Андрій Вікторович Давидюк, курсант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.
E-mail: andrey19941904@gmail.com.
Ігор Михайлович Куликівський, курсант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.
E-mail: ikylikovskiy1995@gmail.com.

Игорь Богданович Яковив, кандидат технических наук, доцент кафедры кибербезопасности и применения автоматизированных информационных систем и технологий, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.
Андрей Викторович Давидюк, курсант, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.
Игорь Михайлович Куликовский, курсант, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.

Ihor Yakoviv, candidate of technical sciences, associate professor, associate professor at the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.
Andrii Davydiuk, cadet, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.
Ihor Kulykivskyi, cadet, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

УДК 621.391:004.056.53 (045)

ПЕТРО ПАВЛЕНКО,
МИКОЛА ВІНОГРАДОВ,
СЕРГІЙ ГНАТЮК,
АНДРІЙ ГІЗУН,
ВІКТОР ГНАТЮК

МЕТОД ФОРМУВАННЯ ПРАВИЛ ЕКСТРАПОЛЯЦІЇ ІНЦИДЕНТІВ ДЛЯ МЕРЕЖЕВО-ЦЕНТРИЧНОГО МОНІТОРИНГУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Інциденти можуть порушити штатний режим функціонування інформаційно-телекомунікаційної системи і призвести до значних матеріальних та іміджевих збитків підприємства. Одним із підходів до інцидент-менеджменту є застосування мережево-центричної теорії управління для моніторингу інцидентів, проте не достатньо формалізованим є етап формування множини базових правил. З огляду на це, у цій роботі розроблено метод формування множини правил екстраполяції інцидентів для мережево-центричного моніторингу інформаційно-телекомунікаційних систем, який за рахунок

визначення можливих типів кібератак та категорій інцидентів, формування вектор-матриць імовірностей реалізації інцидентів, ранжування інцидентів за їх важливістю та визначення граничних значень ймовірностей, формування показників можливості появи інцидентів, а також формування та встановлення правил екстраполяції інцидентів, дозволяє автоматизувати і підвищити точність роботи систем мережево-центричного моніторингу інформаційно-телекомунікаційних систем.

Ключові слова: інцидент, мережево-центричний моніторинг, інформаційна безпека, кібератака, інформаційно-телекомунікаційна система.

Постановка проблеми. Виникнення інцидентів (подій, що можуть порушити конфіденційність, цілісність та доступність інформації у кіберпросторі [1]) може порушити штатний режим функціонування інформаційно-телекомунікаційної системи (ІТС) і призвести до значних матеріальних та іміджевих збитків підприємства [2]. Для локалізації наслідків та попередження рецидиву інцидентів, відповідно до міжнародного стандарту [3], необхідно розробляти ефективні процедури управління інцидентами, що, як правило, включають в себе такі базові процедури як виявлення, ідентифікація, оброблення та розслідування [4, 5]. Одним із підходів є застосування мережево-центричної теорії управління для моніторингу інцидентів – мережево-центрична система моніторингу об'єднує засоби моніторингу (під яким будемо розуміти систематичне накопичення та обробку даних про стан і динаміку зміни параметрів аналізованого об'єкта або процесу і представлення результатів у зручному для керівника або експерта вигляді) всіх рівнів і напрямків управління в єдине ціле.

Аналіз існуючих досліджень та постановка завдання. У роботі [6] розроблено метод мережево-центричного моніторингу інцидентів, який за рахунок обробки динамічно змінюваних параметрів кіберпростору, а саме класифікації кібератак та порівняння їх параметрів з еталонними, формування множини базових правил і встановлення зв'язків між підкласом кібератаки та категорією інцидентів на базі обробки їх статистики, ідентифікації об'єктів захисту та експертного оцінювання впливу на них інцидентів, узгодження суджень експертів та ранжування ступенів небезпеки інцидентів, дозволяє визначити найбільш важливі об'єкти захисту (складові ІТС чи кіберпростору), а також прогнозувати категорії інцидентів, які виникнуть внаслідок реалізації кібератаки, та їх рівень небезпеки (критичності). Проте, етап формування множини базових правил є не достатньо формалізованим і не дозволяє автоматизувати та прогнозувати появу інцидентів з достатньою точністю. Серед відомих підходів варто відзначити [7-8], де чітко формалізовано процес формування правил виявлення кризових ситуацій та порушника інформаційної безпеки відповідно.

