ОБГРУНТУВАННЯ ПІДХОДУ ЩОДО ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Пашкова А.В., Добринін І.С.

Харківський національний університет радіоелектроніки,
кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Україна.

E-mail: anhelina.pashkova@nure.ua,
ihor.dobrynin@nure.ua

Abstract

The correct construction of an information security management system is of key importance for the protection of critical data and the smooth operation of the organization. ISMS allow to identify and minimize the risks associated with information threats, prevent security incidents and protect the confidentiality, integrity and availability of data. A properly built system ensures compliance with legal and regulatory requirements, promotes increased trust on the part of customers and partners, and also forms the basis for continuous monitoring and adaptation to new threats. This paper proposes an approach to determining an appropriate methodology for building an ISMS, and presents the results in the form of tables.

Система управління інформаційною безпекою (СУІБ) це частина загальної системи управління, яка засновується на підході, що базується на ризиках, і призначена для встановлення, впровадження, підтримання та постійного покращення інформаційної безпеки [1]. Основна мета СУІБ – створити комплексну та стійку інфраструктуру, яка забезпечує конфіденційність, цілісність та доступність інформації. Вона може бути побудована на власний розсуд керівника, за вимогами законодавчих документів, управлінських документів та інше.

Для ефективної побудови та управління СУІБ існує декілька різних методів та підходів, які можуть бути побудовані на основі вимог керівника, партнерів, міністерств, міжнародних організацій, тощо. Ці методи допомагають структурувати процеси, оптимізувати ресурси та керувати ризиками. Аналіз літератури за предметною областю показав, що більш широко вживаними є підходи, які ґрунтуються на вимогах лінійки стандартів ISO/IEC 27000, стандартів лінійки серії NIST, методології IT-Grundschutz та інших. З іншого боку, побудова систем управління інформаційною безпекою це є ітераційний процес, який передбачає визначення кращого шляху реалізації її окремих вимог. Саме визначення такого шляху вирішує мережевий аналіз. Тому, в даній роботі пропонується проаналізувати підходи до побудови СУІБ такі як: ISO/IEC 27001, NIST SP 800-53, IT-Grundschutz та мережевий аналіз.

Метою роботи є визначення кращого підходу щодо побудови СУІБ, що є багатокритеріальною задачею, яка полягає у визначенні підходів щодо вибору кращого варіанту. В теорії математики показано, що для вирішення даного класу задач найбільш ефективним та вживаним є застосування методу аналізу ієрархій Томаса Сааті [2].

Загальна ідея цього методу полягає в декомпозиції проблеми вибору на більш прості складові та обробку суджень особою, яка приймає рішення. Через міркування визначається відносна значимість досліджуваних альтернатив за всіма критеріями, що є в ієрархії. Альтернативний варіант, вага якого максимальна, вважається найкращим.

Відповідно до методу аналізу ієрархій першим кроком є визначення цілі, основних критеріїв та альтернатив. Ціллю є визначення методології, як основи для побудови систем управління інформаційною безпекою. Основними критеріями оберемо гнучкість, складність впровадження, вартість, універсальність вимог, інтеграцію з іншими стандартами/методологіями, управління ризиками. Основними альтернативами є ISO/IEC 27001, NIST SP 800-53, IT-Grundschutz та мережевий аналіз. На

основі зазначених даних створимо ієрархію, тобто древо критеріїв та альтернатив, яке надано на рисунку 1, яке наочно показує взаємозв'язки між компонентами даного методу.

