NETWORK AND APPLICATION SECURITY

DOI 10.20535/2411-1031.2023.11.1.283535
УДК 004.056.53

ІГОР СУБАЧ,
ВОЛОДИМИР КУБРАК

ЛЕКСОГРАФІЧНИЙ МЕТОД РІШЕННЯ БАГАТОКРИТЕРІАЛЬНОЇ ЗАДАЧІ ВИБОРУ SIEM-СИСТЕМИ ДЛЯ ПОБУДОВИ СИТУАЦІЙНОГО ЦЕНТРУ З КІБЕРБЕЗПЕКИ

Розглянуто створення Ситуаційного центру з кібербезпеки, його завдання та склад, а також наведено основні технологічні інструменти, які повинні бути включені до ефективного Ситуаційного центру з кібербезпеки. Особлива увага приділена системі управління інцидентами інформаційної безпеки (SIEM), яка є ключовою для Ситуаційного центру з кібербезпеки, тому розглянуто її призначення та основні задачі, які вона повинна вирішувати. Проаналізовано особливості рішення задачі раціонального вибору SIEM-системи. Виділено групи показників, що характеризують ступінь виконання вимог, які пред'являються до SIEM-системи та наведено їх приклади. Запропоновано застосування теорії нечітких множин для обробки експертної інформації про якісні показники, що характеризують SIEM-систему. Проаналізовано особливості, що стосуються прийняття раціонального рішення щодо вибору SIEM-системи. Виділено групи показників, які можуть допомогти в оцінці ступеня відповідності SIEM-системи вимогам, та наведені приклади цих показників. З метою обробки експертної інформації про якісні показники SIEM-системи, було запропоновано використання теорії нечітких множин. Наведено формальну постановку задачі вибору SIEM-системи та запропоновано основні етапи її розв'язання, які включають підготовку початкових даних, вибір методу для рішення багатокритеріальної задачі раціонального вибору SIEM-системи та розробку алгоритму. Запропоновано використання методу нормування кількісних показників SIEM-системи та методу парних порівнянь на основі рангових оцінок для обробки її якісних показників. Розглянуто використання шкали Сааті з 9 бальними значеннями для отримання функцій належності якісних характеристик SIEM-системи на основі експертної оцінки. Розроблений алгоритм побудови функцій належності характеристик SIEM-системи до кожного нечіткого терму. Описано методи вирішення багатокритеріальних задач і запропоновано застосування лексографічного методу для рішення задачі раціонального вибору SIEM-системи в ході побудови Ситуаційного центру з кібербезпеки. Створений та втілений у життя алгоритм його реалізації, і щоб продемонструвати його ефективність, наведено приклад використання для раціонального вибору SIEM-системи. Крім того, надані рекомендації щодо практичного використання отриманих результатів.

Ключові слова: кібербезпека, кіберзахист, SIEM, ситуаційний центр, підтримка рішень, лексографічний метод, теорія нечітких множин.

Постановка проблеми. Протидія сучасним кіберзагрозам є неможливою без застосування сучасних технологій кіберзахисту, які дозволяють здійснювати контроль, збір, зіставлення та обробку інформації з метою виявлення існуючих та прогнозування майбутніх загроз. Важлива роль при цьому відводиться спеціальним підрозділам, які вирішують питання з інформаційної та кібербезпеки на організаційному та технічному рівні – ситуаційним центрам з кібербезпеки (СЦК).

СЦК вирішує наступні завдання [1]:

- здійснення безпосередніх заходів, щодо захисту від кібератак та мінімізації їх збитків;
- розпізнавання слабких місць у кіберзахисті системи та вжиття заходів щодо їхнього усунення;
- централізоване управління безпекою різних пристроїв у системі;
- постійний моніторинг поточного стану загроз системи;
- технічну підтримку з питань організації кіберзахисту системи та інші.

Структурно, СЦК включає три основні компоненти: персонал – кваліфіковані спеціалісти, які володіють сучасними технологіями кібербезпеки, мають компетентності з командної роботи та взаємодії з керівництвом організації; процеси – бізнес-процеси, технологічні процеси, операційні та аналітичні процеси; технології – інструменти виявлення, протидії та запобігання кіберзагрозам.

Ефективний СЦК повинен включати наступні сучасні технологічні інструменти забезпечення кібербезпеки [1], [2]: міжмережевий екран нового покоління (Next-Generation Firewall), систему запобігання вторгненням (IPS), засоби захисту Web-додатків (WAF) та баз даних (Database Protection), засоби захисту електронної пошти (Email-security), засоби виявлення загроз та протидії ним на прикінцевих точках (Endpoint Detection and Response), сканери вразливостей (Vulnerability Scanners), засоби запобігання втраті даних (Data Loss Prevention), засоби розслідування комп'ютерних інцидентів (Forensics), засоби контролю доступу до мережі (Network Access Control) та інші.

