УДК 004.056

АДАПТИВНА МЕТОДИКА ОЦІНКИ РІВНЯ КІБЕРБЕЗПЕКИ IT-СЕРЕДОВИЩА МАЛОГО ПІДПРИЄМСТВА

Філенко О.І.[1]; Бабенко Ю.М., доктор філософії[2]; Бабенко М.В., к.т.н., доц.[3]
[1,2] Київський національний університет ім. Т.Шевченко; [3] Дніпровський державний технічний університет
[1,2] Україна, Київ; [3] Україна, Кам'янське
[1] babenkomahalych@gmail.com; [2] yurii.babenko@knu.ua; [3] mvbab@ukr.net

Анотація. *У роботі розглядається проблема розроблення адаптивної методики оцінки рівня кібербезпеки IT-середовища малого підприємства на основі загальних засобів контролю в галузі інформаційних технологій та ISO/IEC 27001. Запропоновано методику оцінювання, що передбачає ряд послідовних етапів: формування профілю підприємства, побудова унікального набору релевантних контролів на основі цього профілю, подальшої їх фільтрації з жорсткими обмеженнями та кінцеве зважене ранжування.*

Ключові слова: *рівень кібербезпеки; мале підприємство; загальні засоби контролю; ISO/IEC 27001.*

Вступ. Малі підприємства залежать від інформаційних технологій так само критично, як і великі корпорації, проте мають суттєво менші ресурси на аудит і побудову повноцінної системи управління інформаційною безпекою (СУІБ). При цьому їхні IT-середовища кардинально різняться: одні компанії використовують виключно хмарні SaaS-сервіси, тоді як інші підтримують власну серверну інфраструктуру, Active Directory та процеси внутрішньої розробки. Аналіз актуальних міжнародних стандартів показує, що ISO/IEC 27001 [1] та ISO/IEC 27002 [2] задають вичерпні вимоги до СУІБ, але не пропонують єдиного адаптивного інструменту для кількісної оцінки рівня захищеності. Загальні засоби контролю в галузі інформаційних технологій (Information Technology General Controls – ITGC), що охоплюють керування доступом, змінами та резервним копіюванням, формалізовані у фреймворках на кшталт COBIT 2019 [3]. Спеціалізовані керівництва для малого бізнесу, такі як NIST Cybersecurity White Paper 50 [4] та CIS Controls v8 [5], є практичними, але здебільшого подані як статичні чек-листи. Вимірювання ефективності заходів безпеки, запропоноване в NIST SP 800-55 [6], також не вирішує проблеми формування інтегральної оцінки, яка б гнучко реагувала на архітектуру конкретного бізнесу.

Мета дослідження. Таким чином, наявні підходи не пропонують єдиної моделі, яка б одночасно поєднувала ITGC та вимоги ISO/IEC 27001 і при цьому враховувала специфіку IT-середовища. Крім того, класичні фреймворки розроблені для корпоративного сектору із суворим розподілом обов'язків і наявністю окремих посадових осіб. Для малого бізнесу такий підхід призводить до хибного заниження рівня безпеки, оскільки суміжні IT-функції там зазвичай виконує один фахівець. Це формує проблему, на розв'язання якої спрямована робота: розроблення адаптивної методики оцінки рівня кібербезпеки IT-середовища малого підприємства на основі контролю ITGC та ISO/IEC 27001.

Основний текст. Для розв'язання цієї проблеми запропоновано та обґрунтовано адаптивну методику оцінювання, яка реалізує послідовну логіку. Спочатку формується профіль підприємства через опитувальник із питаннями про кількість співробітників, модель IT, наявність розробки та обробки персональних даних, що дозволяє нетехнічному користувачу надавати об'єктивну інформацію. На основі цього профілю будується унікальний набір релева-

нтних контролів шляхом відображення ITGC на Додаток A ISO/IEC 27001, активуючи відповідні вимоги (наприклад, щодо безпеки коду чи фізичних серверів) лише за їх фактичної наявності. Далі застосовується фільтрація за жорсткими обмеженнями: невиконання критичних обов'язкових вимог (індивідуальні облікові записи, бекап) обмежує підсумковий рівень зрілості, запобігаючи маскуванню суттєвих прогалин високими оцінками за другорядні заходи. Наостанок здійснюється зважене ранжування за методом аналізу ієрархій [7], де базові експертні ваги коригуються відповідно до сформованого профілю компанії.

У запропонованій методиці оцінюється не формальна наявність окремих посад або формалізованих регламентів, а факт досягнення контрольної мети (наприклад, виконання функцій керування доступом у межах загальних обов’язків системного адміністратора). Це робить оцінку прагматичною та доступною для компаній без штатного фахівця з безпеки.

Висновки. У результаті проведеного дослідження обґрунтовано критерії та логічну послідовність адаптивної методики оцінювання рівня кібербезпеки. Її головна перевага – перехід від статичного чек-листа до динамічної моделі, яка враховує як технологічну архітектуру, так і організаційні реалії малого бізнесу.

Наступним етапом дослідження є розроблення програмного засобу та експериментальна перевірка на модельних підприємствах того, чи сформуються автоматично концептуально різні набори релевантних елементів контролю, вагові коефіцієнти та плани пріоритетних дій щодо підвищення рівня захищеності.

Використання інструментів ШІ. Під час підготовки матеріалів для мовного редагування тексту використовувався інструмент штучного інтелекту ChatGPT.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection – Information security management systems – Requirements* (Standard No. ISO/IEC 27001:2022). https://www.iso.org/ru/standard/27001.

[2] International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection – Information security controls* (Standard No. ISO/IEC 27002:2022). https://www.iso.org/ru/standard/75652.html.

[3] ISACA. (2018). *COBIT 2019 Framework: Introduction & Methodology*. https://www.isaca.org/store2/product/CB19FIMP-C.

[4] Eliot, D., Marron, J., & Thorn, S. (2026). *Small business cybersecurity: Non-employer firms* (NIST Cybersecurity White Paper 50). https://doi.org/10.6028/NIST.CSWP.50.

[5] Center for Internet Security. (2021). *CIS Critical Security Controls Version 8*. https://www.cisecurity.org/controls/v8.

[6] Schroeder, K., Trinh, H., & Pillitteri, V. Y. (2024). *Measurement guide for information security: Volume 1 – Identifying and selecting measures* (NIST Special Publication 800-55v1). https://doi.org/10.6028/NIST.SP.800-55v1.

[7] Saaty, T. L., & Vargas, L. G. (2012). *Models, methods, concepts & applications of the analytic hierarchy process* (2nd ed.). Springer.

Filenko Oleksandra[1], Babenko Yurii[2]; Babenko Mykhailo[3]

An Adaptive Methodology For Assessing The Cybersecurity Level Of A Small Business's IT Environment

Abstract. *This paper addresses the problem of developing an adaptive methodology for assessing the cybersecurity level of a small business’s IT environment based on information technology general controls and ISO/IEC 27001. An evaluation methodology is proposed that involves a series of sequential stages: creating an enterprise profile, developing a unique set of relevant controls based on this profile, subsequently filtering them using strict constraints, and finally performing a weighted ranking.*

Keywords: *cybersecurity level; small business; general controls; ISO/IEC 27001.*