УДК 004.056(53+57) д.т.н., проф. **Субач І.Ю.** (ІСЗЗІ КПІ ім. Ігоря Сікорського)
Власенко О.В. (ВІТІ ім. Героїв Крут)

DOI: http://doi.org/10.17721/2519-481X/2024/83-10

МЕТОДИКА ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ SIEM-СИСТЕМОЮ В БАЗАХ ДАНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

В умовах інтеграції інформаційно-комунікаційних систем у процеси військової діяльності, питання їх кіберзахисту стає все більш актуальнішим. Основною ціллю для кібератак є бази даних, що переважно містять конфіденційну інформацію. Одним із найефективніших підходів до забезпечення кіберзахисту баз даних інформаційно-комунікаційних систем військового призначення є використання інтелектуальних можливостей SIEM-системи. SIEM дозволяє в режимі реального часу здійснювати моніторинг, аналіз та реагування на потенційні кіберінциденти. У статті запропоновано методику виявлення кіберінцидентів SIEM-системою у базах даних інформаційно-комунікаційних систем військового призначення. Основний акцент зроблено на багаторівневому захисті баз даних, який включає захист на рівні операційної системи, рівні бази даних та системи керування базами даних, а також мережевому рівні захисту. З метою підвищення ефективності виявлення кіберінцидентів на рівні аналізу даних SIEM-системи застосовується удосконалена методика на основі апарату нечіткої логіки. Удосконалення методики досягається шляхом введення ваг антецедентів у нечітких правилах, що дозволяє, у деяких випадках, точніше ідентифікувати кіберінциденти у порівнянні з існуючими моделями та методами. Безпосередньо ваги антецедентів нечітких правил визначаються за допомогою методу парних порівнянь на основі рангових оцінок, здійснених за 9-бальною шкалою Сааті. Представлено алгоритм прийняття рішень щодо ідентифікації кіберінцидентів, який базується на аналізі нечітких правил та ваг їх антецедентів. Наведено приклад розрахунку ваг антецедентів нечітких правил використовуючи метод парних порівнянь на основі рангових оцінок.

Ключові слова: база даних, інформаційно-комунікаційна система, кіберзахист, кіберінцидент, кібербезпека, кібератака, SIEM-система, теорія нечітких множин, нечіткі правила, метод парних порівнянь.

Вступ. У сучасному цифровому світі інформаційно-комунікаційні системи військового призначення (ІКСВП) знаходяться під постійним загрозливим тиском від кібератак, які можуть призвести до порушення безпеки проведення військових операцій, розголошення конфіденційної інформації та завдання збитків військовій інфраструктурі [1-4]. Кіберпростір став не лише ареною для інформаційної війни, але й стратегічним полем битви, де навіть одна успішна кібератака може мати серйозні наслідки. Від протидії кібератакам залежить ефективність виконання військових операцій, захист конфіденційної інформації, а також безпека особового складу та працездатність обладнання інформаційно-комунікаційної системи. Тому розвиток та застосування ефективних засобів виявлення та реагування на кіберінциденти стає невідкладною необхідністю для будь-якої країни чи військової організації.

Одним з основних структурних елементів будь-якої ІКСВП є база даних (БД), яка виконує важливі функції зберігання, організації та доступу до інформації, необхідної для функціонування системи [5]. У ІКСВП БД можуть містити різноманітну інформацію, включаючи дані про військову діяльність, плани, обладнання, персонал, розташування військових об'єктів та інші дані, необхідні для прийняття оперативних рішень та забезпечення безпеки [6]. Оскільки БД зберігає великий обсяг критичних даних, забезпечення безпеки їх стає надзвичайно пріоритетною задачею.

Найбільш ефективним рішенням в контексті кіберзахисту БД ІКСВП є використання системи управління інформацією та подіями безпеки (SIEM-системи) [7, 8]. SIEM-система забезпечує комплексний підхід до кіберзахисту, поєднуючи в собі моніторинг, аналіз та

реагування на потенційні кіберзагрози в реальному часі. Її засоби дозволяють виявляти аномальність у поведінці користувачів та систем, а також аналізувати великі обсяги даних для виявлення підозрілих подій.

У БД ІКСВП, де конфіденційність та цілісність даних є критичними, SIEM-системи виявляються особливо корисними. Вони дозволяють відслідковувати доступ до конфіденційної інформації, виявляти спроби несанкціонованого доступу та інші, а також забезпечувати швидке реагування на кіберінциденти.

Однак, важливо зауважити, що процеси обробки та аналізу даних у SIEM-системах не є завжди досконалими. Незважаючи на те, що ці системи здатні виявляти багато типів кіберінцидентів, вони можуть пропускати нові, наприклад, раніше не відомі типи кібератак, а також є ризик виникнення надмірної генерації сповіщень про потенційні кібеінциденти, що може призвести до ігнорування реально небезпечних подій. Тому процес постійного покращення і оптимізації процесів аналізу та реагування на кіберінциденти у SIEM-системах є важливим та актуальним.

Використання новітніх технологій штучного інтелекту, машинного навчання, обробки великих обсягів даних, а також постійне вдосконалення кореляційних алгоритмів їхнього аналізу може забезпечити більш точне виявлення кіберінцидентів SIEM-системою, що покращить кіберзахист БД ІКСВП у цілому.

Аналіз останніх досліджень. У публікації [9] запропоновано архітектуру інтелектуальної SIEM-системи для виявлення кіберінцидентів у БД ІКСВП. Вона складається з наступних рівнів: рівень збору даних, рівень управління даними, рівень аналізу даних і рівень прийняття та реалізації рішень. Рівень аналізу даних є головним і критичним елементом архітектури [10]. Він забезпечує можливість ефективного виявлення та реагування на кіберінциденти у реальному часі.

У наукових публікаціях процесам аналізу даних у SIEM-системах приділяється велика увага. Це пояснюється тим, що ефективність SIEM-систем безпосередньо залежить від якості цих процесів. Вдосконалення моделей та методів аналізу є постійним процесом, який потребує інноваційних підходів та адаптації до нових кіберзагроз.

У [11] зроблено акцент на важливості впровадження та удосконалення технологій SIEM-систем для підвищення рівня захисту ІКС. Проведено огляд методів кореляції, які можуть бути впроваджені в SIEM-системах для більш ефективного аналізу та протидії кіберінцидентам.

Публікація [12] присвячена використанню моделей машинного та глибокого навчання для виявлення мережевих кібератак, з акцентом на ефективність різних класифікаторів та їх здатність виявляти різні типи кіберінцидентів на основі набору даних UNSW-NB15.

Робота [13] присвячена оптимізації інфраструктури SIEM-системи за допомогою кореляційно-регресійного аналізу подій. Представлено, зменшення кількість помилкових спрацьовувань і підвищення здатності SIEM-системи виявляти кіберінциденти за рахунок покращення нормалізації журналів подій та ефективного використання правил кореляції.

Таким чином, аналіз сучасних досліджень та публікації щодо кореляції та аналізу подій безпеки в SIEM-системах, вказує значний прогрес у цій області. Однак, постійний розвиток кібератак, вимагає подальшого вдосконалення моделей і методів кіберзахисту ІКСВП. Це підкреслює важливість даної роботи для сфери кібербезпеки, зокрема для ефективного виявлення нових типів кібератак/кіберінцидентів SIEM-системами.

