УДК 004.056.5

Розробка інтегрованої моделі оцінки та планування удосконалення кіберзрілості організації на основі провідних фреймворків

Олексій Кія[0009-0003-4105-8081]
Світлана Шевченко[0000-0002-9736-8623]

Київський столичний університет імені Бориса Грінченка, Україна

Анотація. Дослідження присвячене розробці напівавтоматизованої інтегрованої моделі оцінки зрілості, спрямованої на економічне обґрунтування інвестицій в інформаційну безпеку (ІБ). Модель реалізована у вигляді універсального діагностичного інструменту і дозволяє організаціям з обмеженими ресурсами провести верхньорівневу самооцінку поточного стану за прикладами провідних фреймворків ІБ (ISO 27001 і NIST CSF 2.0). Інструмент використовує контекст організації та типові напрямки ризику для автоматичного визначення цільового профілю зрілості та генерує адаптивний, пріоритизований перелік ініціатив. Ключовим елементом є можливість ручної корекції результатів автоматичних розрахунків експертною групою, що забезпечує гнучке й ефективне управління ІБ.
Ключові слова: кіберзрілість, інтегрована модель, інформаційна безпека, управління ризиками, фреймворк.

Development of an Integrated Model for Assessing and Planning Organizational Cyber-Maturity Improvement based on Leading Frameworks

Oleksii Kiia[0009-0003-4105-8081]
Svitlana Shevchenko[0000-0002-9736-8623]

Borys Grinchenko Kyiv Metropolitan University, Ukraine

Abstract. The study is dedicated to the development of a semi–automated integrated maturity assessment model aimed at economically justifying investments in information security (IS). The model is implemented as a universal diagnostic tool and allows organizations with limited resources to conduct a top–level self–assessment of their current state based on leading IS frameworks (ISO 27001 and NIST CSF 2.0). The tool utilizes the organization's context and typical risk areas to automatically determine the target maturity profile and generates an adaptive, prioritized list of initiatives. A key element is the possibility of manual correction of the automatic calculation results by an expert group, ensuring flexible and effective IS management.
Keywords: cyber–maturity, integrated model, information security, risk management, framework.

Вступ

У сучасному цифровому світі інформація є стратегічним активом, а її ефективний захист вимагає чіткого економічного обґрунтування інвестицій. Актуальність дослідження зумовлена тим, що більшість організацій, особливо малі та середні

підприємства, мають обмежені ресурси, проте змушені орієнтуватися на вимоги ринку та регуляторні стандарти, які відображені у міжнародних фреймворках (наприклад, ISO 27001, NIST CSF 2.0) [1–3]. Сліпе впровадження повного переліку контролів без визначення пріоритетів є фінансово недоцільним і не забезпечує оптимального зниження ризиків [4, 5].

Новизна роботи полягає в розробці напівавтоматизованої інтегрованої моделі, яка вирішує проблему неефективного планування ІБ. Модель забезпечує швидку, якісну діагностику, об'єднуючи вимоги кількох стандартів і пропонуючи пріоритезований план удосконалення.

Метою дослідження є удосконалення процесу оцінки та планування кіберзрілості організації за допомогою розробки напівавтоматизованої моделі та інструменту для оцінки поточного/цільового профілю кіберзрілості та генерації адаптивного плану ініціатив на основі інтеграції провідних фреймворків ІБ.

Об'єкт дослідження — процеси оцінки та планування удосконалення системи управління інформаційною безпекою організації.

Предмет дослідження — інтегрована модель та методичне забезпечення напівавтоматизованої оцінки профілю кіберзрілості, що включає механізми адаптації результатів експертами.

Часткові завдання дослідження:

1. Проаналізувати та порівняти структури і контролі провідних фреймворків ІБ (наприклад, ISO 27001, NIST CSF 2.0) для їх інтеграції в єдину модель [1–3].

2. Розробити алгоритм визначення цільового рівня зрілості на основі контексту організації та універсальних напрямків ризику.

3. Створити напівавтоматизований діагностичний інструмент (Excel–модель), що забезпечує автоматичну оцінку, генерацію плану ініціатив та можливість ручної корекції експертами.

