для того, щоб очікувана цінність проекту не була довільною експертною оцінкою. Вона пов'язує результат проекту з ключовими драйверами кіберризiku і бізнес-ефекту. Мінімальна специфікація для МСП може містити шість факторів: інтенсивність загроз; рівень експозиції критичних активів; розрив контролів відносно цільового профілю; ризик третіх сторін; регуляторно-контрактний тиск; ризик самої імплементації. Нехай $R_{i,t}$ – нормалізований економічний ефект кіберпроекту i у періоді/сценарії t , α_i – ефект проекту, не пояснений факторами, $\varepsilon_{i,t}$ – не пояснена, випадкова частина результату проекту у періоді/сценарії, $F_{T,t}$, $F_{E,t}$, $F_{CG,t}$, $F_{TP,t}$, $F_{C,t}$, $F_{I,t}$ – у періоді/сценарії t відповідно інтенсивність актуальних загроз, частка критичних активів/процесів у зоні впливу, розрив контролів відносно цільового профілю, ризик третіх сторін, регуляторно-контрактний тиск, ризик імплементації, а β_{Ti} , β_{Ei} , β_{CGi} , β_{TPi} , β_{Ci} , β_{Ii} – коефіцієнти чутливості результату кіберпроекту i до факторів $F_{T,t}$, $F_{E,t}$, $F_{CG,t}$, $F_{TP,t}$, $F_{C,t}$, $F_{I,t}$ відповідно, тоді спрощений форми нормалізований нетто-ефект проекту:

$$R_{i,t} = \alpha_i + \beta_{Ti}F_{T,t} + \beta_{Ei}F_{E,t} + \beta_{CGi}F_{CG,t} + \beta_{TPi}F_{TP,t} + \beta_{Ci}F_{C,t} + \beta_{Ii}F_{I,t} + \varepsilon_{i,t}$$

Дослідження факторної оптимізації показують, що ощадні факторні моделі знижують шум і покращують позавибіркову якість портфельних рішень [5]. Для МСП це означає: небагато факторів, зрозумілі шкали, регулярне оновлення, перевірка стабільності знаків і обережне використання статистичних методів.

Рекомендована інтегрована рамка. Найбільш придатною для МСП є факторно-обґрунтована mean-CVaR модель з кластерною диверсифікацією та планування з ковзним горизонтом. Вона реалізується у п'ять кроків:

1. Спочатку формується перелік кіберпроектів. Для кожного проекту визначаються вартість, строк, залежності, очікувана вигода та факторний профіль.
2. На другому кроці будується baseline risk profile на основі поточного і цільового профілю кіберзрілості. Тут корисними є рамкові підходи ENISA та NIST [7, 8].
3. Далі формуються сценарії втрат і розраховуються VaR/CVaR.
4. Оптимізуються ваги з лімітами концентрації.
5. Портфель проходить стрес-тести й переглядається щоквартально або за покроковими тригерами.

Отже, інвестиційна привабливість кіберпроекту визначається не лише його індивідуальним ефектом, а й тим, як він змінює профіль ризику портфеля. Найціннішими є проекти, які зменшують хвостові втрати, закривають критичні control gaps, не створюють надмірної концентрації та мають прийнятний ризик впровадження. Для методології це дає перехід від простого ранжування до портфельної оптимізації в умовах обмеженого бюджету й високої невизначеності МСП.

Список використаних джерел

1. Senescall, M., & Low, R. K. Y. (2024). Quantitative portfolio management: Review and outlook. *Mathematics*, 12(18), 2897. <https://doi.org/10.3390/math12182897>
2. Lotfi, S., & Zenios, S. A. (2024). Robust mean-to-CVaR optimization under ambiguity in distributions means and covariance. *Review of Managerial Science*, 18(7), 2115-2140. <https://doi.org/10.1007/s11846-023-00715-z>
3. Ararat, Ç., Cesarone, F., Pinar, M. Ç., & Ricci, J. M. (2024). MAD risk parity portfolios. *Annals of Operations Research*, 336(1), 899–924. <https://doi.org/10.1007/s10479-023-05797-2>
4. Li, X., Uysal, A. S., & Mulvey, J. M. (2022). Multi-period portfolio optimization using model predictive control with mean-variance and risk parity frameworks. *European Journal of Operational Research*, 299(3), 1158–1176. <https://doi.org/10.1016/j.ejor.2021.10.002>
5. Auh, J. K., & Cho, W. (2023). Factor-based portfolio optimization. *Economics Letters*, 228, 111137. <https://doi.org/10.1016/j.econlet.2023.111137>