Зважаючи на це, метою цієї статті є автоматизація та підвищення точності роботи систем мережево-центричного моніторингу за рахунок розробки методу формування евристичних правил визначення ймовірності появи (реалізації) того чи іншого інцидента.

Основна частина дослідження. Метод формування правил екстраполяції інцидентів для мережево-центричного моніторингу ІТС складається з таких п'яти етапів: 1) визначення можливих типів кібератак та категорій інцидентів; 2) формування вектор-матриць імовірностей реалізації інцидентів; 3) ранжування інцидентів за їх важливістю та визначення граничних значень ймовірностей; 4) формування показників можливості появи інцидентів; 5) формування та встановлення правил екстраполяції інцидентів.

Етап 1 – Визначення можливих типів кібератак та категорій інцидентів.

Крок 1. На цьому етапі необхідно задати множину еталонів параметрів кібератак $\mathbf{CA}$, які можуть виникнути в ІТС:

$$\{\bigcup_{i=1}^{n}\mathbf{CA}_i\}=\{\mathbf{CA}_1,\mathbf{CA}_2,...,\mathbf{CA}_n\}, \quad (1)$$

де $\mathbf{CA}_i \subseteq \mathbf{CA}$, $(i=\overline{1,n})$,

n – кількість кібератак, а

$$\mathbf{CA_i} = \{\bigcup_{j=1}^{m_i} \mathbf{CA_{ij}}\} = \{\mathbf{CA_{i1}}, \mathbf{CA_{i2}}, \ldots, \mathbf{CA_{im_i}}\}, \quad (2)$$

при цьому $\mathbf{CA_{ij}}$ $(j = \overline{1, m_i})$ – підмножини підкласів кібератак. Тобто

$$\{\bigcup_{i=1}^{n} \mathbf{CA_i}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} \mathbf{CA_{ij}}\}\} = = \{\{\mathbf{CA_{11}}, \mathbf{CA_{12}}, \ldots, \mathbf{CA_{1m_1}}\}, \{\mathbf{CA_{21}}, \mathbf{CA_{22}}, .., \mathbf{CA_{2m_2}}\}, .., \{\mathbf{CA_{n1}}, \mathbf{CA_{n2}}, \ldots, \mathbf{CA_{nm_n}}\}\}, \ (j = \overline{1, m_i}). \quad (3)$$

Для прикладу, у [6] визначено 22 типи кібератак $\mathbf{CA}$, об'єднанні в 4 класи DOS, R2L, U2R та PROBE, а саме:

$$\{\bigcup_{i=1}^{n} \mathbf{CA_i}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} \mathbf{CA_{ij}}\}\} =$$

$$\mathbf{\{\{BACK, LAND, NEPTUNE, POD, SMURT, TEARDROP\},}$$
$$\mathbf{\{BUFFER\_OVERFLOW, PERL, LOADMODULE, ROOTKIT\},}$$
$$\mathbf{\{FTP\_WRITE, GUESS\_PASSWD, IMAP, MULTIHOP, PHF, SPY,}$$
$$\mathbf{WAREZCLIENT, WAREZMASTER\},}$$
$$\mathbf{\{IPSWEEP, NMAP, PORTSWEEP, SATAN\}\}}.$$

Оскільки на етапі формування правил екстраполяції інцидентів клас кібератаки немає ніякого значення, то сформуємо єдину множину кібератак (без диференціювання на підмножини), що складатиметься з m елементів (типів кібератак):

$$\{\bigcup_{j=1}^{m} \mathbf{CA_j}\} = \{\mathbf{CA_1}, \mathbf{CA_2}, ..., \mathbf{CA_m}\}, \quad (4)$$

