УДК 004.056

Д. С. Джумела

АНАЛІЗ МЕТОДІВ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Вінницький національний технічний університет

Анотація

У роботі розглянуто сучасні підходи до оцінювання ефективності систем захисту інформації (СЗІ). Проаналізовано підходи до визначення кількісних та якісних показників ефективності, що дозволяють оцінити рівень захищеності інформаційних ресурсів і надійність роботи засобів захисту. Також досліджено особливості використання різних методів оцінювання та їх значення для забезпечення стабільної роботи інформаційно-телекомунікаційних систем.

Ключові слова: система захисту інформації, інформаційна безпека, ефективність СЗІ, оцінювання ефективності, кількісні методи, якісні методи, інформаційно-телекомунікаційні системи.

Abstract

The paper considers modern approaches to assessing the effectiveness of information protection systems (IPS). The approaches to determining quantitative and qualitative performance indicators that allow assessing the level of security of information resources and the reliability of the operation of protection tools are analyzed. The features of using various assessment methods and their importance for ensuring the stable operation of information and telecommunication systems are also investigated.

Keywords: information protection system, information security, effectiveness of information security systems, effectiveness assessment, quantitative methods, qualitative methods, information and telecommunication systems.

Вступ

У сучасних інформаційних системах обробляється великий обсяг даних, що можуть мати різний ступінь важливості та конфіденційності. Із розвитком комп'ютерних мереж, цифрових сервісів та інформаційних технологій постійно зростає кількість загроз, пов'язаних із несанкціонованим доступом до інформації, її зміною, пошкодженням або повним знищенням. У таких умовах особливого значення набуває впровадження ефективних систем захисту інформації, які здатні забезпечити належний рівень безпеки під час зберігання, обробки та передавання даних.

Система захисту інформації (СЗІ) являє собою впорядковану сукупність об'єктів і суб'єктів захисту, методів, засобів та організаційних заходів, спрямованих на забезпечення безпеки інформаційних ресурсів. Оскільки система визначається як сукупність взаємопов'язаних елементів, основне призначення СЗІ полягає в об'єднанні всіх складових захисту в єдиний комплекс, у якому кожен елемент виконує власні функції та водночас сприяє ефективному функціонуванню інших компонентів, перебуваючи з ними у логічному й технологічному взаємозв'язку [1]. Використання окремих засобів захисту без їх правильного та комплексного поєднання не завжди забезпечує достатній рівень безпеки, що може зменшувати загальну ефективність системи захисту.

Таким чином, важливим завданням є визначення ефективності роботи систем захисту інформації. Оцінювання ефективності СЗІ здійснюється за допомогою кількісних і якісних показників, які показують рівень захищеності інформаційних ресурсів, надійність роботи засобів захисту та здатність системи протидіяти можливим загрозам і забезпечувати стабільну роботу інформаційно-телекомунікаційних систем.

Мета роботи – проаналізувати сучасні методи оцінювання ефективності систем захисту інформації та визначити їх особливості застосування для встановлення кількісних і якісних показників рівня захищеності інформаційних ресурсів.

Результати дослідження

Оцінювання ефективності СЗІ є важливим етапом управління інформаційною безпекою, оскільки дозволяє визначити, наскільки застосовані засоби та механізми захисту забезпечують необхідний рівень конфіденційності, цілісності та доступності інформації. У практиці інформаційної безпеки

оцінювання ефективності передбачає аналіз відповідності впроваджених заходів безпеки актуальним загрозам, виявлення вразливостей системи та визначення рівня ризиків для інформаційних ресурсів.

Класифікацію методів оцінювання ефективності систем захисту інформації, розділених на якісні та кількісні підходи [2] зображено на рис. 1.

Рис. 1. Класифікація методів оцінювання ефективності систем захисту інформації

Сучасні підходи до оцінки ефективності СЗІ поділяють на дві основні категорії: кількісні та якісні методи оцінювання. Якісні методи зазвичай застосовуються в умовах високої невизначеності та спираються на досвід і професійні знання експертів у сфері інформаційної безпеки. Більш точними є кількісні методи оцінювання ефективності систем захисту інформації, оскільки вони ґрунтуються на глибокому аналізі предметної області дослідження та дозволяють визначити конкретні значення параметрів функціонування системи.

До якісних методів оцінювання ефективності систем захисту інформації відносять офіційний підхід та методи експертних оцінок. Офіційний (нормативний) підхід до оцінювання ефективності систем захисту інформації базується на використанні стандартів і нормативних документів, які встановлюють вимоги до забезпечення інформаційної безпеки. У межах цього підходу оцінювання здійснюється шляхом перевірки відповідності інформаційної системи встановленим вимогам і критеріям захищеності.

