УДК 004.056.5:621.39

DOI: 10.31673/2412-9070.2022.032630

А. Г. ЗАХАРЖЕВСЬКИЙ, канд. техн. наук;
А. О. МАКАРЕНКО, доктор техн. наук,
Державний університет телекомунікацій, Київ

РОЗРОБЛЕННЯ АЛГОРИТМІВ ОЦІНЮВАННЯ СТАНУ ЗАХИСТУ ІНФОРМАЦІЇ ЗАСОБАМИ МЕРЕЖНИХ РЕСУРСІВ ІК-МЕРЕЖІ ЗВ'ЯЗКУ

Описано один із підходів до створення системи оцінювання стану захисту інформації (ОСЗІ), яка може бути використана як для оцінювання інформаційної безпеки (ІБ) типової інформаційної системи (ІС), так і для аналізу особливої системи підприємств телекомунікаційної та інших галузей. Розроблено алгоритми оцінювання стану захисту інформації засобами мережних ресурсів інфокомунікаційної мережі зв'язку. У процесі розроблення алгоритму для опису ймовірнісних характеристик істини гіпотези використовуватимемо поняття «коефіцієнта впевненості». З огляду на комплексне оцінювання ІБ інформаційної системи доходимо висновку, що створення ОСЗІ стає можливим, виправданим, доцільним та необхідним кроком. У цьому разі одним із найважливіших етапів є розроблення алгоритму взаємодії користувача та самої системи, яка в остаточному варіанті унаочнюватиме деяке програмне забезпечення. Взаємодіючи з програмним інтерфейсом, користувач працює з механізмом здобуття результатів аналітичного оцінювання, в якому вибираються категорії даних та база даних (БД). У процесі координування дій користувача та ОСЗІ для досягнення різноманітних, незалежних цілей та завдань різні зони взаємодії всередині ОСЗІ визначаються потребами та вимогами до реалізації цих зон. Існують два етапи визначення зон взаємодії між користувачами ІС та ОСЗІ. Алгоритм взаємодії користувача з ОСЗІ охоплює чотири етапи, протягом яких виробляються кілька запитів від системи та відповідей від користувача. Такий опис алгоритму взаємодії користувача та системи може бути фундаментом для розроблення логіки роботи ОСЗІ.

Ключові слова: система оцінювання стану захисту інформації; інформаційна безпека; інформаційна система; база даних; аналітик.

Вступ

Керівництву великих компаній потрібна точна інформація про стан системи інформаційної безпеки (ІБ) та оптимальні рішення щодо її вдосконалення. Від цього залежить якість керування, здатність компанії ефективно планувати свою діяльність та виживати в конкурентному середовищі. Тут важливими є чіткість подання інформації, швидкість створення нових видів звітів та можливість аналізувати поточні та логовані дані. Кваліфіковано підібраний алгоритм ухвалення рішень ОСЗІ-системи для оцінювання ІБ зможе надати керівникам підприємств такі можливості.

Аудит є одним із головних аспектів оцінювання інформаційної безпеки, оскільки дає змогу об'єктивно, якісно та кількісно оцінити її поточний стан в організації, ґрунтуючись на прийнятих критеріях безпеки. Проведення аудиту вимагає від аналітика глибокого знання законів, а також знайомства зі специфікою даних, що зберігаються і оброблюються в інформаційній системі (ІС) підприємства. Як засіб для полегшення та автоматизації діяльності аналітиків розробляється ОСЗІ-система.

Мета статті — описати один із підходів до створення ОСЗІ, яка може бути використана як для оцінювання ІБ типової інформаційної системи, так і аналізу особливої системи підприємств телекомунікаційної та інших галузей [1].

Основна частина

Систему ОСЗІ можна використовувати для оптимізації ризиків, пов'язаних із наявною концепцією аудиту. До того ж передбачається застосовувати ОСЗІ в сучасній промисловості та науці для мінімізації ризиків. Серед найважливіших особливостей цих систем – їх здатність до самонавчання через постійний аналіз нової інформації та побудову моделей поведінки на основі цього аналізу. Після виходу на ринок ОСЗІ гарантують інноваційний прорив завдяки інтеграції своїх доповнень до основного середовища і створення інтелектуальних модулів, які забезпечують високу ефективність та актуальність.

Слід зазначити, що більшість сучасних ОСЗІ мають дуже вузьку спрямованість і не завжди дають очікуваних результатів. Отже, під час обговорення предметної сфери ОСЗІ галузеві компоненти часто ігноруються і не дістають належного оцінювання, що пояснює актуальність і практичність представленої статті.