Проте основою побудови ефективного СЦК [1], [3], його ядром є застосування SIEM-системи (Security Information and Event Management) – системи управління інформацією та подіями безпеки. Застосування в контурі захисту SIEM-системи дозволяє здійснювати проактивне управління кіберінцидентами, тобто шляхом застосування автоматизованих механізмів, які використовують інформацію про події, що вже відбулися в системі, прогнозувати майбутні події, які будуть відбуватися в ній, а також адаптувати параметри захисту системи до її поточного стану, тим самим здійснюючи превентивні заходи ще до того, коли ситуація в системі стане критичною [3]. Відповідно до цього, SIEM-система повинна вирішувати комплекс задач, до яких можна віднести [3]:

- збір, обробку та аналіз подій безпеки, що поступають до неї з множини різнорідних розподілених джерел;
- виявлення в режимі реального часу або близького до нього кібератак та порушень політики безпеки;
- проведення розслідування кіберінцидентів;
- формування ефективних рішень щодо кіберзахисту системи;
- формування звітних документів і візуалізацію стану системи та інші.

Для вирішення даних задач, SIEM-система, на підставі зібраних з журналів (log-файлів) початкових даних, які накопичують інформацію про події, що відбуваються в системі, відбирає такі, що можуть бути ознаками кібератак або інших небажаних дій в системі.

Головною особливістю рішення задачі вибору SIEM-системи для побудови СЦК є велика кількість різнорідних показників, які характеризують ступінь виконання вимог, що пред'являються до систем даного типу та які можуть бути як кількісними, так й якісними. До якісних показників, насамперед, можна віднести такі, що характеризують наскільки ефективно можна застосовувати SIEM-систему для рішення функціональних задач, які покладаються на неї у складі СЦК, яка буде вартість придбання та застосування системи, наскільки вона надійна та легка в експлуатації та інші.

Аналіз останніх досліджень та публікацій показав, що дані показники можна представити наступним чином [4]-[16]:

$$X = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, \ldots\},$$

де x_1 – підтримка джерел подій;

x_2 – збір подій;

x_3 – кореляція;

x_4 – пошук та аналітика;

x_5 – візуалізація та звітність;

x_6 – пріоритезація та оповіщення;

x_7 – загальні налагодження та встановлений функціонал;

x_8 – масштабуємість, відмовостійкість, зберігання;

x_9 – моніторинг компонентів системи та внутрішній аудит;

x_{10} – зручність користування;

x_{11} – наявність державних сертифікатів відповідності;

x_{12} – додаткові модулі системи;

x_{13} – вартість;

…

Цілком очевидно, що вирішення задачі раціонального вибору SIEM-системи для побудови СЦК характерними є багатокритеріальність та необхідність врахування великої кількості якісних та кількісних показників.

У свою чергу, перша характеристика вимагає застосування ефективного методу рішення багатокритеріальних задач, а друга, для обробки експертної інформації про якісні показники – застосування теорії нечітких множин [17]-[20].

Метою роботи є розробка методу рішення багатокритеріальної задачі раціонального вибору SIEM-системи з врахуванням великої кількості якісних та кількісних показників для побудови ситуаційного центру з кібербезпеки.

Постановка задачі раціонального вибору SIEM-системи. Загальна постановка задачі раціонального вибору SIEM-системи може бути сформульованою наступним чином.

Необхідно знайти

$$S_0 = \arg \underset{s \in S}{opt} W\left(\overline{X}(s)\right), \tag{1}$$

де W – деякий узагальнений показник якості системи;

S – множина можливих варіантів вибору системи;

$\overline{X}(s) = |x_1(s), x_2(s), \ldots, x_k(s), x_{k+1}(s), \ldots, x_n(s)|$ – вектор показників якості SIEM, причому перші k ($i = \overline{1,k}$) вимог є кількісними, а інші n-k: $k = \overline{k+1,n}$ вимог – якісні.

Припущення: величина i-го часткового показника, який характеризує ступінь виконання i-ої вимоги до SIEM, визначається її наближенням до оптимального значення.

Основними етапами розв’язання задачі (1) є:

- підготовка початкових даних;
- вибір методу рішення багатокритеріальної задачі;
- розробка алгоритму (рис. 1).

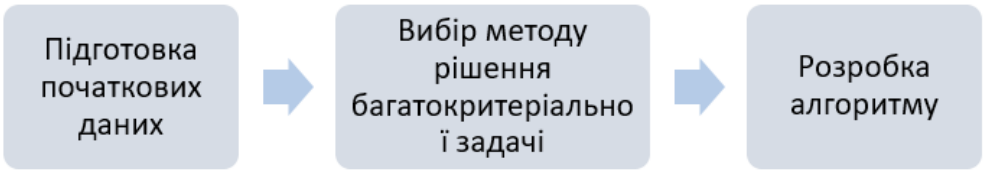

Рисунок 1 – Основні етапи рішення задачі раціонального вибору SIEM-системи

Нормування значення кількісного показника здійснюється наступним чином:

$$x_{ij} = \frac{x_{ij} - x_{ij}^{*}}{x_{ij}^{**} - x_{ij}^{*}}, \tag{2}$$

де x_{ij} – значення *i*-го показника для *j*-го варіанту системи;

x_{ij}^{*}, x_{ij}^{**} – найгірше та найкраще значення показника.