6. Orlando, A. (2021). Cyber risk quantification: Investigating the role of cyber value at risk. *Risks*, 9(10), 184. <https://doi.org/10.3390/risks9100184>
7. European Union Agency for Cybersecurity. (2021). Cybersecurity for SMEs: Challenges and recommendations. <https://doi.org/10.2824/770352>
8. National Institute of Standards and Technology. (2024). NIST cybersecurity framework 2.0: Small business quick-start guide. <https://doi.org/10.6028/NIST.SP.1300>

Сиротюк А. С.,
здобувачка вищої освіти бакалавр,
Артюшок В. С.,
к.е.н., доцент,
Приватний вищий навчальний заклад
"Міжнародний економіко-гуманітарний університет
імені академіка Степана Дем'янчука"

ВПЛИВ КІБЕРБЕЗПЕКИ НА РЕПУТАЦІЮ СУЧАСНОЇ КОМПАНІЇ

У сучасних умовах кібергігієна та кібербезпека є необхідними складовими діяльності як окремих користувачів, так і компаній. Їх значення зростає разом із розвитком цифрових технологій та збільшенням кількості кіберзагроз. Для бізнесу належний рівень цифрової безпеки важливий не лише для захисту інформації та стабільної роботи систем, а й для підтримання позитивної репутації та довіри клієнтів.

Кібергігієна являє собою систему практичних дій, спрямованих на підтримку безпечного функціонування цифрових ресурсів і захист даних. До таких заходів належать регулярне оновлення програмного забезпечення, використання складних паролів, резервне копіювання інформації, контроль доступу до систем, а також уникнення підозрілих сайтів і електронних повідомлень. Дотримання цих правил дозволяє знизити ризик зараження систем шкідливим програмним забезпеченням та обмежити наслідки можливих атак.

Поняття кібербезпеки охоплює ширший спектр заходів, пов'язаних із захистом комп'ютерних систем, мереж і даних від зовнішніх та внутрішніх загроз. Вона передбачає виявлення вразливостей, управління ризиками, моніторинг цифрової інфраструктури, реагування на інциденти та вдосконалення механізмів захисту. Основним завданням кібербезпеки є забезпечення стабільної роботи інформаційних систем і недопущення несанкціонованого доступу до конфіденційної інформації.

Кібергігієна та кібербезпека мають спільну мету — забезпечення надійного захисту цифрового середовища, проте відрізняються за напрямом застосування. Кібергігієна стосується щоденних правил безпечної роботи користувачів і підтримки цифрових систем, тоді як кібербезпека включає комплексну систему організаційних і технічних заходів протидії кіберзагрозам.

Для сучасної компанії ефективний кіберзахист безпосередньо впливає на її ділову репутацію. Витоки даних, хакерські атаки або неналежний рівень захисту інформації негативно позначаються на довірі клієнтів, партнерів і інвесторів. Саме тому впровадження сучасних механізмів кібербезпеки та дотримання принципів кібергігієни є важливими умовами стабільної діяльності підприємства та підтримання його конкурентоспроможності в цифровій економіці [1, с. 212].

В умовах активного використання хмарних сервісів і поширення віддаленого формату роботи традиційні підходи до захисту корпоративних мереж поступово втрачають ефективність. Через розширення цифрового середовища та відсутність чітких меж мережі використання лише фаєрвольного захисту вже не забезпечує належного рівня безпеки. Саме