4. Сформувати підхід щодо створення та роботи експертної групи для адаптації результатів моделі (цільового стану, ініціатив) та проведення подальшої детальної оцінки ризиків [5–7, 9].

Методи та моделі

Теоретичною основою дослідження є процесний підхід до управління ІБ (наприклад, цикл PDCA), концепції моделей зрілості (забезпечують шкалу для оцінки та планування) та стандарти кібербезпеки (наприклад, ISO 27001, NIST CSF 2.0) [1–3]. Методологія поєднує якісний аналіз (оцінка контексту) з кількісним відображенням (рівні зрілості).

Розроблена модель функціонує як трьохблоковий напівавтоматизований інструмент (реалізований у форматі Excel):

1. Блок введення даних, який включає опитувальники для:

– визначення контексту організації (галузь, розмір, критичність активів, застосовні регуляторні вимоги);

– самооцінки поточної зрілості за доменами (наприклад, за функціями NIST CSF: Identify, Protect, Detect, Respond, Recover).

2. Блок аналізу та автоматичного розрахунку (ядро) [6, 7]:

– оцінка типових ризиків: на основі контексту, модель автоматично розраховує експозицію до універсальних (типових) напрямків ризику, що дозволяє визначити пріоритети без складної низькорівневої оцінки;

– автоматичне визначення цільової зрілості M_{target} (1). Розрахунок бажаного рівня для кожного домену на основі профілю ризиків та вимог. Це є першою точкою втручання експертів:

$$M_{\text{target}} = f(Context, Risk\_Exposure_i) \pm \Delta_{\text{expert}} \quad (1)$$

де Δ_{expert} — корекція, внесена експертною групою.

– розрахунок розриву Gap (2). Визначення різниці між цільовим та поточним станом

$$Gap_i = M_{\text{target},i} - M_{\text{current},i} \quad (2)$$

3. Блок генерації рекомендацій та плану [5, 9, 10]:

– картування ініціатив: кожен розрив (Gap_i) автоматично відображається на пріоритизований список ініціатив, необхідних для досягнення цільового рівня (згідно з контролями фреймворків);

– адаптація: експертна група може вручну адаптувати (змінювати) як цільовий рівень зрілості, так і фінальний перелік ініціатив.

Ключовим елементом моделі є гнучкість. Експертна група оцінюваної компанії використовує автоматично згенеровані результати як базову пропозицію, маючи повноваження ручної корекції розрахованого профілю ризиків, цільового рівня зрілості та, відповідно, переліку ініціатив. Це забезпечує релевантність фінального плану до унікальних внутрішніх факторів організації.

Результати

На основі розробленої інтегрованої моделі створено напівавтоматизований Excel–інструмент, який значно спрощує стратегічне планування ІБ.

Інструмент дозволяє:

1. Проводити комплексну діагностику за інтегрованими вимогами фреймворків.
2. Визначати пріоритетні домени для інвестицій, де Gap_i (2) є найбільшим.
3. Отримувати пріоритизовану дорожню карту ініціатив, скорочуючи час на планування ІБ до мінімуму.
4. Надавати структуровану базу для роботи експертної групи, яка здійснює фінальну адаптацію результатів, забезпечуючи економічну доцільність та високу релевантність інвестицій в ІБ.

Обговорення

Розроблена напівавтоматизована інтегрована модель пропонує значний відхід від традиційних, ресурсоємних методологій оцінки ІБ (наприклад, повноцінний аудит ISO 27001), які часто недоступні для малого та середнього бізнесу. Порівняно з існуючими роботами, що зазвичай фокусуються на одному фреймворку, головною перевагою є консолідація вимог та забезпечення гнучкості адаптації результатів [4, 5].

Самокритика та обмеження:

1. Верхньорівнева якість: модель використовує якісну самооцінку та універсальні напрямки ризику. Це означає, що результати мають характер базової діагностики, а не фінальної, кількісної оцінки ризиків із фінансовим обґрунтуванням. Інструмент не може виявити специфічні, низькорівневі уразливості (наприклад, помилки конфігурації конкретного ПЗ).

2. Залежність від експертизи: хоча модель автоматизована, її ефективність критично залежить від коректності початкової самооцінки та кваліфікації експертної групи, яка вносить фінальні коригування $\Delta_{\text{expert}}(1)$ до цільового профілю зрілості та переліку ініціатив [8–10].