Ключовими елементами ОСЗІ є бази даних (БД), бази знань (БЗ) та апарат логічного висновку. Крім того, що ОСЗІ має дозволяти будувати моделі ІТ-структур, загроз і вразливостей, пов'язаних з окремими ІТ-компонентами, захистом конфіденційних даних, вона також має забезпечувати безпеку інформації, що зберігається. Це дасть змогу точно визначити найбільш критичні елементи ІС, а також ризик та збитки, спричинені порушенням їх ІБ.

У процесі побудови системи ОСЗІ найскладніше — це набуття необхідних знань. Інженер зі знань має вирішити, яким методом він буде послуговуватися і в який спосіб збирається взаємодіяти з аналітиком (інтуїтивний чи спостережний) [2].

Під час використання низки стратегій генерації знань (набуття, вилучення та формування) слід починати з вербального подання проблемної галузі. Основою для представлення є не лише глобальні цілі, а й завдання, адміністративні документи, навички спеціаліста та джерела спеціальної, вірогідної інформації [3]. У межах цієї статті БД ОСЗІ створюється на основі стандартів у галузі інформаційної безпеки та низки галузевих документів.

Крім того, під час заповнення БД ОСЗІ важливо зважати на ступінь компетентності аналітика. Інакше кажучи, коефіцієнт компетентності може проілюструвати вагу, яку надано аналітику, коли до статистичного процесу додаються його оцінки. За результатами попередніх експертиз, усі коефіцієнти можуть бути встановлені як числа в діапазоні (0, 1), а рівень аналітики розрахований за допомогою матриці парних порівнянь аналітичних компетенцій. За відсутності достатньої кількості статистичних даних можна визначити коефіцієнти, скориставшись інформацією про аналітика, який пройшов формальне оцінювання:

а) освіта;

б) наукова підготовка;

в) стаж роботи з пріоритетного спрямування;

г) кількість проведених експертиз.

Також оцінювання можна здійснити за допомогою шкали балів — 0, 2, 3, 4, 5. Підсумувавши кількість балів за пунктами а, б, в, г, визначимо первинний бал аналітика B_{aj} в аналітичній групі. Коефіцієнт авторитету з огляду на нормування обчислюється за такою формулою:

$$K_{aj} = \frac{B_{aj}}{\sum_{j=1}^{m} B_{aj}}, \qquad (1)$$

де m — кількість аналітиків у групі. Умова нормування:

$$\sum_{j=1}^{m} K_{aj} = 1. \qquad (2)$$

Отже, завдяки цим розрахункам можна вивести звіт комплексного оцінювання ІБ користувачеві у вигляді кількох варіантів розв'язання задачі щодо поліпшення наявної політики ІБ з відсотковою градацією ефективності застосування конкретного вирішення аналізованої проблеми.

Під час розроблення алгоритму (рис. 1) для опису ймовірнісних характеристик істини гіпотези використовуватимемо поняття «коефіцієнта впевненості» ($K_{вп}$). У разі, якщо $K_{вп} \to 1$, гіпотеза, висунута як своє рішення ОСЗІ, прагне до істини.

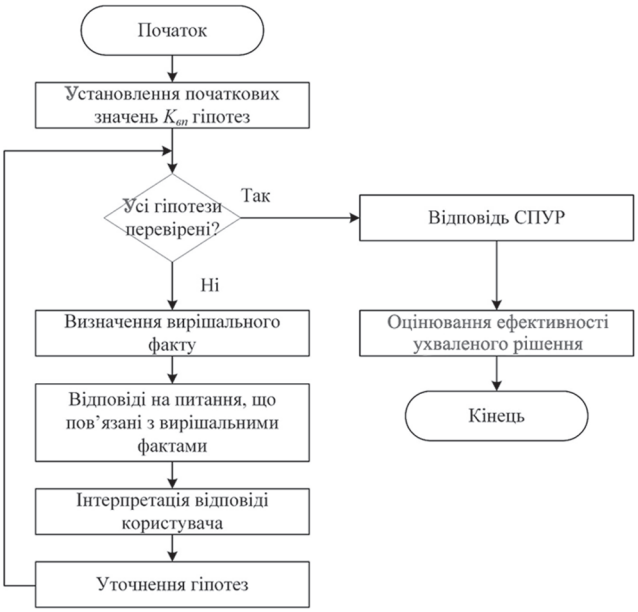

Рис. 1. Алгоритм ухвалення рішень на ОСЗІ

Аналітик за допомогою інформації, здобутої зі своєї практики, визначає для кожної гіпотези (з усієї множини) початкове значення коефіцієнта впевненості. Під час ініціалізації процедури ухвалення рішення ці показники надаватимуться значенням кожної гіпотези.