Метою роботи є розробка методики виявлення кіберінцидентів SIEM-системою, пов’язаних з БД інформаційно-комунікаційних систем військового призначення.

Виклад основного матеріалу. Для досягнення поставленої мети, доцільно застосувати підхід, який представлено у [14, 15]. Суть даного підходу полягає у введені вагових коєфіцієнтів для антецедентів нечітких лінгвістичних правил, що описують кіберінциденти у базі знань, які можуть виникнути під час функціонування ІКСВП. Ці коефіцієнти є числами з інтервалу [0, 1], відображають значимість ознак кіберінциденту у системі нечіткого логічного виводу.

Отже, задача виявлення кіберінцидентів у БД ІКСВП матиме наступний виглід (1):

$$F_l^* = (f_{1l}^*, f_{2l}^*, \dots, f_{nl}^*) \to c_j \in C = (c_1, c_2, \dots, c_m) \quad (1)$$

де F_l^* – множина ознак кіберінциденту, пов'язаному з функціонуванням БД ІКСВП, отриманих з різних рівнів кіберзахисту БД [12].

Область зміни ознак кіберінцидентів $f_{il} \in \left[\underline{f_{il}}, \overline{f_{il}}\right],\ i = 1 \dots n,\ l = 1 \dots L,$ які отримуються з різних рівнів кіберзахисту БД $l = 1 \dots L$ і вихідного значення ідентифікації $c_i \in \left[\overline{c_j}, \underline{c_j}\right],\ j = 1 \dots m.$

Відповідно $\underline{f_{il}}$, $(\overline{f_{il}})$ – нижнє (верхнє) значення ознак кіберінциденту f_{il}, l-го рівня кіберзахисту БД, $i = 1 \dots n,\ l = 1 \dots L;$ $\underline{c_j}$ $(\overline{c_j})$ – нижнє (верхнє) значення результату ідентифікації c_j.

Для вирішення задачі, вхідні і вихідні змінні розглядаються, як лінгвістичні змінні, що задані на універсальних множинах (2) [16, 17]:

$$f_{il} = \left[\underline{f_{il}}, \overline{f_{il}}\right],\ c_j = \left[\underline{c_j}, \overline{c_j}\right] \quad (2)$$

Для оцінки (3) доцільно використовувати якісні терми, які входять до множин термів:

$A_{il} = \{a_{il}^1, a_{il}^2, \dots, a_{il}^k\}$ – терм-множина змінної f_{il}, де a_{il}^k– k-й лінгвістичний терм змінної f_{il}, $k = 1 \dots k_i, i = 1 \dots n$ l-го рівня кіберзахисту БД $l = 1 \dots L$;

$\Delta = \{\delta_1, \delta_2, \dots, \delta_m\}$ – терм-множина змінної c_j, де δ_j, $j = 1 \dots m$ – лінгвістичний терм змінної c_j, m – число можливих класів кіберінцидентів, пов'язаних з БД.

Таким чином, лінгвістичні терми $a_{il}^k \in A_{il}, k = 1 \dots k_i, i = 1 \dots n,\ l = 1 \dots L$ та $\delta_j \in \Delta, j = 1 \dots m$ можна розглядати як нечіткі множини, які задані на універсальних множинах f_{il}, c_j.

Експертні дані можуть бути представленні у вигляді багатовимірної матриці знань про кіберінциденти (табл.1).

Таблиця 1

Багатовимірна таблиця ознак кіберінцидентів у БД ІКСВП і класів, що їм відповідають з урахуванням ваги антецедентів у межах окремих правил

Номер вхідної комбінації значень	Ознаки кіберінцидентів, отримані з різних рівнів кіберзахисту БД										Клас кіберінциденту
	f_{1l}	Ω_{1l}	f_{2l}	Ω_{2l}	…	f_{il}	Ω_{il}	…	f_{nl}	Ω_{nl}	c
11	α_{1l}^{11}	$\Omega_{1l}{}^{11}$	α_{2l}^{11}	$\Omega_{2l}{}^{11}$	…	α_{il}^{11}	$\Omega_{il}{}^{11}$	…	α_{nl}^{11}	$\Omega_{nl}{}^{11}$	δ_1
12	α_{1l}^{12}	$\Omega_{1l}{}^{12}$	α_{2l}^{12}	$\Omega_{2l}{}^{12}$	…	α_{il}^{12}	$\Omega_{il}{}^{12}$	…	α_{nl}^{12}	$\Omega_{nl}{}^{12}$	
…	…		…		…	…		…	…		
$1k_1$	$\alpha_{1l}^{1k_1}$	$\Omega_{1l}{}^{1k}{}_1$	$\alpha_{1l}^{1k_2}$	$\Omega_{2l}{}^{1k}{}_2$	…	$\alpha_{il}^{1k_1}$	$\Omega_{il}{}^{1k}{}_1$	…	$\alpha_{nl}^{1k_1}$	$\Omega_{nl}{}^{1k}{}_1$	
…	…		…		…	…		…	…		…
$j1$	α_{1l}^{j1}	$\Omega_{1l}{}^{j1}$	α_{2l}^{j1}	$\Omega_{2l}{}^{j1}$	…	α_{il}^{j1}	$\Omega_{il}{}^{j1}$	…	α_{nl}^{j1}	$\Omega_{nl}{}^{j1}$	δ_j
$j2$	α_{1l}^{j2}	$\Omega_{1l}{}^{j2}$	α_{2l}^{j2}	$\Omega_{2l}{}^{j2}$	…	α_{il}^{j2}	$\Omega_{il}{}^{j2}$	…	α_{nl}^{j2}	$\Omega_{nl}{}^{j2}$	
…	…		…		…	…		…	…		
jk_j	$\alpha_{1l}^{jk_j}$	$\Omega_{1l}{}^{jk}{}_j$	$\alpha_{2l}^{jk_j}$	$\Omega_{2l}{}^{jk}{}_j$	…	$\alpha_{il}^{jk_j}$	$\Omega_{il}{}^{jk}{}_j$	…	$\alpha_{nl}^{jk_j}$	$\Omega_{nl}{}^{jk}{}_j$	
…	…		…		…	…		…	…		…
m_1	α_{1l}^{m1}	$\Omega_{1l}{}^{m1}$	α_{2l}^{m1}	$\Omega_{2l}{}^{m1}$	…	α_{il}^{m1}	$\Omega_{il}{}^{m1}$	…	α_{nl}^{m1}	$\Omega_{nl}{}^{m1}$	δ_m
m_2	α_{1l}^{m2}	$\Omega_{1l}{}^{m2}$	α_{2l}^{m2}	$\Omega_{2l}{}^{m2}$	…	α_{il}^{m2}	$\Omega_{il}{}^{m2}$	…	α_{nl}^{m2}	$\Omega_{nl}{}^{m2}$	
…	…		…		…		…	…			
mk_m	$\alpha_{1l}^{mk_m}$	$\Omega_{1l}{}^{mk}{}_m$	$\alpha_{2l}^{mk_m}$	$\Omega_{2l}{}^{mk}{}_m$	…	$\alpha_{il}^{mk_m}$	$\Omega_{il}{}^{mk}{}_m$	…	$\alpha_{nl}^{mk_m}$	$\Omega_{nl}{}^{mk}{}_m$	