Відповідно, ступінь близькості *i*-го якісного показника до оптимального значення для *j*-го варіанту SIEM-системи можна визначити за допомогою функції належності $\mu_S(x_i)$. Для побудови функції належності $\mu_S(x_i)$ доцільно застосувати метод, що ґрунтується на рангових оцінках або метод парних порівнянь на основі рангових оцінок [19].

У даному випадку, під рангом елементу $x_i \in X$ розуміється число $r_s(x_i)$, яке характеризує його значимість у формуванні властивості SIEM-системи, яка описується нечітким термом *S*. Припустимо, що чим більшим є ранг показника, тим більшим є значення його функції належності.

Якщо ввести наступні позначення.

$$r_S(x_i) = r_i, \mu_S(x_i) = \mu_i; i = \overline{1,n},$$

то розподіл степенів належності можна представити у наступному виді.

$$\frac{\mu_1}{r_1} = \frac{\mu_2}{r_2} = \ldots \frac{\mu_n}{r_n}, \tag{3}$$

за умови нормування:

$$\mu_1 + \mu_2 + \ldots + \mu_n = 1. \tag{4}$$

На основі (3) визначаються степені належності всіх елементів множини через степені належності, так званого, опорного елементу.

Для опорного елементу $x_1 \in X$, який має функцію належності μ_1:

$$\mu_2 = \frac{r_2}{r_1} \cdot \mu_1;\ \mu_3 = \frac{r_3}{r_1} \cdot \mu_1;\ \ldots;\ \mu_n = \frac{r_n}{r_1} \cdot \mu_1; \tag{5}$$

Для опорного елементу $x_2 \in X$, який має функцію належності μ_2:

$$\mu_2 = \frac{r_1}{r_2} \cdot \mu_2;\ \mu_3 = \frac{r_3}{r_2} \cdot \mu_2;\ \ldots;\ \mu_n = \frac{r_n}{r_2} \cdot \mu_2; \tag{6}$$

Відповідно для опорного елементу $x_n \in X$, який має функцію належності μ_n:

$$\mu_n = \frac{r_1}{r_n} \cdot \mu_n;\ \mu_2 = \frac{r_2}{r_n} \cdot \mu_n;\ \ldots;\ \mu_{n-1} = \frac{r_{n-1}}{r_n} \cdot \mu_n; \tag{7}$$

З (5)-(7) та умови нормування (4) отримаємо:

$$\begin{cases} \mu_1 = \left(1 + \frac{r_2}{r_1} + \frac{r_3}{r_1} + \ldots + \frac{r_n}{r_1}\right)^{-1} \\ \mu_2 = \left(\frac{r_1}{r_2} + 1 + \frac{r_3}{r_2} + \ldots + \frac{r_n}{r_2}\right)^{-1} \\ \cdots \\ \mu_n = \left(\frac{r_1}{r_n} + \frac{r_2}{r_n} + \frac{r_3}{r_n} + \ldots + 1\right)^{-1} \end{cases} \quad (8)$$

На основі (8) можна обчислювати степені приналежності $\mu_s(x_i)$ за відносними оцінками рангів $\frac{r_i}{r_j} = \xi_{ij}, i, j = \overline{1,n},$ які створюють наступну матрицю:

$$\Xi = \begin{bmatrix} 1 & \frac{r_2}{r_1} & \frac{r_3}{r_1} & \ldots & \frac{r_n}{r_1} \\ \frac{r_1}{r_2} & 1 & \frac{r_3}{r_2} & \ldots & \frac{r_n}{r_2} \\ \ldots & \ldots & \ldots & \ldots & \vdots \\ \frac{r_1}{r_n} & \frac{r_2}{r_n} & \frac{r_3}{r_n} & \ldots & 1 \end{bmatrix} \quad (9)$$

Неважко побачити, що властивостями матриці (9) є наступні: вона є діагональною, транзитивною та елементи матриці, які є симетричними відносно головної діагоналі, зв'язані залежністю: $\xi_{ij} = 1/\xi_{ji}$.

Оскільки матриця (9) є матрицею парних порівнянь рангів елементів, то для експертних оцінок її елементів можна застосовувати 9-ти бальну шкалу Сааті [21]: $\xi_{ij} = r_i / r_j$ (таблиця 1).

Таблиця 1 - Шкала відносної важливості

Інтенсивність відносної важливості	Означення
1	Рівна важливість вимог, які порівнюються
3	Слабка перевага одного над іншим
5	Сильна перевага
7	Очевидна перевага
9	Абсолютна перевага
2,4,6,8	Проміжні рішення між двома сусідніми оцінками

Таким чином, за допомогою (8) експертні дані [22] про ранги елементів (їхні попарні порівняння) перетворюються у функцію належності нечіткого терму.

Алгоритм побудови функції належності включає наступні кроки.