де $\mathbf{CA_i} \subseteq \mathbf{CA}$, $(j = \overline{1, m})$,

m – кількість типів кібератак, а при умові, що $m = 22$ (відповідно до [6,9]) вираз (4) матиме такий вигляд:

$$\{\bigcup_{j=1}^{22} \mathbf{CA_j}\} = \{\mathbf{CA_1}, \mathbf{CA_2}, ..., \mathbf{CA_{22}}\} =$$

$$\mathbf{\{BACK, LAND, NEPTUNE, POD, SMURT, TEARDROP,}$$
$$\mathbf{BUFFER\_OVERFLOW, PERL, LOADMODULE, ROOTKIT,}$$
$$\mathbf{FTP\_WRITE, GUESS\_PASSWD, IMAP, MULTIHOP, PHF, SPY,}$$
$$\mathbf{WAREZCLIENT, WAREZMASTER,}$$
$$\mathbf{IPSWEEP, NMAP, PORTSWEEP, SATAN\}.}$$

де $\mathbf{CA_1} = \mathbf{BACK}$, $\mathbf{CA_2} = \mathbf{LAND}$,…, $\mathbf{CA_{22}} = \mathbf{SATAN}$ – типи кібератак відповідно до [9].

Крок 2. Кожен з визначених видів кібератаки може виникати в залежності від значень параметрів контрольованого середовища і з певною імовірністю приводити до появи (реалізації) інцидентів, множина яких відповідно до [6] може бути задана таким чином:

$$\mathbf{I} = \{\bigcup_{i=1}^{n} \mathbf{I_i}\} = \mathbf{\{I_1, I_2, ..., I_n\}}, \ (i = \overline{1, n}), \quad (5)$$

де n – кількість можливих категорій інцидентів.

Наприклад, згідно рекомендацій CERT-UA (табл. 6 у [6]), при $n = 7$ маємо 7 основних категорій інцидентів (Malware, Internet Fraud, Unauthorized Access, Botnet, DDoS, Money Theft, Identity Theft):

$$\mathbf{I} = \{\bigcup_{i=1}^{7} \mathbf{I_i}\} = \{I_1, I_2, I_3, I_4, I_5, I_6, I_7\} = \{MW, IF, UA, BN, DD, MT, IT\},$$

де $I_1 = MW, I_2 = IF, I_3 = UA, I_4 = BN, I_5 = DD, I_6 = MT, I_7 = IT$ – категорії інцидентів.

Етап 2 – Формування вектор-матриць імовірностей реалізації інцидентів.

Згадане значення імовірностей реалізації інцидента визначеної категорії при проведенні певної кібератаки $PR_{CA_1}^{I_1} \dots PR_{CA_m}^{I_n}$ (нормоване від 0 до 1 або у відсотках) визначається експертним оцінюванням на основі статистики інцидентів. Відповідно, для кожної категорії інцидента може бути сформована вектор-матриця, елементи якої вказують на поточну оцінку експертом імовірності появи інцидента при ідентифікації одного із заданих типів кібератак.

$$\mathrm{PR}^{\mathrm{I_i}} = \left| PR_{CA_1}^{I_i} \quad PR_{CA_2}^{I_i} \quad \dots \quad PR_{CA_m}^{I_i} \right|, \ \mathrm{i} = \overline{1, \mathrm{n}}. \tag{6}$$

Наприклад, за умов дослідження, зазначених в [6], при $\mathrm{m} = 22$ і $\mathrm{n} = 7$ з урахуванням (6) матимемо 7 матриць PR^{I_i}:

$$\mathrm{PR}^{\mathrm{MW}} = \left| PR_{\mathbf{BACK}}^{\mathrm{MW}} \quad PR_{\mathbf{LAND}}^{\mathrm{MW}} \quad \dots \quad PR_{\mathbf{SATAN}}^{\mathrm{MW}} \right|, \text{при } \mathrm{i} = 1;$$

$$\mathrm{PR}^{\mathrm{IF}} = \left| PR_{\mathbf{BACK}}^{\mathrm{IF}} \quad PR_{\mathbf{LAND}}^{\mathrm{IF}} \quad \dots \quad PR_{\mathbf{SATAN}}^{\mathrm{IF}} \right|, \text{при } \mathrm{i} = 2;$$

$$\dots$$

$$\mathrm{PR}^{\mathrm{IT}} = \left| PR_{\mathbf{BACK}}^{\mathrm{IT}} \quad PR_{\mathbf{LAND}}^{\mathrm{IT}} \quad \dots \quad PR_{\mathbf{SATAN}}^{\mathrm{IT}} \right|, \text{при } \mathrm{i} = 7.$$

Етап 3 – Ранжування інцидентів за їх важливістю та визначення граничних значень імовірностей.