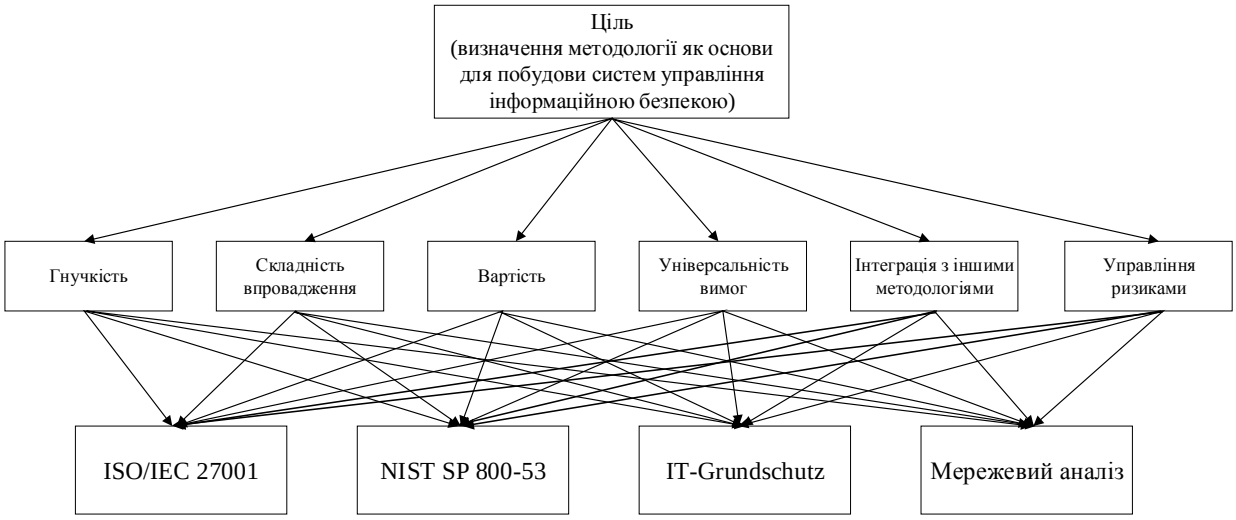

Рис. 1. Древо критеріїв та альтернатив

Другим кроком при розрахунку є формування матриці попарних порівнянь, зі значеннями в матриці від 1 до 9, де 1 у випадку якщо порівнювані підходи за аналізованим критерієм однаково кращі і 9 – якщо один із підходів має абсолютну перевагу в порівнянні з іншим за відповідним критерієм. Наприклад мережевий аналіз є найбільш гнучким через свою адаптивність до змін завдяки своїй здатності динамічно оновлювати залежності між вузлами та пріоритетами. У той час як стандарти, такі як ISO/IEC 27001 [3] та NIST SP 800-53 [4], мають більш жорстко закріплену структуру, мережевий підхід забезпечує гнучкішу реакцію на нові ризики та зміни в середовищі. IT-Grundschutz, у свою чергу, є більш гнучким ніж ISO/IEC 27001 та NIST SP 800-53 через модульну структуру, каталог заходів та можливість імплементації, однак він є гіршим за критерієм гнучкості, ніж мережевий аналіз. Незважаючи на модульність, IT-Grundschutz все ще має певну фіксовану структуру, що може обмежувати адаптацію під час значних змін у загрозах чи бізнес-середовищі [5].

Для вирішення задачі був проведений аналіз кожного з критеріїв. Проведено розрахунок вагового стовпця критеріїв за метою. Для цього складені аналогічні матриці порівняння варіантів (альтернатив) за кожним із критеріїв. Знайдена сума елементів кожного стовпця.

Нехай $K_1...K_n$ – безліч критеріїв з n елементів, тоді $W_1...W_n$ – інтенсивності прояву цих елементів. Тоді розрахунок ваги критеріїв відбувається за формулою [2]:

$$B_n = \frac{P_n}{S}, \tag{1}$$

де P_n розраховується за формулою:

$$P_n = \sqrt[n]{1 \cdot \frac{W_n}{W1} \cdot \ldots \cdot \frac{W_n}{W2}}; \tag{2}$$

S – у свою чергу розраховуються за формулою:

$$S = \sum_{i=1}^{n} P_i. \tag{3}$$

Далі поділені усі елементи матриці на суму елементів відповідного стовбця, як у формулі (1) та внесені в таблицю 1.

Таблиця 1. Матриця ваг альтернатив за кожним критерієм

Стандарт	Гнучкість	Універсальність	Управління ризиками	Вартість	Складність	Інтеграція
Мережевий аналіз	0,66	0,55	0,047	0,58	0,517	0,53
IT-Grundschutz	0,17	0,25	0,145	0,24	0,262	0,27
NIST SP 800-53	0,09	0,12	0,312	0,09	0,131	0,11
ISO/IEC 27001	0,08	0,08	0,496	0,09	0,09	0,09

Аналогічно за даними розрахунками були знайдені ваги кожного критерія а саме: гнучкість, вага якого дорівнює 44,5 %, універсальність – 23,9 %, управління ризиками – 14,4 %, вартість – 8,9 %, складність – 5,3 % та інтеграція з іншими методиками – 3 %. Відповідно до методу аналізу ієрархій передбачається визначення ваг альтернатив. Для цього перемножимо отриману матрицю на стовпець. Результати розрахунків надано нижче.

$$C = A \cdot B = \begin{pmatrix} 0{,}66 & 0{,}55 & 0{,}04 & 0{,}58 & 0{,}51 & 0{,}53 \\ 0{,}17 & 0{,}25 & 0{,}14 & 0{,}24 & 0{,}26 & 0{,}27 \\ 0{,}09 & 0{,}12 & 0{,}31 & 0{,}09 & 0{,}13 & 0{,}11 \\ 0{,}08 & 0{,}08 & 0{,}49 & 0{,}09 & 0{,}09 & 0{,}09 \end{pmatrix} \cdot \begin{pmatrix} 0{,}445 \\ 0{,}238 \\ 0{,}144 \\ 0{,}088 \\ 0{,}052 \\ 0{,}03 \end{pmatrix} = \begin{pmatrix} 0{,}5252 \\ 0{,}1998 \\ 0{,}1336 \\ 0{,}1414 \end{pmatrix}.$$

Результати розрахунків показують, що ваги альтернатив із погляду досягнення поставленої мети дорівнюють:

- Мережевий аналіз дорівнює 0,5252 або 52,52 %;
- IT-Grundschutz – 0,1998 або 19,98 %;
- NIST SP 800-53 – 0,1336 або 13,36 %;
- ISO/IEC 27001 – 0,1414 або 14,14 %.

Таким чином, аналіз, проведений у даній роботі, показує, що відповідно до прийнятих припущень, методологічним підґрунтям для побудови СУІБ краще обрати підхід, який використовується у мережевому аналізі, так як його значення за критеріями гнучкості становить у 66 %, універсальності у 55 %, управління ризиками у 4,7 %, вартості впровадження у 58%, складності впровадження у 51,7 %, інтеграції з іншими методологіями у 53 %, що робить підсумковий відсоток у 52,52 %.

Отже, в даній роботі була визначена базовий підхід для побудови СУІБ за критеріями гнучкості, універсальності, управління ризиками, вартості, складності та інтеграції. Проведені розрахунки показали, що для вирішення поставленої задачі, в якості базової методики, доцільно використовувати мережевий аналіз.

Література

1. ISO/IEC 27000 Information security management. URL : https://www.iso.org/standard/27000 (дата звернення: 15.09.2024).
2. Saaty, T. L. The Analytic Hierarchy Process / T. L. Saaty. – New York: McGraw-Hill International, 1980. 287 с.
3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. URL : https://www.iso.org/standard/27001 (дата звернення: 15.09.2024).
4. SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. URL : https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.html (дата звернення: 15.09.2024).
5. BSI IT-Grundschutz – Informationssicherheit mit System. URL : https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html (дата звернення: 15.09.2024).