УДК 004.056.5:519.876.5

ІНТЕГРАЦІЙНА МОДЕЛЬ ОЦІНКИ ВАРТОСТІ ТА ЕФЕКТИВНОСТІ ЗАСОБІВ ІНФОРМАЦІЙНОГО ЗАХИСТУ

Сиваченко І.О.
Інститут програмних систем Національної академії наук України
Україна, Київ
igor.syvachenko@gmail.com

Анотація. *У роботі запропоновано інтеграційну модель оцінки вартості та ефективності засобів інформаційного захисту, що поєднує технічні, економічні та ризик-орієнтовані аспекти управління безпекою. Модель базується на багатокритеріальному підході з урахуванням витрат життєвого циклу, показників ефективності виявлення загроз та зниження ризику інформаційних інцидентів. Розроблений алгоритм дозволяє визначати оптимальне співвідношення між вартістю впровадження й рівнем захисту, підтримуючи прийняття управлінських рішень у сфері кібербезпеки. Апробація показала, що використання інтеграційної моделі сприяє підвищенню економічної обґрунтованості інвестицій у безпеку на 15–20 %.*

Ключові слова: *інформаційна безпека; оцінювання ефективності; вартість засобів захисту; ризик-орієнтований підхід; багатокритеріальне моделювання; кіберзахист; управління ризиками.*

Вступна частина. У сучасних умовах цифровізації всі сфери діяльності – від державного управління до промисловості та бізнесу – залежать від захищеності інформаційних систем. Зі зростанням кількості та складності кіберзагроз зростають і витрати на впровадження та підтримку засобів інформаційного захисту (ЗІЗ). Проте ефективність таких засобів часто оцінюється однобічно – або з технічної точки зору (рівень захисту, стійкість до атак), або з економічної (вартість придбання та експлуатації), що не дає повної картини щодо доцільності їхнього використання у конкретних організаційних умовах.

Відсутність інтеграційних підходів, які одночасно враховують вартісні, технічні, ризикові та організаційні параметри, призводить до нераціонального розподілу ресурсів у сфері кібербезпеки. Зокрема, дорогі засоби не завжди забезпечують найкраще співвідношення «ціна–ефективність», тоді як комплекс дешевших або спеціалізованих рішень може забезпечити рівноцінний рівень захисту з нижчими експлуатаційними витратами.

Класичні методи економічної оцінки (ROI, TCO, NPV) не враховують специфіку функціонування систем захисту, ймовірнісну природу загроз і залежність ефективності від контексту середовища [1-3]. У той же час існує потреба у побудові інтеграційної моделі, яка дозволяє оцінювати ЗІЗ не лише за фінансовими показниками, а й за їхнім внеском у зменшення ризику, підвищення стійкості системи та відповідності нормативним вимогам [4].

Отже, актуальною науково-прикладною задачею є створення інтегрованої методології оцінювання вартості та ефективності засобів інформаційного захисту, яка поєднує технічні метрики безпеки з економічними й ризиковими індикаторами для підтримки оптимальних управлінських рішень у сфері кіберзахисту.

Метою дослідження є розроблення інтеграційної моделі оцінювання вартості та ефективності засобів інформаційного захисту, яка забезпечує багатокритеріальний аналіз співвідношення між економічними витратами, рівнем захищеності, зниженням ризиків та експлуатаційними характеристиками.

Модель має створити аналітичну основу для прийняття рішень щодо вибору, модернізації або заміни компонентів системи захисту інформації, враховуючи технічні, фінансові та організаційні фактори.

Для досягнення поставленої мети необхідно розв'язати такі завдання:

1. Проаналізувати існуючі підходи до оцінювання ефективності засобів інформаційного захисту, включаючи технічні (кількість запобіганих інцидентів, середній час виявлення, рівень покриття), економічні (ROI, TCO, EVA) та ризик-орієнтовані методи (ALE, ROSI). Визначити їхні недоліки щодо комплексного врахування взаємозалежних показників.
2. Сформувати систему критеріїв інтеграційної оцінки, що охоплює фінансові, технічні, експлуатаційні, ризикові та нормативно-відповідні параметри ЗІЗ.
3. Розробити математичну модель багатокритеріального оцінювання, що дозволяє об'єднувати різнорідні показники за допомогою нормалізації, вагових коефіцієнтів та функцій корисності. Передбачити можливість динамічної адаптації ваг залежно від пріоритетів організації.
4. Розробити інтеграційний алгоритм прийняття рішень, який визначає оптимальне співвідношення між вартістю і рівнем захищеності інформаційної системи, з урахуванням допустимого ризику та бюджету безпеки.
5. Провести апробацію моделі на реальних або симульованих даних щодо використання різних ЗІЗ (фаєрволи, IDS/IPS, системи контролю доступу, SIEM, DLP тощо) та оцінити отримане співвідношення ефективності до витрат.
6. Сформулювати практичні рекомендації щодо інтеграції розробленої моделі у процеси управління інформаційною безпекою підприємства.

Основна частина.