Сформовані значення вектор-матриць поелементно порівнюються з величиною PR_{lim} – граничним значенням імовірності, за якого експерт впевнений у виникненні інцидента I внаслідок реалізації кібератаки **CA** (визначається на основі аналізу статистики інцидентів). Це значення може бути одне для всіх кібератак та інцидентів, проте для підвищення точності і адекватності мережево-центричного моніторингу пропонується його диференціювати для різних категорій інцидентів. Граничне значення імовірності в такому разі залежатиме від важливості (критичності) інцидента, що визначається експертним оцінювання на основі таких показників, наприклад, як імовірні частота реалізації, величина збитків, впливи на різні складові контрольованого середовища. Один з можливих методів проведення експертного порівняння важливості інциденту – попарного порівняння з визначенням квадратного кореня – описаний в [10-12]. Чим більшим є показник важливості категорії інцидента, тим менше значення граничної імовірності $PR_{lim}^{\mathrm{I_i}}$ тобто система виявлення інцидентів, заснована на методі мережево-центричного моніторингу, спрацює значно раніше в порівнянні з менш важливими інцидентами.

Наприклад, з огляду на те, що визначено 7 категорій інцидентів згідно рекомендацій CERT-UA (хоча можна використати й інші підходи до категоризації, наприклад [3, 13] тощо) пропонується ввести 7 рівнів критичності (проте кількість рівнів критичності не обов'язково має дорівнювати кількості категорій інцидентів – ця кількість може бути як більшою, так і меншою) і визначити відповідні значення $PR_{lim}^{\mathrm{I_i}}$ для них (див. табл. 1).

Таблиця 1 – Значення граничних ймовірностей залежно від критичності інцидента

Рівень критичності інцидента	$PR_{lim}^{\mathrm{I_i}}$
1	0,15
2	0,2
3	0,25
4	0,3
5	0,32
6	0,333
7	0,35

У табл. 1 рівні критичності зазначені у порядку спадання, тобто найбільш важливі інциденти відносяться до 1 рівня критичності і вони будуть зафіксовані при $PR_{lim}^{\mathrm{I_i}} = 0{,}15$, а найменш важливі відносяться до 7 рівня відповідно при $PR_{lim}^{\mathrm{I_i}} = 0{,}35$. У результаті проведення експертного порівняння були отримані такі результати (див. табл. 2):

Таблиця 2 – Результати експертного порівняння

Інцидент, $\mathrm{I_i}$	Коефіцієнт важливості	Рівень критичності	$PR_{lim}^{\mathrm{I_i}}$
$\mathrm{I_1}$ = MW	0,2	3	0,25
$\mathrm{I_2}$ = IF	0,3	2	0,2
$\mathrm{I_3}$ = UA	0,05	5	0,32
$\mathrm{I_4}$ = BN	0,01	7	0,35
$\mathrm{I_5}$ = DD	0,35	1	0,15
$\mathrm{I_6}$ = MT	0,03	6	0,333
$\mathrm{I_7}$ = IT	0,06	4	0,3

Етап 4 – Формування показників можливості появи інцидентів.

Ознакою появи інциденту є спрацювання певного евристичного правила, що поєднує між собою залежність між власне появою інцидента та можливістю впливу кібератаки на його реалізацію. Для опису цієї евристики введемо показник можливості появи інцидента, що задається матрицею:

$$\mathrm{V^{Ii}} = \left|\mathrm{V_{CA_1}^{Ii}} \quad \mathrm{V_{CA_2}^{Ii}} \quad \ldots \quad \mathrm{V_{CA_m}^{Ii}}\right| = \left|PR_{\mathrm{CA_1}}^{I_i} \geq PR_{lim}^{I_i} \quad PR_{\mathrm{CA_2}}^{I_i} \geq PR_{lim}^{I_i} \quad \ldots \quad PR_{\mathrm{CA_m}}^{I_i} \geq PR_{lim}^{I_i}\right|, \qquad (7)$$

при чому $\mathrm{V_{CA_m}^{Ii}} = \begin{cases} 1, \text{ якщо } PR_{\mathrm{CA_m}}^{I_i} \geq PR_{lim}^{I_i} \\ 0, \text{ в іншому випадку} \end{cases}$.