1. Задати лінгвістичну змінну (якісну характеристику SIEM-системи).
2. Визначити універсальну множину на якій задається лінгвістична змінна (значення якісної характеристики SIEM-системи).
3. Задати сукупність нечітких термів $\{S_1, S_2, \ldots, S_n\}$, які використовуються для оцінки заданої на першому кроці змінної.
4. Для кожного нечіткого терму S_j, $j = \overline{1,m},$ сформувати матрицю (9).

5. На основі формул (8) обчислити функції належності елементів (характеристик SIEM-системи) до кожного нечіткого терму.

6. Процедуру нормування отриманих функцій належності здійснювати шляхом їхнього ділення на найбільше значення функції належності.

Аналіз показує [23]-[25], що найбільш розповсюдженими методами для рішення багатокритеріальної задачі (1) є наступні: метод головного показника, методи узагальненого адитивного / мультиплікативного показника, методи узагальненого мінімаксного показника та лексографічні методи. Слід зауважити, що всі наведені методи мають достоїнства та недоліки, а вибір методу значною мірою визначається повнотою та достовірністю експертних знань про важливість та ступінь взаємозв'язку часткових показників якості.

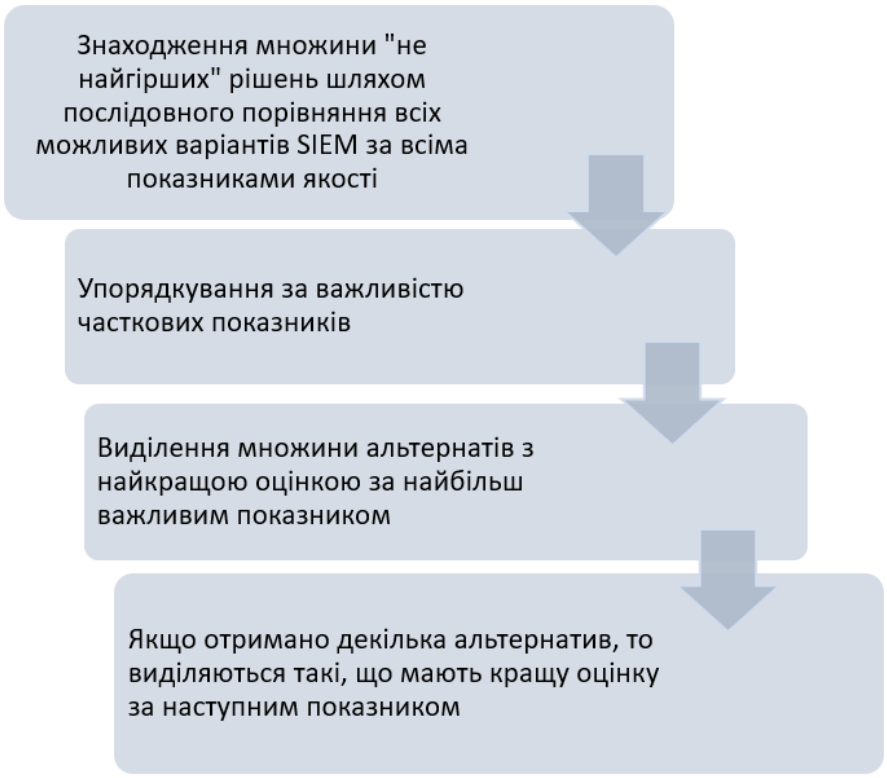

Рисунок 2 – Послідовність етапів рішення задачі раціонального вибору SIEM-системи лексографічним методом

Оскільки саме лексографічні методи є найменш вимогливими до експертної інформації про ступінь переваги часткових показників, то для рішення задачі раціонального вибору SIEM-системи для побудови СЦК, цілком доцільно обрати саме лексографічний метод, суть застосування якого полягає у наступному (рис. 2)

На попередньому етапі рішення задачі, шляхом послідовного порівняння всіх можливих варіантів SIEM-системи за всіма показниками якості, знаходиться множина "не найгірших рішень" (парето-оптимальних рішень) [22]-[25].

Далі, усі часткові показники упорядковуються за важливістю. Потім виділяється множини альтернатив з найкращою оцінкою за найбільш важливим показником. У випадку, коли така альтернатива єдина, то вона вважається найкращою. В іншому випадку, коли отримано декілька альтернатив, то з них виділяються такі, що мають кращу оцінку за іншим показником і так далі.

Таким чином, алгоритм реалізації лексографічного методу рішення задачі раціонального вибору системи складається з наступних кроків.

1. Упорядковуються часткові показники якості за важливістю:

$$x_1(s) > x_2(s) > \ldots > x_n(s).$$

2. Для кожного показника визначається величина припустимої поступки $\Delta x_i, i = \overline{1,n},$ у межах якої варіанти SIEM-системи, які порівнюються, вважаються рівноцінними.