Наведемо алгоритм ухвалення рішень на основі дій, які здійснюватиме ОСЗІ для оцінювання ІБ (див. рис. 1).

1. Розрахунок коефіцієнтів упевненості для всіх гіпотез у певній безлічі, беручи до уваги припущення щодо потреби в прийнятті заходів безпеки.

2. Підтвердження чи спростування гіпотез із використанням фактів та доказів з БЗ.

3. Визначення вирішального факту зміни $K_{вп}$ кожної гіпотези.

4. Відповіді на питання, пов'язані з вирішальними фактами. Робота підсистеми взаємодії між ОСЗІ та користувачем.

5. Інтерпретація відповіді користувача.

6. Уточнення гіпотези.

7. Відповідь системи підтримки ухвалення рішень (СПУР).

8. Оцінювання ефективності ухваленого рішення.

Далі розглянемо дві моделі подання знань — на основі прецедентів і на основі знань. Розглянемо типову ситуацію (з огляду на прецеденти) для початкових етапів створення БЗ для ОСЗІ. Відсутність прикладів ухвалення рішень унеможливлює формулювання правил. Однак система вже має знання про попередні прецеденти (випадки, ситуації).

Прецеденти мають бути структуровані в базі в такий спосіб, щоб робота СПУР на їх основі була ефективною. Наприклад, захист ІС або її частин за

допомогою заходів безпеки може бути поділений на організаційні, програмні та апаратні заходи. Під час ухвалення рішень у такій моделі існує послідовність процедур:

- створення нового прецеденту (опис проблемної ситуації);
- пошук схожої ситуації в базі прецедентів;
- пошук нового рішення чи видозміна наявного (залежно від наявності випадку в базі);
- аналіз та оцінювання ефективності ухваленого рішення;
- навчання (наповнення) бази прецедентів.

Перший крок процесу —узагальнення поточної ситуації на основі інформації, наданої в БД про корпоративну мережу та всю ІС, а також про всі засоби ІБ. Отже, спочатку створюється приклад прецеденту. Зазвичай приклад прецеденту охоплює пояснення проблеми її вирішення, підсумкові показники. Зразок використання прецеденту описується такою формулою [5]:

$$P_k = \langle ID(P_k), C_i, X_{ki}, D_k, E_k \rangle, \quad (3)$$

де $ID(P_k)$ — ідентифікатор прецеденту; C_i — клас прецеденту; X_{ki} — безліч значень ознак, що становлять опис проблемної ситуації; D_k — безліч можливих рішень прецеденту; E_k — безліч оцінок ефективності ухвалених рішень.

Далі в основі прецедентів розпочинається процес пошуку використання аналогічної проблеми. Кожна ознака у виразі (3) перевіряється по черзі. Після завершення пошуку конкретне рішення модифікується для відповідності вихідному завданню або відшукується нове рішення з більш високою ймовірністю ефективності. У першому сценарії ефективність оцінюється за здобутим результатом, у другому — нове рішення користувача заноситься до БД (відбувається навчання системи).

Альтернативна модель, що базується на правилах, відома як продукційна модель. Правила — це сукупність знань із організованою логічною системою. Вони нагадують логічні міркування аналітика з ІБ, що має багаторічний досвід вирішення проблем. Для розв'язання подібних завдань правила в ОСЗІ можна поділити на кілька категорій:

- класифікація ІС, що висувають вимоги до ІБ;
- визначення складу ІС;
- виявлення загроз та вразливостей у ІС;
- оцінювання та аналіз ризиків;
- наповнення БЗ та ін.

У найпростішому вигляді правило описується виразом:

$$R = \langle U_1, U_2, \ldots, U_n; I \rangle, \quad (4)$$

де $U_1, \ldots, U_n$ — попередні умови спрацьовування правила (передумови); I — висновок. До того ж, що більше n, то краще система ухвалює рішення, але пошук рішення може забрати більше часу.