Під час дослідження інциденту $\mathrm{I_1 = MW}$ (рівень критичності якого 3, а звідси $PR_{lim}^{\mathrm{I_1}} = PR_{lim}^{\mathrm{MN}} = 0{,}25$) отримали наступні значення імовірностей $PR_{\mathrm{CA_j}}^{\mathrm{I_1}} = \left|0{,}1; 0{,}2; \ldots; 0{,}03\right|$.

Обрахуємо для такого випадку матрицю $\mathrm{V^{I_1}}$ і відобразимо результати у вигляді табл. 3.

Таблиця 3 – Можливість появи інцидента

$PR_{lim}^{\mathrm{I_1}}$	0,25																					
$PR_{\mathrm{CA_j}}^{\mathrm{I_1}}$	0,1	0,2	0,1	0,25	0,2	0,1	0,02	0,05	0,1	0,3	0,04	0,4	0,01	0,1	0,28	0,1	0,05	0,05	0,3	0,05	0,5	0,03
	0	0	0	1	0	0	0	0	0	1	0	1	0	0	1	0	0	0	1	0	1	0

Таким чином $\mathrm{V^{I_1}} = \left|0\,0\,0\,1\,0 \ldots 1\,0\,1\,0\right|$, а $\left\|\mathrm{V^{I_1}}\right\| = 6$. Аналогічно здійснюються обрахунки для інших категорій інцидентів.

Етап 5 – Формування та встановлення правил екстраполяції інцидентів.

На цьому етапі, залежно від критичності ІТС (яка може, наприклад, відноситись (або не відноситись) до критичної інформаційної інфраструктури), обирається один з двох варіантів формування та встановлення правил екстраполяції інцидентів.

Варіант 1

Показник можливості появи інцидента V^{Ii} свідчить про появу інциденту лише в тому разі, якщо хоча б один з його елементів дорівнює не нулю (7), тобто потужність матриці $\left\|\mathrm{V}^{\mathrm{Ii}}\right\| > 0$.

Тоді евристичне правило для виявлення інцидента певної категорії матиме такий вигляд:

$$\mathrm{PR}_{\mathrm{v1}}^{\mathrm{Ii}} = \left\|\mathrm{V}^{\mathrm{Ii}}\right\| > 0 = \bigvee_{\mathrm{j=1}}^{\mathrm{m}} \left\|(PR_{\mathrm{CA_j}}^{I_{\mathrm{i}}} \geq PR_{lim}^{I_{\mathrm{i}}})\right\| > 0 \rightarrow I_n, \tag{8}$$

що можна інтерпретувати наступним чином: “якщо потужність матриці-показника можливості появи інцидента більша нуля, тобто хоча б одне значення імовірностей реалізації інцидента визначеного класу при проведення певної кібератаки більше за граничним значенням імовірності, то експерт впевнений у появі інциденту”.

Згідно умов дослідження для $\mathrm{I}_1 = \mathrm{MW}$ буде активовано наступне правило $PR_{\mathrm{V_1}}^{\mathrm{I_1}} = \left\|\mathrm{V}^{\mathrm{I_1}}\right\| > 0 = \overset{22}{\underset{\mathrm{j=1}}{\mathrm{V}}} \left\|PR_{\mathrm{CA_j}}^{\mathrm{I_1}} \geq PR_{\mathrm{lim}}^{\mathrm{I_1}}\right\| > 0 = \overset{22}{\underset{\mathrm{j=1}}{\mathrm{V}}} \left\|PR_{\mathrm{CA_j}}^{\mathrm{I_1}} > 0,25\right\| > 0 = 6 > 0 \rightarrow \mathrm{I}_1$, тобто враховуючи, що $\left\|\mathrm{V}^{\mathrm{I_1}}\right\| = 6$ експерт впевнений в можливості реалізацій інциденту.