3. Для першого показника $x_1(s)$ формується множина Ψ_1 рівноцінних варіантів SIEM-системи, які задовольняють наступній умові:

$$\max\left(x_{1j} - x_{1k}\right) \le \Delta x_1,\ j = \overline{1,m};\ k = \overline{1,m};\ k \ne j. \tag{10}$$

4. Якщо множина Ψ_1 містить тільки один варіант, то він вважається найкращим. В іншому випадку – коли вона містить більш ніж одну альтернативу, то необхідно перейти до розгляду усіх варіантів множини Ψ_1 за показником $x_2(s)$.

5. Для другого показника $x_2(s)$, з множини варіантів Ψ_1, формується множина варіантів Ψ_2, які задовольняють умові:

$$\max\left(x_{2j} - x_{2k}\right) \le \Delta x_2, i \in \Psi_1;\ k \in \Psi_1;\ k \ne j. \tag{11}$$

6. Якщо множина Ψ_2 містить один варіант, то він вважається найкращим. В іншому випадку – знайдені варіанти розглядаються за показником $x_3(s)$ і так далі.

7. У випадку, коли послідовно переглянуто всі показники та отримано множину $\Psi = \Psi_1 \times \Psi_2 \times \ldots \times \Psi_n,$ що містить більш ніж одну альтернативу, можливі два варіанти: зменшити величину припустимої поступки $\Delta x_i, i = \overline{1,n},$ починаючи з першого за важливістю показника та повторити алгоритм з початку або надати можливість особі що приймає рішення (ОПР) щодо вибору найкращого варіанту.

Для ілюстрації роботи запропонованого алгоритму, наведемо приклад щодо застосування його до вибору раціонального варіанту SIEM-системи [26].

Для вибору SIEM-системи використаємо чотири часткових показники: $x_1(s)$ – вартість та $x_2(s)$ – підтримка джерел подій, які є кількісними, а також $\mu_{x_3}(s)$ – масштабуємість та $\mu_{x_4}(s)$ – зручність користування, що є якісними показниками.

Для розгляду обрано 5 варіантів вибору SIEM-системи $s_j,\ j = \overline{1,5}.$

У результаті проведених розрахунків та отриманих експертних оцінок було отримано наступні дані, які характеризують ступінь відповідності SIEM-системи заданим вимогам:

$$x_1 = \left\{\frac{0,8}{s_1}; \frac{0,8}{s_2}; \frac{0,7}{s_3}; \frac{0,5}{s_4}; \frac{0,6}{s_5}\right\};$$

$$x_2 = \left\{\frac{0,7}{s_1}; \frac{0,8}{s_2}; \frac{0,6}{s_3}; \frac{0,7}{s_4}; \frac{0,8}{s_5}\right\};$$

$$x_3 = \left\{\frac{0,4}{s_1}; \frac{0,6}{s_2}; \frac{0,7}{s_3}; \frac{0,8}{s_4}; \frac{0,7}{s_5}\right\};$$

$$x_4 = \left\{\frac{0,5}{s_1}; \frac{0,6}{s_2}; \frac{0,5}{s_3}; \frac{0,6}{s_4}; \frac{0,3}{s_5}\right\}.$$

1. Показники за важливістю упорядковані наступним чином:

$$x_1 > x_2 > \mu_S(x_3) > \mu_s(x_4).$$

2. Величина припустимої поступки $\Delta x_i = 0{,}1,\ i = \overline{1{,}4}.$

3. При максимальному значенні першого показника $x_1 = 0{,}8$ та величиною припустимої поступки $\Delta x_1 = 0{,}1$ до множини Ψ_1 рівноцінних варіантів SIEM-системи, які задовольняють умові (2) включено наступні варіанти:

$$\Psi_1 = \{S_1, S_2, S_3\}.$$

4. З множини Ψ_1, за другим показником x_2 при виконанні умови (3): $x_2 = 0{,}8$ та $\Delta x_2 = 0{,}1$ до множини Ψ_2 включено варіанти:

$$\Psi_2 = \{S_1, S_2\}.$$

5. З множини варіантів: $\Psi = \Psi_1 \times \Psi_2$ за третім показником x_3 при виконанні умов (3) $x_3 = 0{,}6$ та $\Delta x_3 = 0{,}1$ до множини Ψ_3 включено варіанти:

$$\Psi_3 = \{S_2\}.$$

Раціональним вибором SIEM для побудови СЦК є другий варіант.

Висновки. У результаті проведених досліджень показано, що ефективним методом для рішення багатокритеріальної задачі раціонального вибору SIEM-системи для СЦК є лексографічний метод. Сформульовано групи кількісних та якісних показників, які характеризують вимоги до SIEM у складі СЦК. Запропоновано математичний апарат для обробки кількісних та якісних показників SIEM-системи. Обґрунтовано доцільність застосування процедури нормування кількісних показників SIEM-системи та застосування методу попарних порівнянь на основі рангових оцінок для обробки її якісних показників. Сформульовано формальну постановку задачі раціонального вибору SIEM-системи для її функціонування у складі СЦК та виділено основні етапи її вирішення. Розроблено алгоритм реалізації лексографічного методу та доведеного його до практичної реалізації у вигляді алгоритму.