Тоді, з врахуванням ваг ознак кіберінцидентів у БД ІКСВП, нечітка база знань, яка представлена сукупністю нечітких правил “ЯКЩО-ТО”, що зв’язують лінгвістичні оцінки ознак кіберінцидентів з результатами їхньої ідентифікації, прийме наступний вигляд [14, 15]:

ЯКЩО ($f_{il} = \alpha_{1l}^{11}$з вагою $\Omega_{1l}{}^{11}$) ТА ($f_{2l} = \alpha_{2l}^{11}$ з вагою $\Omega_{2l}{}^{11}$) ТА…ТА ($f_{nl} = \alpha_{nl}^{11}$з вагою $\Omega_{nl}{}^{11}$) АБО

($f_{il} = \alpha_{1l}^{12}$з вагою $\Omega_{1l}{}^{12}$) ТА ($f_{2l} = \alpha_{2l}^{12}$з вагою $\Omega_{2l}{}^{12}$) ТА…ТА ($f_{nl} = \alpha_{nl}^{12}$з вагою $\Omega_{nl}{}^{12}$) АБО

($f_{il} = \alpha_{1l}^{1k_1}$з вагою $\Omega_{1l}{}^{1k_1}$) ТА ($f_{2l} = \alpha_{2l}^{1k_1}$з вагою $\Omega_{2l}{}^{1k_1}$) ТА…ТА ($f_{nl} = \alpha_{nl}^{1k_1}$з вагою $\Omega_{nl}{}^{1k_1}$) ТО (с=δ_1),…

…, ЯКЩО ($f_{il} = \alpha_{1l}^{j1}$з вагою $\Omega_{1l}{}^{j1}$) ТА ($f_{2l} = \alpha_{2l}^{j1}$з вагою $\Omega_{2l}{}^{j1}$) ТА…ТА ($f_{nl} = \alpha_{nl}^{j1}$з вагою $\Omega_{nl}{}^{j1}$) АБО

($f_{il} = \alpha_{1l}^{j2}$з вагою $\Omega_{1l}{}^{j2}$) ТА ($f_{2l} = \alpha_{2l}^{j2}$з вагою $\Omega_{2l}{}^{j2}$) ТА…ТА ($f_{nl} = \alpha_{nl}^{j2}$з вагою $\Omega_{nl}{}^{j2}$) АБО

($f_{il} = \alpha_{1l}^{jk_j}$з вагою $\Omega_{1l}{}^{jk_j}$) ТА ($f_{2l} = \alpha_{2l}^{jk_j}$з вагою $\Omega_{2l}{}^{jk_j}$) ТА…ТА ($f_{nl} = \alpha_{nl}^{jk_j}$з вагою $\Omega_{nl}{}^{jk_j}$) ТО (с=δ_j),…

…, ЯКЩО ($f_{il} = \alpha_{1l}^{m1}$ з вагою $\Omega_{1l}{}^{m1}$) ТА ($f_{2l} = \alpha_{2l}^{m1}$з вагою $\Omega_{2l}{}^{m1}$) ТА…ТА ($f_{nl} = \alpha_{nl}^{m1}$з вагою $\Omega_{nl}{}^{m1}$) АБО

($f_{il} = \alpha_{1l}^{m2}$з вагою $\Omega_{il}{}^{m2}$)ТА($f_{2l} = \alpha_{2l}^{m2}$з вагою $\Omega_{2l}{}^{m2}$)ТА…ТА($f_{nl} = \alpha_{nl}^{m2}$з вагою $\Omega_{nl}{}^{m2}$) АБО

($f_{il} = \alpha_{1l}^{mk_m}$з вагою $\Omega_{il}{}^{mk_m}$)ТА($f_{2l} = \alpha_{2l}^{mk_m}$з вагою $\Omega_{2l}{}^{mk_m}$)ТА…ТА($f_{nl} = \alpha_{nl}^{mk_m}$з вагою $\Omega_{nl}{}^{mk_m}$)

ТО(с=δ_m), (3)

де α_{il}^{jk} - лінгвістична оцінка ознаки кіберінциденту у БД ІКСВП $f_{il}, i = 1 \dots n$; l=1…L у рядку k j-ої диз’юнкції, що визначається на терм-множині $A_i = \{\alpha_{il}^1, \alpha_{il}^2, \dots, \alpha_{il}^{k_i}\}$;

$\delta_j \in \Delta, j = 1 \dots m$ - лінгвістична оцінка класу кіберінциденту у БД ІКСВП, що визначається на терм-множині $\Delta = \{\delta_1, \delta_2, \dots, \delta_m\}$,

$\Omega_{nl}{}^{mk}$ - вага ознак кіберінцидентів у межах правил.

З урахуванням вагових коефіцієнтів антецедентів у межах нечітких правил, нечітка база знань (3), може бути представленою модифікованою системою нечітких рівнянь (4) наступним чином:

$$\mu^{\delta_j}(f_{1l}, f_{2l}, \dots, f_{nl}) = \vee_{k=1}^{k_j} \left\{ \wedge_{i=1}^{n} \left[\mu^{\alpha_{il}^{jk}}(f_{il})\, \Omega_{il}^{jk} \right] \right\}, j = 1 \dots m \quad (4)$$

Шляхом заміни операцій $\wedge$ та $\vee$ на операції min та max, які їм відповідають, модифікова модель нечіткої ідентифікації кіберінцидентів SIEM-системами [13] із зваженими антецедентами нечітких правил прийме наступний вигляд:

$$\mu^{\delta_j}(f_{il}, f_{2l}, \dots, f_{nl}) = \underset{k = \overline{1, k_j}}{\overset{max}{}} \left\{ \underset{i = \overline{1, n}}{\overset{min}{}} \left\{ \mu^{\alpha_{il}^{jk}}(f_{il})\, \Omega_{il}^{jk} \right\},\ j = \overline{1, m} \right\}. \quad (5)$$

Дана модель є основою для розробки правило-орієнтованого методу виявлення кіберінцидентів, пов’язаних з БД SIEM-системи із врахуванням ознак кіберінцидентів, отриманих з різних рівнів кіберзахисту БД ІКСВП.

Графічно задачу ідентифікації кіберінцидентів можна представити наступним чином (рис.1):

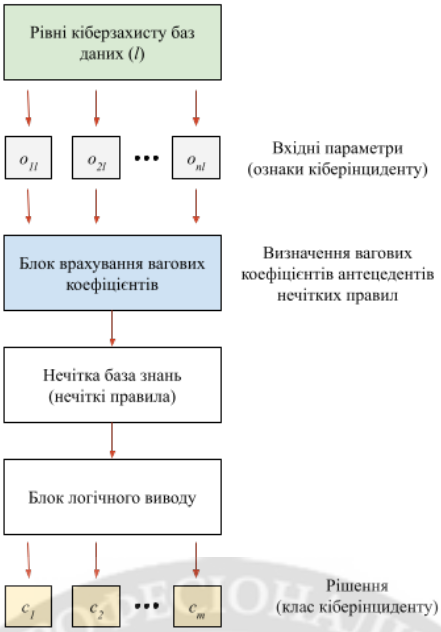

Рисунок 1 – Графічна інтерпретація задачі ідентифікації кіберінцидентів в БД ІКСВП

Основними труднощами, які виникають під час вирішення наведеної задачі є:

1. Обробка та аналіз великих обсягів даних є дуже ресурсномісткою і потребує значної обчислювальної потужності. Відповідно до цього, для виявлення кіберінцидентів у великих масивах даних необхідно застосовувати методи і алгоритмів, здатні швидко обробляти накопичену інформацію.