До таких документів належать, зокрема, НД ТЗІ 2.5-004-99 [3], який визначає критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу та встановлює класи захищеності систем. Нормативний документ НД ТЗІ 3.7-003-2023 [4] регламентує порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційних системах та визначає вимоги до організації і виконання цих робіт.

Серед міжнародних стандартів важливе місце займає ISO/IEC 27001 [5], який встановлює вимоги до систем управління інформаційною безпекою, а також ISO/IEC 27002 [6], що містить рекомендації щодо реалізації заходів захисту інформації та управління ризиками інформаційної безпеки. Крім того, стандарт ISO/IEC 15408 [7] визначає міжнародні критерії оцінювання безпеки інформаційних технологій і використовується для оцінювання рівня довіри до програмних та апаратних засобів захисту.

Метод експертних оцінок ґрунтується на використанні досвіду, знань та професійних навичок спеціалістів у сфері інформаційної безпеки. У межах цього підходу оцінювання ефективності СЗІ здійснюється на основі аналізу думок експертів, які визначають рівень захищеності системи, можливі загрози, уразливості та ефективність застосованих засобів захисту [8].

Методи експертних оцінок можуть реалізовуватися у вигляді індивідуальних методів, до яких належать інтерв'ю та анкетування. Метод інтерв'ю передбачає безпосереднє спілкування аналітика з

експертом, під час якого фахівець надає відповіді на поставлені запитання та може детальніше пояснити свою думку щодо рівня захищеності системи або факторів, що впливають на ефективність СЗІ. Це дозволяє уточнювати окремі аспекти та отримувати більш розгорнуту інформацію. Метод анкетування полягає у письмовому опитуванні експертів за допомогою спеціально підготовленої анкети, що дає змогу отримати незалежні оцінки від кількох фахівців. Перевагою цього методу є можливість зібрати думки різних експертів, однак результати можуть залежати від правильності формулювання запитань анкети.

Іншою групою методів експертної оцінки є колективні методи, що спрямовані на формування узгодженої спільної думки шляхом взаємодії залучених фахівців. До таких методів відносять метод комісії, метод Делфі, конференцію ідей та метод відстороненого опитування. Вони дозволяють використовувати широкий спектр теоретичних і практичних знань та враховувати досвід фахівців, що підвищує точність і об'єктивність оцінки навіть за відсутності достатніх статистичних даних.

Метод комісії передбачає проведення спільного обговорення проблеми групою експертів, під час якого кожен учасник висловлює власну думку, після чого відбувається колективне обговорення та узгодження позицій. У результаті дискусії формується спільне рішення або оцінка, що приймається на основі консенсусу або голосування.

Метод Делфі ґрунтується на багатоетапному опитуванні групи експертів, яке проводиться анонімно. Експерти незалежно надають свої оцінки або прогнози, після чого результати узагальнюються та надсилаються їм для повторного перегляду. Процедура може повторюватися кілька разів, що дає змогу поступово зблизити позиції учасників і отримати більш обґрунтовану колективну оцінку [9].

Конференція ідей полягає у спільному обговоренні проблеми з метою генерування максимальної кількості можливих рішень або пропозицій. Учасники пропонують різні ідеї щодо покращення стану системи або підвищення ефективності її функціонування, після чого ці ідеї аналізуються та відбираються найбільш доцільні. Такий підхід сприяє появі нових нестандартних рішень.

Метод відстороненого опитування передбачає отримання експертних оцінок без безпосередньої взаємодії між експертами. Збір інформації здійснюється шляхом індивідуального письмового опитування або анкетування, що дозволяє уникнути взаємного впливу учасників та забезпечити незалежність їхніх суджень.

Кількісний підхід до оцінювання СЗІ передбачає застосування стохастичних методів та формальних моделей, що дозволяє об'єктивно визначати значення показників якості системи.

Стохастичні методи застосовуються для оцінювання ймовірності виникнення загроз, ризиків витоку інформації або порушення роботи системи. До стохастичних методів належать частотний, статистичний та ймовірнісний підходи.

Частотний метод ґрунтується на аналізі статистичних даних щодо частоти виникнення певних подій у минулому. На основі цих даних визначається ймовірність повторення подібних подій у майбутньому та оцінюється можливий збиток від реалізації відповідних загроз. Перевагою методу є можливість отримання обґрунтованих кількісних оцінок, однак його застосування потребує наявності значного обсягу достовірних статистичних даних.

Наступним є статистичний метод, який дозволяє оцінювати стан системи на основі обробки даних за визначений період часу. Такий підхід передбачає статистичний аналіз інформації про події, що відбулися, і використовується для визначення показників ефективності або частоти реалізації загроз.