Варіант 2

Залежно від потужності матриці V^{Ii} визначається можливість реалізації інцидента, що визначається лінгвістичною змінною:

$$\mathrm{LI}_{\mathrm{q}}^{\mathrm{I_n}} = \bigcup_{\mathrm{q=1}}^{4} \{LI_{\mathrm{q}}^{\mathrm{I_n}}\} = \{\text{низька}, \text{середня}, \text{висока}, \text{критична}\} = \{\mathrm{H}, \mathrm{C}, \mathrm{B}, \mathrm{K}\}. \tag{9}$$

Так, оскільки елементи матриці V^{Ii} приймають значення “0” або ”1”, то її максимальна потужність $\left\|\mathrm{V}^{\mathrm{Ii}}\right\| = 22$. Звідси сформуємо множину правил екстраполяції інцидентів певної категорії:

$$\begin{aligned}
&\mathrm{PR}_{\mathrm{v2}}^{\mathrm{Ii}} = \{\left\|\mathrm{V}^{\mathrm{Ii}}\right\| = 0,..,5 = \bigwedge_{\mathrm{j=1}}^{\mathrm{m}} \left\|(PR_{\mathrm{CA_j}}^{I_{\mathrm{i}}} \geq PR_{lim}^{I_{\mathrm{i}}})\right\| = 0,..,5 \rightarrow \mathrm{LI}_1^{\mathrm{I_n}},\\
&\left\|\mathrm{V}^{\mathrm{Ii}}\right\| = 6,..,9 = \bigwedge_{\mathrm{j=1}}^{\mathrm{m}} \left\|(PR_{\mathrm{CA_j}}^{I_{\mathrm{i}}} \geq PR_{lim}^{I_{\mathrm{i}}})\right\| = 6,..,9 \rightarrow \mathrm{LI}_2^{\mathrm{I_n}},\\
&\left\|\mathrm{V}^{\mathrm{Ii}}\right\| = 10,..,15 = \bigwedge_{\mathrm{j=1}}^{\mathrm{m}} \left\|(PR_{\mathrm{CA_j}}^{I_{\mathrm{i}}} \geq PR_{lim}^{I_{\mathrm{i}}})\right\| = 10,..,15 \rightarrow \mathrm{LI}_3^{\mathrm{I_n}},\\
&\left\|\mathrm{V}^{\mathrm{Ii}}\right\| > 15 = \bigwedge_{\mathrm{j=1}}^{\mathrm{m}} \left\|(PR_{\mathrm{CA_j}}^{I_{\mathrm{i}}} \geq PR_{lim}^{I_{\mathrm{i}}})\right\| > 15 \rightarrow \mathrm{LI}_4^{\mathrm{I_n}}\}.
\end{aligned} \tag{10}$$

Множину правил екстраполяції інцидентів можна інтерпретувати таким чином ”якщо потужність матриці-показника можливості появи інцидента від 0 до 5, тобто не більше 5 ймовірностей реалізації інцидента визначеного класу при проведення певної кібератаки більше за граничним значенням імовірності, то впевненість експерта в появі інциденту – низька, якщо потужність матриці-показника можливості появи інцидента від 6 до 9, тобто не більше 9, але й не менше 6 ймовірностей реалізації інцидента визначеного класу при проведення певної кібератаки більше за граничним значенням імовірності, то впевненість експерта в появі інциденту – середня, якщо потужність матриці-показника можливості появи інцидента від 10 до 15, тобто не більше 15, але й не менше 10 ймовірностей реалізації інцидента визначеного класу при проведення певної кібератаки більше за граничним значенням імовірності, то впевненість експерта в появі інциденту – висока, а якщо потужність матриці-показника можливості появи інцидента більше 15, тобто не менше 15 ймовірностей реалізації інцидента визначеного класу при проведення певної кібератаки більше за граничним значенням імовірності, то впевненість експерта в появі інциденту – критична”.