2. Дані про події у системі містять велику кількість неструктурованих або нерелевантних даних, що ускладнює ідентифікацію дійсно важливих подій.

3. Дані можуть надходити з різних джерел, які мають різні формати та структури. Об’єднання та кореляція таких даних може бути складним завданням.

4. Відомості про кіберінциденти можуть бути неповними або фрагментованими. Відсутність достатньої кількості ознак може ускладнити ідентифікацію і кореляцію подій.

5. Налаштування та тренування моделей машинного навчання потребує значних ресурсів і знань. Постійна адаптація моделей до нових загроз є необхідною, що може бути складним процесом.

Наведене підтверджує доцільність створення у складі SIEM-системи інтелектуальної підсистеми підтримки прийняття рішень, в основу функціонування якої має бути покладена модель ідентифікації кіберінцидентів на основі нечітких правил та нечіткого логічного виводу.

При цьому, для її розробки необхідно враховувати лінгвістичний характер типу кіберінциденту (вихідна змінна) та його ознак (вхідні змінні). У свою чергу, причинно-наслідкові зв’язки між кіберінцидентом та його ознаками повинні бути описані експертом зрозумілою мовою, а після цього, формалізовані у вигляді множини нечітких логічних правил.

Слід зауважити, що при великій кількості ознак кіберінцидентів, доцільно побудувати дерево логічного виводу, яке визначає порядок вкладення висловлювань одне в одне [16, 17].

На рис. 2 наведено дерево логічного виводу для нечіткого кореляційного правила: якщо на одному сервері баз даних з тією самою IP-адресою відбулося п’ять спроб доступу до різних таблиць, які завершилися невдало протягом п’яти хвилин, при цьому використовувалися різні ідентифікатори користувачів БД, а також було здійснено успішний доступ до будь-якої таблиці з тієї ж самої IP-адреси протягом цього часу, то ця подія повинна бути розглянута офіцером з безпеки.

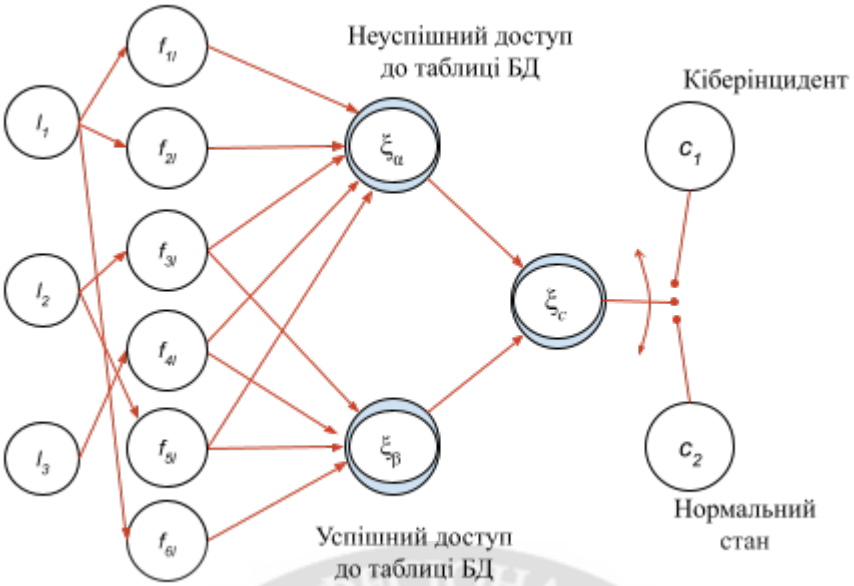

Рисунок 2 - Дерево логічного виводу для нечіткого кореляційного правила

У даному прикладі рівні кіберзахисту БД відтворено через $l_1 \div l_3$ (табл. 2), а ознаки кібреінциденту БД через $f_{1l} \div f_{6l}$ (табл. 3).

Таблиця 2

Рівні кіберзахисту БД

Рівень	Зміст рівня
l_1	Рівень БД та СКБД
l_2	Рівень ОС
l_3	Рівень мережі

Таблиця 3

Ознаки кіберінциденту БД відповідно її рівнів захисту

Ознака	Рівні кіберзахисту БД	Зміст ознаки	Тип
f_{1l}	l_1	Кількість невдалих спроб доступу до таблиць	Числовий
f_{2l}	l_1	Кількість ідентифікаторів користувачів БД	Числовий
f_{3l}	l_2	Тривалість за часом спроб входу до системи	Числовий
f_{4l}	l_3	Кількість IP-адрес, що задіяні під час доступу до таблиць	Числовий
f_{5l}	l_2	Кількість серверів баз даних, що задіяні під час доступу до таблиць	Числовий
f_{6l}	l_1	Кількість вдалих спроб доступу до таблиць	Числовий

Відповідно, через c_1 та c_2 позначено тип події, що відбувається у БД ІКСВП (табл. 4)

Таблиця 4

Ознаки кіберінциденту БД ІКСВП

Подія	Зміст події
α	Неуспішний доступ до таблиці БД
β	Успішний доступ до таблиці БД
c_1	Кіберінцидент
c_2	Нормальний стан системи

Структура дерева логічного виводу відповідає відношенням (6) – (8):

$$c = \xi_c(\alpha, \beta), \tag{6}$$

$$\alpha = \xi_\alpha(f_{1l}, f_{2l}, f_{3l}, f_{4l}, f_{5l}), \tag{7}$$

$$\beta = \xi_\beta(f_{3l}, f_{4l}, f_{5l}, f_{6l}). \tag{8}$$

Таблиця 5

Багатовимірна матриця знань про кіберінциденти

Ознака	Значення	Тип	Кіберінцидент
		α	
f_{1l}	В		
f_{2l}	В		
f_{3l}	Н	В	
f_{4l}	Н		
f_{5l}	вС		C_1
Ознака	Значення	β	
f_{3l}	нС		
f_{4l}	Н	В	
f_{5l}	В		
f_{6l}	Н		
Ознака	Значення	α	
f_{1l}	вС		
f_{2l}	вС		
f_{3l}	нС	вС	
f_{4l}	Н		
f_{5l}	С		C_1
Ознака	Значення	β	
f_{3l}	нС		
f_{4l}	Н	вС	
f_{5l}	вС		
f_{6l}	Н		

Для оцінки значень лінгвістичних змінних $f_{1l} \div f_{6l}$, α, β застосовується єдина шкала якісних термів: Н – низький; нС – нижче за середній; С – середній; вС – вище за середній; В – високий. Кожний з цих термів задається відповідною функцією належності.