Однією з груп стохастичних методів є ймовірнісні методи, які дозволяють оцінювати ймовірність відмови системи в результаті впливу різних факторів. Використання ймовірнісного підходу допомагає формалізувати ризики та передбачати потенційні загрози, що виникають у системі.

Формальні моделі використовуються для математичного опису процесів функціонування системи захисту інформації та аналізу її ефективності. Такі моделі дозволяють формалізувати взаємозв'язки між елементами системи та визначити оптимальні рішення щодо підвищення рівня захисту. До формальних моделей належать матричні, багаторівневі, оптимізаційні та багатокритеріальні моделі.

Матричні моделі застосовуються для представлення взаємозв'язків між загрозами, вразливостями та засобами захисту у вигляді таблиць або матриць. Багаторівневі моделі відображають структуру системи захисту на різних рівнях, що дозволяє аналізувати взаємодію між її компонентами. Оптимізаційні моделі спрямовані на пошук найкращих рішень щодо розподілу ресурсів або вибору заходів захисту. Багатокритеріальні моделі використовуються у випадках, коли необхідно врахувати кілька критеріїв оцінювання, наприклад ефективність, вартість та надійність засобів захисту.

Висновки

У роботі проведено аналіз сучасних методів оцінювання ефективності систем захисту інформації, які застосовуються для визначення рівня захищеності інформаційних ресурсів та надійності функціонування засобів безпеки в інформаційно-телекомунікаційних системах. Розглянуто основні підходи до оцінювання ефективності СЗІ, зокрема якісні та кількісні методи, що дозволяють оцінювати рівень інформаційної безпеки з урахуванням різних критеріїв та показників.

У процесі дослідження проаналізовано експертні методи оцінювання, офіційний підхід, стохастичні методи, а також формальні моделі, які використовуються для математичного опису процесів функціонування систем захисту інформації та визначення ефективності реалізованих механізмів безпеки. Встановлено, що кожен із підходів має власні переваги та обмеження, а їх застосування залежить від специфіки інформаційної системи, доступності статистичних даних, рівня формалізації процесів та необхідної точності оцінювання.

Проведений аналіз показав, що оцінювання ефективності систем захисту інформації є складним багатокритеріальним завданням, яке потребує комплексного підходу та врахування взаємодії різних компонентів системи безпеки.

Таким чином, подальші дослідження у цьому напрямі повинні бути спрямовані на вдосконалення методів оцінювання ефективності систем захисту інформації, розробку більш точних моделей аналізу та інтеграцію сучасних підходів управління інформаційною безпекою, що дозволить підвищити рівень захищеності інформаційних ресурсів у сучасних інформаційних системах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Комплексні системи захисту інформації : навчальний посібник. Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін. – Вінниця: ВНТУ, 2018. 118 с.
2. Наукоємні технології в інфокомунікаціях: обробка інформації, кібербезпека, інформаційна боротьба : монографія / за заг. ред. В. М. Безрука, В. В. Баранника. Харків : Видавництво «Лідер», 2017. 600 с.
3. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу : нормативний документ системи технічного захисту інформації. Київ, 1999. Затв. наказом ДСТСЗІ СБУ від 28.04.1999 № 22 (зі змінами від 28.12.2012 № 806).
4. НД ТЗІ 3.7-003-2023. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі : нормативний документ системи технічного захисту інформації. Київ, 2023. Затв. наказом Адміністрації Держспецзв'язку від 28.10.2023 № 924.
5. ISO/IEC 27001 certification standard. ISO 27001 information security standards. URL: https://www.iso27001security.com/html/27001 (last accessed: 09.03.2026).
6. ISO/IEC 27002 controls catalogue. ISO 27001 information security standards. URL: https://www.iso27001security.com/html/27002.html (last accessed: 09.03.2026).
7. ДСТУ ISO/IEC 15408-1:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 1. Вступ та загальна модель (ISO/IEC 15408-1:2022, IDT).
8. Методи експертних оцінок: теорія, методологія, напрямки використання : монографія / Б. Є. Грабовецький. – Вінниця: ВНТУ, 2010. 171 с.
9. M. Zosym. Метод Дельфі (Delphi method). 26.05.2023. URL: https://www.maxzosim.com/delphi-method/ (дата звернення: 09.03.2026).

Джумела Даяна Стефанівна – студентка групи 1БС-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: daianadzhumela@gmail.com

Науковий керівник: ***Дудатьєв Андрій Веніамінович*** – к.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: dudatyev.andrey@vntu.edu.ua

Daiana Dzhumela – student of group 1BS-22b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: daianadzhumela@gmail.com

Scientific supervisor: ***Andrii Dudatiev*** – PhD (Eng), Associated Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia, email: dudatyev.andrey@vntu.edu.ua