Наприклад, за зазначених умов дослідження для $I_1 = \text{MW}$ використаємо наступне правило:

$$\text{PR}^{I_1} = \{\left\|\text{V}^{I_1}\right\| = 0,..,5 = \underset{j=1}{\overset{22}{\wedge}}\left\|(PR^{I_1}_{\text{CA}_j} \geq PR^{I_1}_{lim})\right\| = \underset{j=1}{\overset{22}{\wedge}}\left\|(PR^{I_1}_{\text{CA}_j} \geq 0,25)\right\| = 0,..,5 \rightarrow \text{H},$$

$$\left\|\text{V}^{I_1}\right\| = 6,..,9 = \underset{j=1}{\overset{22}{\wedge}}\left\|(PR^{I_1}_{\text{CA}_j} \geq PR^{I_1}_{lim})\right\| = \underset{j=1}{\overset{22}{\wedge}}\left\|(PR^{I_1}_{\text{CA}_j} \geq 0,25)\right\| = 6,..,9 \rightarrow \text{C},$$

$$\left\|\text{V}^{I_1}\right\| = 10,..,15 = \underset{j=1}{\overset{22}{\wedge}}\left\|(PR^{I_1}_{\text{CA}_j} \geq PR^{I_1}_{lim})\right\| = \underset{j=1}{\overset{22}{\wedge}}\left\|(PR^{I_1}_{\text{CA}_j} \geq 0,25)\right\| = 10,..,15 \rightarrow \text{B},$$

$$\left\|\text{V}^{I_1}\right\| > 15 = \underset{j=1}{\overset{22}{\wedge}}\left\|(PR^{I_1}_{\text{CA}_j} \geq PR^{I_1}_{lim})\right\| = \underset{j=1}{\overset{22}{\wedge}}\left\|(PR^{I_1}_{\text{CA}_j} \geq 0,25)\right\| > 15 \rightarrow \text{K}\}.$$

Оскільки $\left\|\text{V}^{I_1}\right\| = 6$, то із заданої множини правил буде активовано правило (спрацює) $\left\|\text{V}^{I_1}\right\| = 6,..,9 = \underset{j=1}{\overset{22}{\wedge}}\left\|(PR^{I_1}_{\text{CA}_j} \geq 0,25)\right\| = 6 \rightarrow \text{C}$. Тобто в такому випадку експерт впевнений в "СЕРЕДНІЙ" можливості реалізації інциденту $I_1 = \text{MW}$.

Висновки. Таким чином, у цій роботі розроблено метод формування множини правил екстраполяції інцидентів для мережево-центричного моніторингу ІТС, який за рахунок визначення можливих типів кібератак та категорій інцидентів, формування вектор-матриць імовірностей реалізації інцидентів, ранжування інцидентів за їх важливістю та визначення граничних значень імовірностей, формування показників можливості появи інцидентів, а також формування та встановлення правил екстраполяції інцидентів, дозволяє автоматизувати і підвищити точність роботи систем мережево-центричного моніторингу ІТС. Створене на основі цього методу програмне забезпечення може використовуватись як модуль у складі засобів мережево-центричного моніторингу, а також як окремий інструментальний засіб команд реагування на інциденти типу CERT / CSIRT.

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

[1] В.О. Гнатюк, "Аналіз дефініцій поняття "інцидент" та його інтерпретація у кіберпросторі", *Безпека інформації*, том 19, № 3. с. 175-180, 2013. doi: 10.18372/2225-5036.19.5620.

[2] S. Hnatiuk, V. Hnatiuk, V. Kononovich, and I. Kononovich, "Transformation of Information and Social-Psychological Security Paradigms (Part 1)", *Informatics and Mathematical Methods in Simulation.* vol. 6, iss. 3, pp. 227-239, 2016.

[3] International Organization for Standardization. (2011, Aug. 17). *ISO/IEC 27035, Information technology. Security techniques. Information security incident management*. [Online]. Available: https://www.iso.org/standard/44379.html. Accessed on: Aug., 28, 2016.

[4] С.О. Гнатюк, Ю.Є. Хохлачова, А.О. Охріменко, та А.К. Гребенькова, "Теоретичні основи побудови та функціонування систем управління інцидентами інформаційної безпеки", *Захист інформації*, том 14, № 1, с. 121-126, 2012. doi: 10.18372/2410-7840.14.2073.