З формальної точки зору задача ідентифікації кіберінцидентів на основі нечітких правил відповідає математичній моделі ідентифікації об'єкту з дискретним виходом [16, 17]. Так, для ідентифікації кіберінцидента c_1, співвідношення має наступний вигляд:

$$\mu^{c_1}(c) = [\mu^B(\alpha) \wedge \mu^B(\beta)] \vee [\mu^{вC}(\alpha) \wedge \mu^{вC}(\beta)], \tag{9}$$

де $\mu^B(\alpha) = [\mu^B(f_{1l}) \wedge \mu^B(f_{2l}) \wedge \mu^H(f_{3l}) \wedge \mu^H(f_{4l}) \wedge \mu^{вC}(f_{5l})]$,

$\mu^B(\beta) = [\mu^{нC}(f_{3l}) \wedge \mu^H(f_{4l}) \wedge \mu^B(f_{5l}) \wedge \mu^H(f_{6l})]$;

$\mu^{вC}(\alpha) = [\mu^{вC}(f_{1l}) \wedge \mu^{вC}(f_{2l}) \wedge \mu^{нC}(f_{3l}) \wedge \mu^H(f_{4l}) \wedge \mu^C(f_{5l})]$,

$\mu^{вC}(\beta) = [\mu^{нC}(f_{3l}) \wedge \mu^H(f_{4l}) \wedge \mu^{вC}(f_{5l}) \wedge \mu^H(f_{6l})]$;

У загальному випадку, наведені нечіткі логічні рівняння дозволяють приймати рішення щодо ідентифікації кіберінциденту за наступним алгоритмом (рис. 3):

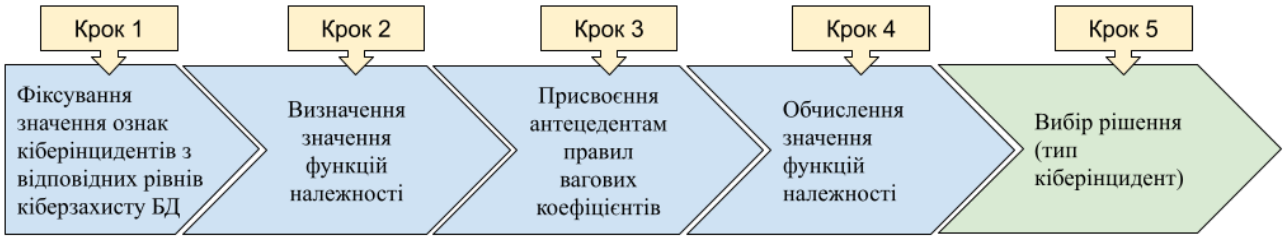

Рисунок 3 – Алгоритм ідентифікації кіберінциденту

Крок 1. Фіксуються значення ознак кіберінцидентів $F^* = (f_{1l}^*,\ f_{2l}^*,\ \dots,\ f_{nl}^*)$.

Крок 2. Визначаються значення функцій належності $\mu^k(f_{il}^*)$ при фіксованих значеннях параметрів $f_{il}^*, i = \overline{1,n}; k = \overline{1,K_i}$.

Крок 3. Присвоїти антецедентам правил вагові коефіцієнти Ω_i^k.

Крок 4. На основі логічних рівнянь (3.16) обчислюються значення функцій належності $\mu^{c_j}(f_{1l}^*, f_{2l}^*, \dots, f_{nl}^*)$ за вектором ознак $F^* = (f_{1l}^*,\ f_{2l}^*,\ \dots,\ f_{nl}^*)$ для всіх типів кіберінцидентів $c_1, c_2, \cdots, c_m$.

Логічні операції І (∧) та АБО (∨) над функціями належності заміняються операціями min та max:

$$\mu^k(f_{il}^*)\,\Omega_i^k \wedge \mu^k(f_{jl}^*)\Omega_j^k = min\ \left[\mu^k(f_{il}^*)\Omega_i^k, \mu^k(f_{jl}^*)\Omega_j^k\right];\ i \neq j, \tag{10}$$

$$\mu^k(f_{il}^*)\Omega_i^k \vee \mu^k(f_{jl}^*)\Omega_j^k = max\ \left[\mu^k(f_{il}^*)\Omega_i^k, \mu^k(f_{jl}^*)\Omega_j^k\right];\ i \neq j, \tag{11}$$

Крок 5. Вибір рішення c_j^* (тип кіберінцидента) за умови:

$$\mu^{c_j}(f_{1l}^*, f_{2l}^*, \dots, f_{nl}^*) = max\ [\mu^{c_j}(f_{1l}^*,\ f_{2l}^*,\ \dots,\ f_{nl}^*)]. \tag{12}$$

Слід зауважити, що вирішення задачі присвоєння вагових коефіцієнтів антецедентам правил може бути зведеною до визначення степенів належності елементів до множини й побудові на їх основі функцій належності (ФН). Цьому присвячено роботу [16] . Проте, для її ефективного вирішення, необхідно зробити правильний вибір необхідного метода побудови ФН з метою використання подальших методів її обробки. Тому, дане питання потребує більш глибокого дослідження. Задача визначення вагових коефіцієнтів антецедентів нечітких правил може бути сформульованою наступним чином.

Дано: нечітка база знань, що містить нечіткі правила виду (3).

Необхідно: для кожної пари антецедентів правила визначити ступінь переваги та побудувати ФН нечіткій множині “важливість”, яка характеризує “степінь важливості” антецедента в правилі та представляє собою умову його домінування.

Для методів формування ФН характерним є [18]:

способом опитування (індивідуальний (d_1), груповий (d_2));

видом процедури збору даних (порівняння (p_1), оцінювання об’єктів (p_2), порівняння пар об’єктів (p_3));

типологією експертної інформації (ранжування (e_1), парне або послідовне порівняння(e_2));

уявленням про характер порівняння або оцінювання (порівняння здійснюється за степенем виразності певної характеристики (v_1) чи за степенем віддаленості від ідеальної точки (v_2);

інтерпретацією експертної інформації (розгляд результатів порівняння або оцінювання як детермінованих (N) так й імовірнісних (D)).

Крім того, з точки зору практичної реалізації до наведеного переліку слід додати: простоту та зручність (трудомісткі (T) та простоту й компактність у реалізації(L)).

Отже, для обґрунтованого вибору методу побудови ФН нечітких множин для рішення конкретної практичної задачі, його слід розглядати, як кортеж вигляду:

$$M = \langle \alpha, \beta, \gamma, \phi, \sigma, \theta, \rangle, \quad (13)$$

де α– спосіб експертного опитування;

β – вид процедури збору даних;

γ– тип експертної інформації, яка використовується;

ϕ – характер порівняння або оцінювання;

σ – інтерпретація даних експертного опитування;

θ– простота та зручність.

Крім того, основними вимогами до процедури побудови ФН [18] є наступні.

Опитування експертів повинно здійснюватися при наявності ясної фізичної інтерпретації поняття степені приналежності в режимі "оператор-комп'ютер".

Процедури побудови ФН не повинні нав'язувати експерту апріорних обмежень на його відповіді (наприклад, вимагати транзитивних оцінок).

Кількість запитань до експерта повинно бути невеликим. Наприклад, для застосування методу парних порівнянь число об'єктів, які порівнюються не повинно перевищувати 15.

Визначення ФН повинно здійснюватися при фіксованій множині термів відповідної лінгвістичної змінної.

Процедура повинна включати алгоритми формалізації нечітких множин як з числовою, так й нечислової областями визначення.