Правило спрацює, якщо буде виконано всі умови U_n, які можна пов'язати за допомогою І, АБО, НЕ. Загалом це правило застосовується, коли всі твердження є вірогідними. Якщо це не так, ним не слід послуговуватися. У цьому разі потрібно користуватися $K_{\text{вп}}$, тобто:

$$R = \langle U_1, K_{\text{вп}1}, U_2, K_{\text{вп}2}, \ldots, U_n, K_{\text{вп}1n}; I, K_{\text{вп}} \rangle. \quad (5)$$

Звернення до БЗ ОСЗІ відбувається на другому етапі під час встановлення вирішального факту. На заключному етапі ефективність ухваленого рішення оцінюється за допомогою аналізу ризиків. Оцінювання ризиків здійснюється для всіх можливих рішень. Процедура визначення ризику поділена на такі етапи:

- розрахунок вартості технічних ризиків;
- розрахунок потенційної шкоди.

Технічний ризик визначає розмір ризику ІБ, що охоплює ймовірність дій загроз та використання вразливостей кожного компонента інформаційної інфраструктури. При цьому береться до уваги рівень конфіденційності, цілісності та доступності цих компонентів. Для розв'язання проблеми можна скористатися такими формулами:

$$\begin{aligned} R_c &= K_c P(T) P(V); \\ R_i &= K_i P(T) P(V); \\ R_a &= K_a P(T) P(V), \end{aligned} \quad (6)$$

де R_c — ризик конфіденційності; K_c — коефіцієнт конфіденційності інформаційного активу; $P(T)$ — можливість реалізації небезпеки; $P(V)$ — імовірність використання вразливості; R_i — ризик цілісності; K_i — коефіцієнт цілісності інформаційного активу; R_a — ризик доступності; K_a — коефіцієнт доступності інформаційного активу.

Середнє значення ризику розраховується за таким виразом:

$$R_{\text{сер}} = \frac{(R_c + R_i + R_a)}{3}. \quad (7)$$

Розмір збитків L обчислюється для кожного активу:

$$L = R_{\text{сер}} S, \quad (8)$$

де S — втрати, що залежать від вартості ресурсів, ум. од. Аналітики встановлюють втрати для різних типів ресурсів, що захищаються в межах ІС.

Наявність БЗ, що містить правила вибору відповідних моделей та алгоритмів ухвалення рішень, допомагає обґрунтувати альтернативні варіанти залежно від того, як реалізовано компоненти вихідного завдання.

Комплексне оцінювання ІБ ІС зумовлює висновок, що створення ОСЗІ стає можливим, виправданим, доцільним та необхідним кроком. У цьому разі одним із найважливіших етапів є розроблення алгоритму взаємодії користувача та самої системи, яка в кінцевому варіанті представлятиме деяке програмне забезпечення.

Взаємодіючи з програмним інтерфейсом, користувач працює з механізмом здобуття результатів аналітичного оцінювання, в якому вибираються категорії даних та БЗ. У процесі координування дій користувача та ОСЗІ для досягнення різноманітних, незалежних цілей та завдань різні зони взаємодії всередині ОСЗІ визначаються потребами та вимогами до реалізації цих зон.

Існують такі етапи визначення зон взаємодії між користувачами ІС та ОСЗІ:

• у результаті діалогу між учасниками відносин (користувачем ІС та ОСЗІ) розподіляються їх дії, контролюються та відстежуються цілі не тільки користувачів ІС та ОСЗІ, а й розв'язуваного завдання;

• незалежні дані, запроваджені користувачем, аналізуються, тобто відбувається перетворення даних природною мовою.

Алгоритм взаємодії користувача (рис. 2) з ОСЗІ складається з чотирьох етапів, протягом яких виробляються кілька запитів від системи та відповідей від користувача.

1. Початкові запити ОСЗІ:

• визначити галузь діяльності підприємства (галузева БЗ) або вибрати універсальну БЗ, щоб оцінити ІБ;

• увести вихідні дані щодо промислової ІС підприємства: розміри, активи, відповіді на запити ОСЗІ відповідно до закладеної БЗ на основі запропонованих на стадії формування БЗ стандартів. Водночас уведення даних можливе в різній формі: числові, текстові, із вибором одного або кількох варіантів чи введення свого варіанта відповіді.

2. Оброблення системою введених користувачем даних та ухвалення рішення згідно з розробленим алгоритмом.

3. Після проведеного аналізу система видає користувачеві оцінку ефективності ухвалених рішень з огляду на галузеву складову (за потреби).

4. За запитом користувача підсумкові дані подаються як вихідний звіт, який містить результатні оцінки безпеки на основі застосування різноманітних математичних методів та рекомендацій щодо скорочення кількості вразливостей і зниження ризиків підприємства, а також ризики в промисловій системі.