Отримані результати можуть бути використанні на практиці під час вирішення задач створення СЦК та раціонального вибору його програмного забезпечення, зокрема, SIEM-системи.

Перспективними напрямами подальших наукових досліджень є розробка моделей та методів виявлення кіберінцидентів SIEM-системою в інформаційно-комунікаційній системі з урахуванням неповноти та неточності інформації про них.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] I. Subach, D. Mogylevich, A. Mykytiuk, V. Kubrak, and S. Korotaev, “Design methodology of cybersecurity situational center”, *CEUR Workshop Proceedings*, vol. 2859, pp. 210-219, 2021, [Online]. Available: http://ceur-ws.org/Vol-3187/paper8.pdf. Accessed on: Apr. 04, 2023.

[2] Was ist ein Security Operations Center (SOC)?, 2017. [Online]. Available: https://www.security-insider.de/was-ist-ein-security-operations-center-soc-a-617980/, Accessed on: Apr. 05, 2023.

[3] І. Субач, В. Кубрак, та А. Микитюк, “Архітектура та функціональна модель перспективної проактивної інтелектуальної системи SIEM-системи для кберзахисту об’єктів критичної інфраструктури”, *Information Technology and Security,* vol 7., iss. 2., pp. 208-215, 2019, doi: https://doi.org/10.20535/2411-1031.2019.7.2.190570.

[4] Methodology for a Sectoral Cybersecurity Assessment, 2021. [Online]. Available: https://www.enisa.europa.eu/publications/methodology-for-a-sectoralcybersecurity-assessment. Accessed on: Mar. 11, 2023.

[5] What is security incident and event management (SIEM)?, 2020. [Online]. Available: https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem. Accessed on: Feb. 17, 2023.

[6] P. Kirvan, How to select a security analytics platform, plus vendor options, 2023. [Online]. Available: https://www.techtarget.com/searchsecurity/tip/How-to-select-a-security-analytics-platform-plus-vendor-options. Accessed on: Jan. 12, 2023.

[7] Gartner Magic Quadrant, [Online]. Available: https://www.gartner.com/en/research/methodologies/magic-quadrants-research. Accessed on: Apr. 04, 2023.

[8] B. Canner, Comparing the Top SIEM Vendors, 2018. [Online]. Available: https://solutionsreview.com/security-information-event-management/comparing-the-top-siem-vendors-solutions-review. Accessed on: Apr. 04, 2023.

[9] B. J. Oltsik, SOAPA: Unifying SIEM and SOAR with IBM security QRadar and IBM security resilient, 2020. [Online]. Available: https://www.ibm.com/security/digital-assets/resilient/unifying-siem-and-soar-with-soapa. Accessed on: May 04, 2023.

[10] M. Vielberth, and G. Pernul, "A Security Information and Event Management Pattern", *in Proc. 12th Latin American conference on pattern languages of programs (SugarLoafPLoP 2018)*, Brazil, 2018, p. 27.

[11] K. Agrawal, and H. Makwana, "A Study on Critical Capabilities for Security Information and Event Management", *International journal of science and research (IJSR)*, vol. 4, iss. 7, pp. 1893-1896, 2015.

[12] H. Karlzén, "An analysis of security information and event management systems", 2009. [Online]. Available: http://publications.lib.chalmers.se/records/fulltext/89572.pdf. Accessed on: Jan. 23, 2023.

[13] SIEM product comparison, 2019. [Online]. Available: https://comminity.softwaregrp.com/dcvta86296. Accessed on: May 20, 2023.

[14] SIEM competitive comparision, 2019 [Online]. Available: https://www.securonix.com/products/competitive-comparison. Accessed on: Apr. 04, 2023.

[15] Б. Герасимов, та І. Субач, "Показники якості інформаційного забезпечення та їх вплив на ефективність застосування ІСППР", *Вісник КНУ ім. Т. Г. Шевченка*, вип. 20, с. 27-29, 2008.

[16] І. Субач, В. Рябцев, та А. Голуб, "Модель показників ефективності системи інформаційно-аналітичного забезпечення прийняття рішення", *Праці Військового інституту телекомунікації та інформатизації*, вип. 1, с. 27-37, 2005.

[17] І. Субач, та В. Фесьоха, "Модель виявлення аномалій в інформаційно-телекомунікаційних мережах органів військового управління на основі нечітких множин та нечіткого логічного виводу", *Збірник наукових праць ВІТІ*, № 3. с. 158-164, 2017.

[18] V. Fesokha, I. Subach, V. Kubrak, A. Mykytiuk, and S. Korotaiev, "Zero-day polymorphic cyberattacks detection using fuzzy inference system", *Austrian journal of technical and natural sciences: scientific journal*, no. 5-6. pp. 8-13, 2020, doi: https://doi.org/10.29013/AJT-20-5.6-8-13.

[19] A. P. Rotshtein, *Intellectual Technologies of Identification: Fuzzy Logic, Genetic Algorithms Neuron Networks.* Vinnitsa, Ukraine: UNIVERSUM, 1999.