Аналіз поставленої задачі та характеру діяльності офіцерів з безпеки показує, що для її вирішення може бути застосований метод типу (14) [19]:

$$\langle d_1, p_3, e_2, v_1, N, L \rangle, \quad (14)$$

де d_1 –індивідуальний спосіб опитування;

p_3 –процедура збору даних – порівняння пар об'єктів;

e_2 –типологія експертної інформації – парне або послідовне порівняння;

v_1 – характер порівняння або оцінювання – порівняння здійснюється за степенем виразності певної характеристики;

N – інтерпретація експертної інформації – розгляд результатів порівняння або оцінювання, як детермінованих;

L – простота та зручність у реалізації.

Визначеним вимогам відповідає метод, який базується на ідеї розподілу ступенів належності елементів універсальної множини відповідно до їх рангів або метод парних порівнянь на основі рангових оцінок [16, 17, 19-21].

Отже, для вирішення задачі, під рангом антецеденту $f_{jl}.l_{f_{jl}k_{f_j}} \in O^T$ будемо розуміти число $r_\Omega\left(f_{jl}.l_{f_{jl}k_{f_j}}\right)$, яке характеризує значимість антецеденту у формуванні правила, яке описується нечітким термом Ω. Припускаємо, що виконується правило: чим більшим є ранг елемента, тим більшою є ступінь його належності.

Уведемо наступні позначення (15):

$$r_\Omega\left(f_{jl}.l_{f_{jl}k_{f_j}}\right) = r_j,\ \mu_\Omega\left(f_{jl}.l_{f_{jl}k_{f_j}}\right) = \mu_j,\ j = \overline{1,n}. \quad (15)$$

Тоді правило розподілу ступенів приналежності задається у вигляді співвідношення: $\frac{\mu_1}{r_1} = \frac{\mu_2}{r_2} \ldots \frac{\mu_n}{r_n}$, з умовою нормування: $\mu_1 + \mu_2 + \ldots + \mu_n = 1$.

Враховуючи це, отримуються співвідношення (15), які дають змогу обчислити ступені приналежності $\mu_\Omega(f_{jl}.l_{f_{jl}k_{f_j}})$ антецедентів $f_{jl}.l_{f_{jl}k_{f_j}} \in F^T$ до нечіткого терму Ω шляхом використання відносних оцінок рангів $\frac{r_i}{r_j} = a_{ij},\ i,j = \overline{1,n}$.

$$\left.\begin{aligned}
\mu_1 &= \left(1 + \frac{r_2}{r_1} + \frac{r_3}{r_1} + \ldots + \frac{r_n}{r_1}\right)^{-1} \\
\mu_2 &= \left(\frac{r_1}{r_2} + 1 + \frac{r_3}{r_2} + \ldots + \frac{r_n}{r_2}\right)^{-1} \\
&\ldots \\
\mu_n &= \left(\frac{r_1}{r_n} + \frac{r_2}{r_n} + \frac{r_3}{r_n} + \ldots + 1\right)^{-1}
\end{aligned}\right\} \quad (16)$$

За допомогою них створюється матриця (17), яка може інтерпретуватися як матриця парних порівнянь рангів. Для експертних оцінок елементів цієї матриці можна застосувати 9-ти бальну шкалу Сааті [18] (табл. 6):

1 – при відсутності переваги r_j над r_i;

3 – при слабій перевазі r_j над r_i;

5 – при суттєвій перевазі r_j над r_i;

7 – при явній перевазі r_j над r_i;

7 – при абсолютній перевазі r_j над r_i;

2, 4, 6, 8 – проміжні порівняльні оцінки.

$$A = \begin{bmatrix} 1 & \frac{r_2}{r_1} & \ldots & \frac{r_n}{r_1} \\ \frac{r_1}{r_2} & 1 & \ldots & \frac{r_n}{r_2} \\ \ldots & \ldots & \ldots & \ldots \\ \frac{r_1}{r_n} & \frac{r_2}{r_n} & \ldots & 1 \end{bmatrix} \quad (17)$$

Таким чином, на основі матриці (17) у відповідності до формул (16) можна визначити вагові коефіцієнти відносної важливості $\omega\left(f_{jl}, l_{f_{jl}k_{fi_j}}\right)$ антецедентів $f_{jl}.l_{f_{jl}k_{f_j}} \in F^T$ та побудувати функцію належності нечіткого терму Ω.

Таблиця 6

Шкала відносної важливості

Інтенсивність важливості	Якісна оцінка	Пояснення
0	Незрівнянність	Немає сенсу порівнювати елементи.
1	Рівна важливість елементів, що порівнюються	Елементи є рівними за значимістю.
3	Помірна (слаба) перевага одного над іншим	Існують показання про перевагу одного елемента над іншим, але вони не є переконливими.
5	Сильна (суттєва) перевага	Існують гарні докази і логічні критерії, котрі можуть показати, що елемент є більш важливим.
7	Очевидна перевага	Існує переконливий доказ більшої значимості одного елемента над іншим.
9	Абсолютна перевага	Максимально підтверджується відчутність одного елемента над іншим.
2, 4, 6, 8	Проміжні значення між двома сусідніми оцінками	Коли є необхідним компроміс.

Для прикладу візьмемо нечітке правило: Якщо кількість підозрілих SQL-запитів є Високою та Частота запитів є Високою та використання ресурсів СКБД є Високим , то це кіберінцидент, пов'язаний з БД**.**

Крок 1: Оцінювання парних порівнянь

Побудова матриці, в якій експерт оцінює важливість кожного антецедента порівняно з іншими антецедентами в нечіткому правилі. Наприклад, відповідно до наведеного правила:

A1: Кількість підозрілих SQL-запитів є Високою

A2: Частота запитів є Високою

A3: Використання ресурсів СКБД є Високим

Матриця парних порівнянь має виглядати наступним чином, де експерт (аналітик з кібербезпеки) оцінює важливість одного антецедента в порівнянні з іншим (табл. 7).

Таблиця 7

Матриця парних порівнянь антецедентів нечіткого правила

	A1	A2	A3
A1	1	5	1/3
A2	1/5	1	3
A3	3	1/3	1

В цій матриці кожне число показує, як експерт оцінює важливість одного антецедента в порівнянні з іншими в нечіткому правилі. Якщо експерт вважає, що антецедент A1 (Кількість підозрілих SQL-запитів) важливіший за антецедент A2 (Частота запитів), він ставить 5 балів, що вказує на цей відносний ранг.

Крок 2: Нормалізація матриці парних порівнянь

Після того, як матриця побудована, потрібно її нормалізувати, щоб отримати відносні ваги кожного антецедента.

Спочатку обчислимо суми кожного стовпця:

Сума стовпця A1: 1 + 1/5 + 3 = 4,2

Сума стовпця A2: 5 + 1 + 1/3 = 6,33

Сума стовпця A3: 1/3 + 3 + 1 = 4,33

Для подальшої нормалізації значення у кожному стовпці ділимо на загальну суму оцінок у цьому стовпці(табл. 8).