Розглянутий опис алгоритму взаємодії користувача та системи може бути фундаментом для розроблення логіки роботи ОСЗІ. На певних етапах алгоритм звертається до БЗ ОСЗІ. Для того, щоб у звіті про результат проведеного оцінювання ІБ завжди містилися актуальні рекомендації стосовно зниження або усунення ризиків ІС підприємства, потрібно утримувати БЗ в актуальному стані, а для цього (крім внесення до неї основних стандартів) слід аналізувати та додавати/коригувати нові

Рис. 2. Алгоритм взаємодії користувача та системи, що розробляється

методи кібербезпеки в промислових системах та цифровому виробництві.

Висновки

Засобів гарантованого забезпечення ІБ, на жаль, немає. Цей процес неперервний і потребує особливої уваги. Компаніям, які дійсно цінують свою безпеку, потрібно передусім відшукати та усунути всілякі недоліки своєї ІС самостійно, щоб зловмисник не встиг цим скористатися.

У ІТ досить багато програмних продуктів, що дають змогу це здійснити. Також знайдеться багато інших інструментів, за допомогою яких можна і потрібно підтримувати ІБ інформаційно-телекомунікаційних систем.

Досліджена в статті структура ОСЗІ дозволить побудувати модель, яка стане початком програмної реалізації, а вивчені методи кібербезпеки дадуть можливість застосовувати їх у процесі розроблення функціонала ОСЗІ.

Наведені результати є основою, навколо якої надалі будуватиметься система, здатна зменшити витрати, пов'язані з аудитом ІБ, а також сприятиме збільшенню захищеності інформаційно-телекомунікаційних систем від зовнішнього несанкціонованого впливу.

Список використаної літератури

1. ***Atymtayeva L.*** *Development of expert system for information security audit [Електронний ресурс] // International Journal of Computer Research. URL: https://www.proquest.com/openview/f0e5a2b2d5ecc3250b158be2ffd91aa8/1?pq-origsite=gscholar&cbl=2034869*

2. ***Беркман Л.Н., Сторчак К. П., Захаржевський А. Г.*** *Підвищення показників якості системи керування сучасними та перспективними телекомунікаційними мережами // Зв'язок. 2020. №2. С. 3–7.*

3. ***Кожухівський А. Д., Ільїн О. Ю., Савченко В. А.*** *Прогнозування динаміки підозрілої активності в мережі на основі аналізу мережного трафіку // Зв'язок. 2021. №6. С. 26–30.*

4. ***Yevseiev S., Ponomarenko V., Laptiev O. [et al.]*** *Synergy of building cybersecurity systems / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov (Eds.). Kharkiv: PC mechnology center, 2021. P. 188.*

5. ***Lehner P., Zirk D.*** *Cognitive Factors in User/ Expert-System Interaction // Journal of the Human Factors and Ergonomics Society. 1987. 29. P. 97–109.*

A. Zakharzhevsky, A. Makarenko

DEVELOPMENT OF ALGORITHMS FOR ASSESSING THE STATE OF INFORMATION PROTECTION BY MEANS OF NETWORK RESOURCES OF IR COMMUNICATION NETWORKS

The article describes one of the approaches to the creation of a system assessment of the state of information protection (ASIP), which can be used both for the IS assessment of a typical information system and for the analysis of a special system of enterprises in the telecommunications and other industries. Algorithms for assessing the state of information protection by means of network resources of the information and communication network have been developed. When developing an algorithm to describe the probabilistic characteristics of the truth of the hypothesis, we will use the concept of "confidence coefficient". A comprehensive evaluation of IS of the information system leads to the conclusion that the creation of an ASIP becomes a possible, justified, expedient and necessary step. In this case, one of the most important stages is the development of the user interaction algorithm and the system itself, which will ultimately represent some software. Interacting with the software interface, the user works with the mechanism for obtaining the results of the analytical evaluation, in which the data categories and DB are selected. In the process of coordinating the actions of the user and the ASIP to achieve various, independent goals and tasks, different interaction zones within the ASIP are determined by the needs and requirements for the implementation of these zones. There are two stages of defining areas of interaction between IS users and ASIP. The user interaction algorithm with ASIP consists of four stages, during which several requests from the system and responses from the user are produced. This description of the algorithm of interaction between the user and the system can be the foundation for developing the logic of ASIP work. At certain stages, the algorithm turns to the DB ASIP. In order for the report on the result of the IS assessment to always contain relevant recommendations for reducing or eliminating IT risks, the enterprise must keep the DB in an up-to-date state, and for this (in addition to introducing basic standards into it), new cyber security methods should be analyzed and added/corrected in industrial systems and digital production.

Keywords: system assessment of the state of information protection; information security; information system; database; analyst.