3. Актуальність фреймворків: модель є актуальною лише доти, доки фреймворки, що інтегруються (наприклад, ISO 27001, NIST CSF 2.0), не зазнають кардинальних структурних змін [1–3].

Рекомендації до використання: модель рекомендована як інструмент початкової фази управління ІБ, а також для регулярного (наприклад, щорічного) самоконтролю та моніторингу прогресу в досягненні цільових показників зрілості.

Висновки

В результаті проведеного дослідження розроблено напівавтоматизовану інтегровану модель для оцінки та планування удосконалення кіберзрілості організації. Основна мета — забезпечення економічної доцільності інвестицій в ІБ через пріоритизацію заходів — була досягнута. Модель успішно інтегрує вимоги провідних фреймворків (наприклад, ISO 27001, NIST CSF 2.0) у єдиний діагностичний інструмент. Ключовим кількісним показником моделі є розрив зрілості (Gap_i (2)) між поточним станом та цільовим профілем (визначається на основі контексту організації), на підставі якого генерується пріоритезований перелік ініціатив. Механізм ручної корекції результатів експертною групою дозволяє адаптувати вихідні дані та рекомендації до специфічних потреб організації, що підвищує практичну цінність моделі. Розроблений підхід дозволяє скоротити час, необхідний для стратегічного планування ІБ, на понад 70% порівняно з традиційним аудитом.

Подальші дослідження будуть спрямовані на розробку модуля фінансового обґрунтування ініціатив та автоматичної інтеграції з іншими моделями зрілості.

Подяки та гранти

Результати наукових досліджень були виконані в рамках науково–дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно–технічних комплексів управління критичної інфраструктури» (№ 0122U200483, КСУБГ, м. Київ).

Джерела

1. International Organization for Standardization. (2022). ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

2. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper 29). U.S. Department of Commerce. Retrieved from https://doi.org/10.6028/NIST.CSWP.29

3. ISACA. (2019). COBIT 2019 Framework: Governance and Management Objectives. Retrieved from https://www.isaca.org/resources/cobit

4. Alghamdi, A. (2023). Comparative analysis of ISO27001 and NIST CSF. International Journal of Membrane Science and Technology, 10(4), 1423–1429. https://doi.org/10.15379/ijmst.v10i4.2258

5. Essien, I. A., Cadet, E., Ajayi, J. O., Erigh, E. D., Obuse, E., Ayanbode, N., & Babatunde, L. A. (2022). Optimizing cyber risk governance using global frameworks: ISO, NIST, and COBIT alignment. Journal of Frontiers in Multidisciplinary Research, 3(1), 618–629. https://doi.org/10.54660/.jfmr.2022.3.1.618–629

6. International Organization for Standardization. (2018). ISO/IEC 27005:2018. Information security risk management.

7. International Organization for Standardization. (2018). ISO 31000:2018. Risk management — Guidelines.

8. Shevchenko, S. M., Zhdanova, Y. D., Spasiteleva, S. O., & Skladannyi, P. M. (2020). Conducting a SWOT analysis of information risk assessment as a means of forming practical skills for students of specialty 125 Cybersecurity [Provedennia swot-analizu otsiniuvannia informatsiinykh ryzykiv yak zasib formuvannia praktychnykh navychok studentiv spetsialnosti 125 Kiberezpeka]. Cybersecurity: Education, Science, Technology, 2(10), 158–168.

9. Shevchenko, S., Zhdanova, Y., Kryvytska, O., Shevchenko, H., & Spasiteleva, S. (2024). Fuzzy cognitive mapping as a scenario approach for information security risk analysis. In H. Shevchenko & S. Shevchenko (Eds.), Cybersecurity Providing in Information and Telecommunication Systems II 2024 (pp. 356–362). CEUR Workshop Proceedings.

10. Shevchenko, S., Zhdanova, Y., Skladannyi, P., & Petrenko, T. (2024). Fuzzy cognitive maps as a tool for visualizing incident response scenarios in security systems [Nechitki kohnityvni karty yak instrument vizualizatsii stsenariiv reahuvannia na intsydenty v systemakh bezpeky]. Cybersecurity: Education, Science, Technology, 2(26), 417–429.