Таблиця 8

Нормалізована матриці парних порівнянь

	A1	A2	A3
A1	0,23	0,79	0,07
A2	0,05	0,15	0,69
A3	0,71	0,05	0,23

Крок 3: Отримання оберненої матриці

Виходячи з того, що логічні операції І (∧) та АБО (∨) над функціями належності заміняються операціями min та max, то для врахування "степені важливості" антецедента, доцільно значення ваг зробити оберненими (табл. 9):

Таблиця 9

Обернена матриця парних порівнянь

	A1	A2	A3
A1	0,77	0,21	0,93
A2	0,95	0,85	0,31
A3	0,29	0,95	0,77

Крок 4: Визначення вектору ваг

Далі обчислюється середнє значення кожного рядка нормалізованої матриці:

Вага для A1: (0,77+ 0,21 + 0,93) / 3 ≈ 0.6

Вага для A2: (0,95 + 0,85 + 0,31) / 3 ≈ 0.7

Вага для A3: (0,29 + 0,95 + 0,77) / 3 ≈ 0.7

Крок 5: Створення нечіткого правила з вагою антецедентів

Якщо кількість підозрілих SQL-запитів є Високою з вагою 0,6 і Частота запитів є Високою з вагою 0,6 та використання ресурсів СКБД є Високим з вагою 0,7, то це кіберінцидент у БД**.**

Висновки. Запропонована методика виявлення кіберінцидентів в БД ІКСВП, на відміну від існуючих, дозволяє, шляхом застосування нечіткої моделі з вагами антецедентів правил, усунути невизначеність під час логічного виводу для прийняття рішень офіцером безпеки у деяких ситуаціях. Для визначення ваги антецедентів нечітких правил запропоновано використання методу парних порівнянь на основі рангових оцінок. Експериментальна перевірка застосування запропонованої методики на практиці дозволяє зробити висновок про підвищення точності виявлення кіберінцидентів у ІКСВП. Практична цінність методики полягає у можливості виявлення кіберінцидентів SIEM-системами в умовах неповноти та нечіткості інформації про них.

ЛІТЕРАТУРА:

1. Фесьоха В.В., Кисиленко Д.Ю., Нестеров О.М. Аналіз спроможності існуючих систем антивірусного захисту та покладених у їхню основу методів до виявлення нового шкідливого програмного забезпечення у військових інформаційних системах / Системи і технології зв'язку, інформатизації та кібербезпеки 2023. Т. 3. С. 143–151.

2. Байдур О., Вдосконалення кіберзахисту збройних сил з урахуванням досвіду протидії військовим кіберобераціям російської федерації в 2022 році, Кібербезпека: освіта, наука, техніка 2022, 1, 31-45. URL: https:// doi.org/10.28925/2663-4023.2022.17.3145.

3. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році [Електронний ресурс]. – Режим доступу: https://scpc.gov.ua/uk/articles/334

4. Герасимов, Б.М., Субач, І.Ю., Хусаінов, П.В., Міщенко, В.О. (2008) Аналіз задач моніторингу інформаційних мереж та методів підвищення ефективності їх функціонування. Сучасні інформаційні технології у сфері безпеки та оборони, 3(3), 24−27.

5. Субач І., Власенко О. Інформаційні технології захисту баз даних від кібератак в інформаційних системах військового призначення. Collection «Information Technology and Security».2022. No 10 (2). С. 177–193. URL: https://doi.org/10.20535/2411-1031.2022.10.2.270412.

6. Субач,І., Герасимов,Б. (2008). Показники якості інформаційного забезпечення та їх вплив на ефективність застосування ІСППР. Вісник Національного університету ім. Тараса Шевченка,20, 27–29.

7. O. Podzins, A. Romanovs, Why SIEM is Irreplaceable in a Secure IT Environment?, Open Conference of Electrical, Electronic and Information Sciences (eStream), Vilnius, Lithuania, 2019, pp. 1-5, URL: https:// doi.org/10.1109/eStream.2019.8732173.

8. Granadillo, Gustavo Gonzalez. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors (Basel, Switzerland) 21. 2021: n. pag. URL: https:// doi.org/10.3390/s21144759.

9. Субач І., Власенко О., Архітектура інтелектуальної SIEM-системи для виявлення кіберінцидентів у базах даних інформаційно-телекомунікаційних системах військового призначення. Збірник наукових праць ВІТІ. 2023. No4. С. 82–92. URL: https:// doi.org/10.58254/viti.4.2023.07.82.

10. Самохвалов, Ю., Толюпа, С. (2017). Кореляція подій у SIEM-системах з урахуванням немонотонного вывода. Захист інформації, 19(1), 5-9.

11. O. Sievierinov, M. Ovcharenko, Analysis of correlation rules in Security information and event management systems, Fourth International Scientific and Technical Conference «COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES»,– Kharkiv: NURE, 2020. – С. 24–25.

12. K.A. Dhanya, Sulakshan Vajipayajula, Kartik Srinivasan, Anjali Tibrewal, T. Senthil Kumar, T. Gireesh Kumar, Detection of Network Attacks using Machine Learning and Deep Learning Models, Procedia Computer Science, Volume 218, 2023, Pages 57-66, https://doi.org/10.1016/j.procs.2022.12.401.

13. Thursday Ehis, A.- mudu. (2023). Optimization of Security Information and Event Management (SIEM) Infrastructures, and Events Correlation/Regression Analysis for Optimal Cyber Security Posture. *Archives of Advanced Engineering Science*, 1–10. https://doi.org/10.47852/bonviewAAES32021068.

14. Субач І., Власенко О., Нечіткі моделі виявлення кіберінцидентів у базах даних інформаційно-комунікаційних систем військового призначення. Збірник наукових праць ВІТІ. 2024. No5. С. 165–180. URL: https://doi.org/10.58254/viti.5.2024.15.165.

15. Субач,І, Здоренко,Ю., Фесьоха,В. (2018). Методика виявлення кібератак типу JS(HTML) / Scrinject на основі застосування математичного апарату теорії нечітких множин. Збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут, 4, 125–131

16. Rotshtein A. P. Medical diagnostics using fuzzy logic. Vinnitsa: Continent-PRIM, 1996. 132 p.

17. Rothstein A. Intelligent identification technologies: fuzzy sets, genetic algorithms, neural networks. Vinnytsia: UNIVERSUM, 1999.

18. Borisov A.N., Krumberg O.A., Fedorov I.P. Decision-making based on fuzzy models: examples of use. - Riga: Znanie, 1990. - 184 c.

19. Субач, І. і Микитюк, А. (2023) «Методика формування нечітких асоціативних правил із зваженими атрибутами з бази даних SIEM-системи для виявлення кіберінцидентів в спеціальних інформаційно-комунікаційних системах», Collection "Information Technology and Security", 11(1), с. 47–59. https://doi.org/0.20535/2411-1031.2023.11.1.283575.

20. Шапочка М. К., Макарюк О. В. Застосування експертних оцінок при прийнятті рішень за умов невизначеності. Механізм регулювання економіки. 2006. № 4. С. 142-148.

21. Дебела, І. (2024). Проблеми синтезу рішення за нечітких умов: узгодження індивідуальних експертних оцінок. *Економічний простір*, (191), 174-177. https://doi.org/10.32782/2224-6282/191-28.

REFERENCES:

1. Fesokha V.V., Kysylenko D.Iu., Nesterov O.M. Analiz spromozhnosti isnuiuchykh system antyvirusnoho zakhystu ta pokladenykh u yikhniu osnovu metodiv do vyiavlennia novoho shkidlyvoho prohramnoho zabezpechennia u viiskovykh informatsiinykh systemakh / Systemy i tekhnolohii zviazku, informatyzatsii ta kiberbezpeky 2023. T. 3. S. 143–151.