[20] A. Piegat, *Fuzzy modeling and control*, Heidelberg, Germany: Springer, 2001.

[21] Н. Д. Панкратова, та Н. І. Недашківська, *Метод і моделі аналізу ієрархій. Теорія. Застосування: навч. посіб.*, Київ, Україна: НТУУ "КПІ", 2010.

[22] Г. М. Гнатієнко, та В. Є. Снитюк, *Експертні технології прийняття рішень*, Київ, Україна: Маклаут, 2008.

[23] R. E. Steuer, *Multiple criteria optimization: theory, computations, and application*, New York, USA: John Wiley & Sons Inc., 1986.

[24] Y. Sawaragi, *Theory of multiobjective optimization. mathematics in science and engineering*, vol. 176, Orlando, USA: Academic Press Inc., 1985.

[25] J. Branke, D. Kalyanmoy, K. Miettinen, and R. Slowinski, "*Multiobjective optimization: interactive and evolutionary approaches",* in *Lecture notes in computer science*, Berlin, Heidelberg, Germany: Springer, 2008, pp. 27-57.

[26] I. Subach, V. Kubrak, and A. Mykytiuk, "Methodology of rational choice of security incident management system for building operational security center", *CEUR Workshop Proceedings*, vol. 2577, pp. 11-20, 2019, [Online]. Available: http://ceur-ws.org/Vol-2577/paper2.pdf. Accessed on: Feb. 21, 2023.

Стаття надійшла до редакції 20.05.2023.

REFERENCES

[1] I. Subach, D. Mogylevich, A. Mykytiuk, V. Kubrak, and S. Korotaev, "Design methodology of cybersecurity situational center", *CEUR Workshop Proceedings*, vol. 2859, pp. 210-219, 2021, [Online]. Available: http://ceur-ws.org/Vol-3187/paper8.pdf. Accessed on: Apr. 04, 2023.

[2] Was ist ein Security Operations Center (SOC)?, 2017. [Online]. Available: https://www.security-insider.de/was-ist-ein-security-operations-center-soc-a-617980/, Accessed on: Apr. 05, 2023.

[3] I. Subach, A. Mykytiuk, and V. Kubrak, "Architecture and functional model of a perspective proactive intellectual SIEM for cyber protection of objects of critical infrastructure", *Information Technology and Security*, vol. 7., iIss. 2., pp. 208–215, 2019, doi: https://doi.org/10.20535/2411-1031.2019.7.2.190570.

[4] Methodology for a Sectoral Cybersecurity Assessment, 2021. [Online]. Available: https://www.enisa.europa.eu/publications/methodology-for-a-sectoralcybersecurity-assessment. Accessed on: Mar. 11, 2023.

[5] What is security incident and event management (SIEM)?, 2020. [Online]. Available: https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem. Accessed on: Feb. 17, 2023.

[6] P. Kirvan, How to select a security analytics platform, plus vendor options, 2023. [Online]. Available: https://www.techtarget.com/searchsecurity/tip/How-to-select-a-security-analytics-platform-plus-vendor-options. Accessed on: Jan. 12, 2023.

[7] Gartner Magic Quadrant, [Online]. Available: https://www.gartner.com/en/research/methodologies/magic-quadrants-research. Accessed on: Apr 04, 2023.

[8] B. Canner, Comparing the Top SIEM Vendors, 2018. [Online]. Available: https://solutionsreview.com/security-information-event-management/comparing-the-top-siem-vendors-solutions-review. Accessed on: Apr. 04, 2023.

[9] B. J. Oltsik, SOAPA: Unifying SIEM and SOAR with IBM security QRadar and IBM security resilient, 2020. [Online]. Available: https://www.ibm.com/security/digital-assets/resilient/unifying-siem-and-soar-with-soapa. Accessed on: May 04, 2023.

[10] M. Vielberth, and G. Pernul, "A Security Information and Event Management Pattern", *in Proc. 12th Latin American conference on pattern languages of programs (SugarLoafPLoP 2018)*, Brazil, 2018, p. 27.

[11] K. Agrawal, and H. Makwana, "A Study on Critical Capabilities for Security Information and Event Management", *International journal of science and research (IJSR)*, vol. 4, iss. 7, pp. 1893-1896, 2015.

[12] H. Karlzén, "An analysis of security information and event management systems", 2009. [Online]. Available: http://publications.lib.chalmers.se/records/fulltext/89572.pdf. Accessed on: Jan. 23, 2023.

[13] SIEM product comparison, 2019. [Online]. Available: https://comminity.softwaregrp.com/dcvta86296. Accessed on: May 20, 2023.

[14] SIEM competitive comparision, 2019 [Online]. Available: https://www.securonix.com/products/competitive-comparison. Accessed on: Apr. 04, 2023.

[15] B. Gerasimov, and I. Subach, "Quality indicators of information support and it impact on the effectiveness of decision support systems", *Bulletin of Taras Shevchenko Kyiv National university of Ukraine*, no. 20, pp. 27-29**,** 2008.