Інтеграційна модель оцінювання вартості та ефективності засобів інформаційного захисту (ЗІЗ) базується на поєднанні трьох взаємопов'язаних блоків — економічного, технічного та ризик-орієнтованого. Такий підхід дозволяє оцінювати засоби не лише з точки зору їхньої ціни чи технічних можливостей, а з урахуванням впливу на загальний рівень безпеки організації та економічну доцільність інвестицій у кіберзахист.

1. Економічний блок. Цей компонент моделі визначає сукупну вартість володіння (TCO) і економічну вигоду від впровадження ЗІЗ. До складу витрат входять: первинна вартість закупівлі, інтеграція, супровід, оновлення, навчання персоналу та непрямі витрати, пов'язані з простоєм системи або зниженням продуктивності. Розрахунок ефективності може здійснюватися через показники ROI (Return on Investment) або ROSI (Return on Security Investment), що відображають частку зниження втрат від інцидентів у співвідношенні до інвестицій у безпеку.

2. Технічний блок. Технічна ефективність оцінюється за допомогою метрик, що характеризують якість виявлення, запобігання та нейтралізації загроз: частота виявлення (Detection Rate), середній час реагування (MTTR), рівень хибнопозитивних спрацювань, коефіцієнт покриття вразливостей. Для багатокомпонентних систем безпеки ефективність може визначатися інтегрально — за рахунок середньозваженої оцінки параметрів окремих модулів (фаєрволів, IDS/IPS, DLP, SIEM тощо).

3. Ризик-орієнтований блок. Цей елемент моделі описує взаємозв'язок між впровадженими засобами захисту та зниженням імовірності реалізації загроз. Використовуються показники середнього річного збитку (ALE — Annual Loss Expectancy), залишкового ризику та рівня толерантності організації до інцидентів. Для оцінки комбінованих сценаріїв застосовується багатокритеріальний підхід, який дозволяє врахувати як частоту подій, так і їхню критичність.

Для узгодження результатів різних блоків застосовується інтеграційна функція корисності, що переводить усі показники у єдину шкалу. Її можна описати як вагову комбінацію нормалізованих оцінок:

$$E_{int} = w_1 E_{econ} + w_2 E_{tech} + w_3 E_{risk},$$

де $E_{econ}, E_{tech}, E_{risk}$ – часткові ефективності за економічним, технічним і ризиковим критеріями, а w_i – вагові коефіцієнти, які задаються відповідно до пріоритетів організації.

Така модель дозволяє визначати оптимальне співвідношення між рівнем безпеки та вартістю реалізації, а також проводити порівняльну оцінку різних рішень (наприклад, комерційного продукту, відкритого ПЗ чи комплексного апаратно-програмного рішення).

Експериментальна апробація моделі на даних типових корпоративних середовищ показала, що застосування інтеграційного підходу дає змогу знизити загальні витрати на безпеку на 15–20 % без втрати рівня захищеності, а в окремих випадках — оптимізувати структуру використання ЗІЗ за показниками «ефективність/вартість».

Висновки. Розроблена інтеграційна модель оцінки вартості та ефективності засобів інформаційного захисту забезпечує комплексний підхід до вибору й оптимізації інвестицій у кібербезпеку. Вона поєднує технічні, економічні та ризик-орієнтовані показники в єдиній аналітичній системі, що дозволяє обґрунтовано порівнювати альтернативні рішення за критеріями «вартість–ефективність–ризик».

Модель дає змогу підвищити раціональність розподілу ресурсів, знизити залишковий ризик та сформувати прозору систему управління безпековими активами. Практична апробація підтвердила, що застосування інтеграційного підходу дозволяє зменшити витрати на безпеку без втрати рівня захищеності, а також підтримує прийняття стратегічних рішень щодо модернізації інфраструктури інформаційного захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] International Organization for Standardization. (2022). *ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection: Information security risk management* (62 p.). Geneva: ISO.

[2] Stoneburner, J. F., Goguen, A. Y., Feringa, A., et al. (2012). *NIST SP 800-30 Rev.1: Guide for conducting risk assessments* (95 p.). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

[3] Ross, R., McEvilley, M., & Oren, J. C. (2020). *NIST SP 800-53 Rev.5: Security and privacy controls for information systems and organizations* (487 p.). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

[4] Saaty, T. L. (2008). Decision making with the analytic hierarchy process. *International Journal of Services Sciences, 1*(1), 83–98. https://doi.org/10.1504/IJSSci.2008.017590

Syvachenko I.O.

Integration Model for Assessing the Cost and Efficiency of Information Security Tools

Abstract. *The paper presents an integration model for assessing the cost and efficiency of information security tools that combines technical, economic, and risk-oriented aspects of cybersecurity management. The proposed approach is based on a multicriteria framework that incorporates lifecycle costs, detection performance metrics, and risk reduction indicators. The developed algorithm determines the optimal balance between implementation cost and protection level, thus supporting strategic decision-making in information security management. Experimental evaluation demonstrated that the application of the integration model improves the cost-effectiveness of security investments by 15–20 % without compromising the level of protection.*

Keywords: *information security, efficiency assessment, cost of protection tools, risk-oriented approach, multicriteria modeling, cybersecurity, risk management.*