2. Baidur O., Vdoskonalennia kiberzakhystu zbroinykh syl z urakhuvanniam dosvidu protydii viiskovym kiberoberatsiiam rosiiskoi federatsii v 2022 rotsi, Kiberbezpeka: osvita, nauka, tekhnika 2022, 1, 31-45. URL: https:// doi.org/10.28925/2663-4023.2022.17.3145.

3. Statystychnyi zvit za rezultatamy roboty Systemy vyiavlennia vrazlyvostei i reahuvannia na kiberintsydenty ta kiberataky v 2023 rotsi [Elektronnyi resurs]. – Rezhym dostupu: https://scpc.gov.ua/uk/articles/334

4. Herasymov, B.M., Subach, I.Iu., Khusainov, P.V., Mishchenko, V.O. (2008) Analiz zadach monitorynhu informatsiinykh merezh ta metodiv pidvyshchennia efektyvnosti yikh funktsionuvannia. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, 3(3), 24−27.

5. Subach I., Vlasenko O. Informatsiini tekhnolohii zakhystu baz danykh vid kiberatak v informatsiinykh systemakh viiskovoho pryznachennia. Collection «Information Technology and Security».2022. No 10 (2). S. 177–193. URL: https://doi.org/10.20535/2411-1031.2022.10.2.270412.

6. Subach,I., Herasymov,B. (2008). Pokaznyky yakosti informatsiinoho zabezpechennia ta yikh vplyv na efektyvnist zastosuvannia ISPPR. Visnyk Natsionalnoho universytetu im. Tarasa Shevchenka,20, 27–29.

7. O. Podzins, A. Romanovs, Why SIEM is Irreplaceable in a Secure IT Environment?, Open Conference of Electrical, Electronic and Information Sciences (eStream), Vilnius, Lithuania, 2019, pp. 1-5, URL: https:// doi.org/10.1109/eStream.2019.8732173.

8. Granadillo, Gustavo Gonzalez. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors (Basel, Switzerland) 21. 2021: n. pag. URL: https:// doi.org/10.3390/s21144759.

9. Subach I., Vlasenko O., Arkhitektura intelektualnoi SIEM-systemy dlia vyiavlennia kiberintsydentiv u bazakh danykh informatsiino-telekomunikatsiinykh systemakh viiskovoho pryznachennia. Zbirnyk naukovykh prats VITI. 2023. No4. S. 82–92. URL: https:// doi.org/10.58254/viti.4.2023.07.82.

10. Samokhvalov, Yu., Toliupa, C. (2017). Koreliatsiia podii u SIEM-systemakh z urakhuvanniam nemonotonnoho vыvoda. Zakhyst informatsii, 19(1), 5-9.

11. O. Sievierinov, M. Ovcharenko, Analysis of correlation rules in Security information and event management systems, Fourth International Scientific and Technical Conference «COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES»,– Kharkiv: NURE, 2020. – C. 24–25.

12. K.A. Dhanya, Sulakshan Vajipayajula, Kartik Srinivasan, Anjali Tibrewal, T. Senthil Kumar, T. Gireesh Kumar, Detection of Network Attacks using Machine Learning and Deep Learning Models, Procedia Computer Science, Volume 218, 2023, Pages 57-66, https://doi.org/10.1016/j.procs.2022.12.401.

13. Thursday Ehis, A.- mudu. (2023). Optimization of Security Information and Event Management (SIEM) Infrastructures, and Events Correlation/Regression Analysis for Optimal Cyber Security Posture. *Archives of Advanced Engineering Science*, 1–10. https://doi.org/10.47852/bonviewAAES32021068.

14. Subach I., Vlasenko O., Nechitki modeli vyiavlennia kiberintsydentiv u bazakh danykh informatsiino-komunikatsiinykh system viiskovoho pryznachennia. Zbirnyk naukovykh prats VITI. 2024. No5. S. 165–180. URL: https://doi.org/10.58254/viti.5.2024.15.165.

15. Subach,I, Zdorenko,Iu., Fesokha,V. (2018). Metodyka vyiavlennia kiberatak typu JS(HTML) / Scrinject na osnovi zastosuvannia matematychnoho aparatu teorii nechitkykh mnozhyn. Zbirnyk naukovykh prats Viiskovoho instytutu telekomunikatsii ta informatyzatsii imeni Heroiv Krut, 4, 125–131

16. Rotshtein A. P. Medical diagnostics using fuzzy logic. Vinnitsa: Continent-PRIM, 1996. 132 p.

17. Rothstein A. Intelligent identification technologies: fuzzy sets, genetic algorithms, neural networks. Vinnytsia: UNIVERSUM, 1999.

18. Borisov A.N., Krumberg O.A., Fedorov I.P. Decision-making based on fuzzy models: examples of use. - Riga: Znanie, 1990. - 184 c.

19. Subach, I. i Mykytiuk, A. (2023) «Metodyka formuvannia nechitkykh asotsiatyvnykh pravyl iz zvazhenymy atrybutamy z bazy danykh SIEM-systemy dlia vyiavlennia kiberintsydentiv v spetsialnykh informatsiino-komunikatsiinykh systemakh», Collection "Information Technology and Security", 11(1), s. 47–59. https://doi.org/0.20535/2411-1031.2023.11.1.283575.

20. Shapochka M. K., Makariuk O. V. Zastosuvannia ekspertnykh otsinok pry pryiniatti rishen za umov nevyznachenosti. Mekhanizm rehuliuvannia ekonomiky. 2006. № 4. S. 142-148.

21. Debela, I. (2024). Problemy syntezu rishennia za nechitkykh umov: uzghodzhennia indyvidualnykh ekspertnykh otsinok. Ekonomichnyi prostir, (191), 174-177. https://doi.org/10.32782/2224-6282/191-28.

Dr. Tech. Sci. Prof. Subach I.Y., Vlasenko O.V.

METHODOLOGY FOR DETECTING CYBER INCIDENTS BY SIEM IN DATABASES OF MILITARY INFORMATION AND COMMUNICATION SYSTEMS

With the integration of information and communication systems into military operations, the issue of their cyber defense is becoming increasingly important. The main target for cyberattacks are databases that mostly contain confidential information. One of the most effective approaches to ensuring cybersecurity of databases of military information and communication systems is to use the intelligent capabilities of a SIEM system. SIEM allows real-time monitoring, analysis and response to potential cyber incidents. The article proposes a methodology for detecting cyber incidents by a SIEM system in databases of military information and communication systems.

The main emphasis is placed on the multi-level protection of databases, which includes protection at the operating system level, the database level and the database management system, as well as the network level of protection. In order to improve the efficiency of cyber incident detection at the level of SIEM data analysis, an improved methodology based on fuzzy logic is used. Improvement of the methodology is achieved by introducing weights of antecedents in fuzzy rules, which allows, in some cases, to identify cyber incidents more accurately compared to existing models and methods. The weights of the antecedents of fuzzy rules are determined using the method of pairwise comparisons based on the rankings made on the 9-point Saaty scale. A decision-making algorithm for identifying cyber incidents based on the analysis of fuzzy rules and the weights of their antecedents is presented. An example of calculating the weights of antecedents of fuzzy rules using the method of pairwise comparisons based on rank estimates is given.

Keywords: database, information and communication system, cyber protection, cyber incident, cybersecurity, cyber attack, SIEM system, fuzzy set theory, fuzzy rules, pairwise comparison method.