[16] I. Subach, V. Riabtsev, and A. Golub, "Effectiveness indicators model of the informational and analytical support system of the decision making", *Proceedings of the military institute of telecommunications and informatization*, vol. 1, pp. 27-37, 2005.

[17] I. Subach, and V. Fesokha, "Anomalies detection model at the information and telecommunication networks of command and control stuffs based on fuzzy sets and fuzzy logic output", *Collection of scientific works of MITI*, no. 3. pp.158-164, 2017.

[18] V. Fesokha, I. Subach, V. Kubrak, A. Mykytiuk, and S. Korotaiev, "Zero-day polymorphic cyberattacks detection using fuzzy inference system", *Austrian journal of technical and natural sciences: scientific journal*, no. 5-6. pp. 8-13, 2020, doi: https://doi.org/10.29013/AJT-20-5.6-8-13.

[19] A. P. Rotshtein, *Intellectual Technologies of Identification: Fuzzy Logic, Genetic Algorithms Neuron Networks.* Vinnitsa, Ukraine: UNIVERSUM, 1999.

[20] A. Piegat, *Fuzzy modeling and control*, Heidelberg, Germany: Springer, 2001.

[21] N. D. Pankratova, and N. I. Nedashkivska, *Method and models of hierarchy analysis. Theory. Application: textbook,* Kyiv, Ukraine: NTUU "KPI", 2010.

[22] H. M. Hnatiienko, and V. Ye. Snytiuk, *Decision making expert technologies,* Kyiv, Ukraune: McLaut, 2008.

[23] R. E. Steuer, *Multiple criteria optimization: theory, computations, and application*, New York, USA: John Wiley & Sons Inc., 1986.

[24] Y. Sawaragi, *Theory of multiobjective optimization. mathematics in science and engineering*, vol. 176, Orlando, USA: Academic Press Inc., 1985.

[25] J. Branke, D. Kalyanmoy, K. Miettinen, and R. Slowinski, "*Multiobjective optimization: interactive and evolutionary approaches",* in *Lecture notes in computer science*, Berlin, Heidelberg, Germany: Springer, 2008, pp. 27-57.

[26] I. Subach, V. Kubrak, and A. Mykytiuk, "Methodology of rational choice of security incident management system for building operational security center", *CEUR Workshop Proceedings*, vol. 2577, pp. 11-20, 2019, [Online]. Available: http://ceur-ws.org/Vol-2577/paper2.pdf. Accessed on: Feb. 21, 2023.

IHOR SUBACH,
VOLODYMYR KUBRAK

LEXICAL METHOD FOR SOLVING A MULTICRITERIA PROBLEM OF SELECTING A SIEM FOR BUILDING A SITUATIONAL CENTER FOR CYBERSECURITY

The author considers the creation of a Cybersecurity Situation Center (CSC), its tasks and composition, and also provides the main technological tools that should be included in an effective CSC. Particular attention is paid to the information security incident management system (SIEM), which is key to the CSC, and its purpose and main tasks that it should solve are considered. The authors analyzes the peculiarities of solving the problem of rational selection of a SIEM. The groups of indicators characterizing the degree of fulfillment of the requirements for a SIEM are allocated and their examples are given. The use of fuzzy set theory for processing expert information on qualitative indicators characterizing a SIEM is proposed. The features related to making a rational decision on the choice of a SIEM are analyzed. Groups of indicators that can help in assessing the degree of compliance of a SIEM with the requirements are allocated, and examples of these indicators are given. In order to process expert information on the qualitative indicators of a SIEM, the use of fuzzy set theory is proposed. A formal statement of the problem of selecting a SIEM is presented and the main stages of its solution are proposed, including the preparation of initial data, the choice of a method for solving the multi-criteria problem of rational selection of a SIEM and the development of an algorithm. It is proposed to use the method of normalization of quantitative indicators of a SIEM and the method of pairwise comparisons based on rank estimates to process its qualitative indicators. The use of the Saaty scale with 9 point values to obtain membership functions for the qualitative characteristics of a SIEM based on expert evaluation is considered. An algorithm for constructing membership functions of SIEM characteristics for each fuzzy term is developed. Methods for solving multi-criteria problems are described and the use of the lexical method is proposed to solve the problem of rational selection of a SIEM in the course of building a Cybersecurity Situation Center. An algorithm for its implementation has been created and implemented, and to demonstrate its effectiveness, an example of its use for the rational selection of a SIEM is given. In addition, recommendations for the practical use of the obtained results are given.

Key words: cybersecurity, cyber defense, SIEM, situation center, decision support, lexical method, fuzzy set theory.

Субач Ігор Юрійович, доктор технічних наук, доцент, завідувач кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-9344-713X, igor_subach@ukr.net.

Кубрак Володимир Олександрович, аспірант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0001-8877-5289, volodymir.kubrak@ukr.net.

Subach Ihor, doctor of technical science, associate professor, head at the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Kubrak Volodymyr, postgraduate student, Institute of special communications and information protection National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.