[5] A. Hizun, V. Hnatyuk, N. Balyk, and P. Falat, "Approaches to Improve the Activity of Computer Incident Response Teams", in *Proc. 8th International conference. Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2015)*, Warsaw, Poland, September 2015, vol. 1, pp. 442-447. doi: 10.1109/IDAACS.2015.7340775.

[6] О.Г. Корченко, В.О. Гнатюк, Є.В. Іванченко, С.О. Гнатюк, та Н.А. Сєйлова, "Метод мережево-центричного моніторингу кіберінцидентів в сучасних інформаційно-телекомунікаційних системах", *Захист інформації*, том 18, № 3, с. 229-247, 2016. doi: 10.18372/2410-7840.18.10852.

[7] А.І. Гізун, В.О. Гнатюк, та О.М. Супрун, "Формалізована модель побудови евристичних правил для виявлення інцидентів", *Вісник Інженерної академії України*, № 1, с. 110-115, 2015.

[8] А.О. Корченко, А.І. Гізун, В.В. Волянська, та О.В. Гавриленко, "Евристичні правила на основі логіко-лінгвістичних зв'язок для виявлення та ідентифікації порушника інформаційної безпеки", *Захист інформації*, том 15, № 3, с. 251-257, 2013. doi: 10.18372/2410-7840.15.4862.

[9] KDD CUP99 [Online]. Available: https://kdd.ics.uci.edu/databases/kddcup99/task.html. Accessed on: Aug., 28, 2016.

[10] А.Г. Корченко, *Построение систем защиты информации на нечетких множествах: Теория и практические решения*. Київ, Україна: МК-Пресс, 2006.

[11] V.A. Olutayo, and A.A. Eludire, "Traffic Accident Analysis Using Decision Trees and Neural Networks", *International Journal of Information Technology and Computer Science (IJITCS)*, vol. 6, № 2, pp. 22-28, 2014. doi: 10.5815/ijitcs.2014.02.03.

[12] А.О. Корченко, В.А. Козачок, та А.І. Гізун, "Метод оцінки рівня критичності для систем управління кризовими ситуаціями", *Захист інформації*, том 17, № 1, с. 86-98, 2015. doi: 10.18372/2410-7840.17.8349.

[13] K.K. Sindhu, B.B. Meshram, "Digital Forensic Investigation Tools and Procedures", *International Journal of Computer Network and Information Security (IJCNIS)*, vol. 4, № 4, pp. 39-48, 2012. doi: 10.5815/ijcnis.2012.04.05

Стаття надійшла до редакції 18 вересня 2016 року.

REFERENCES

[1] V.O. Hnatiuk, "Analysis of «incident» definitions and its interpretation in cyberspace", *Bezpeka ìnformacìì*, vol. 19, iss. 3. pp. 175-180, 2013. doi: 10.18372/2225-5036.19.5620.

[2] S. Hnatiuk, V. Hnatiuk, V. Kononovich, and I. Kononovich, "Transformation of Information and Social-Psychological Security Paradigms (Part 1)", *Informatics and Mathematical Methods in Simulation.* vol. 6, iss. 3, pp. 227-239, 2016.

[3] International Organization for Standardization. (2011, Aug. 17). *ISO/IEC 27035, Information technology. Security techniques. Information security incident management*. [Online]. Available: https://www.iso.org/standard/44379.html. Accessed on: Aug., 28, 2016.

[4] S.O. Hnatiuk, Yu.Ye. Khokhlachova, A.O. Okhrimenko, and A.K. Hrebenkova, "The theoretical basis of construction and operation of information security incident management systems", *Zahist ìnformacìï*, vol. 14, iss. 1, pp. 121-126, 2012. doi: 10.18372/2410-7840.14.2073.

[5] A. Hizun, V. Hnatyuk, N. Balyk, and P. Falat, "Approaches to Improve the Activity of Computer Incident Response Teams", in *Proc. 8th International conference. Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2015)*, Warsaw, Poland, September 2015, vol. 1, pp. 442-447. doi: 10.1109/IDAACS.2015.7340775.

[6] O.H. Korchenko, V.O. Hnatiuk, Ye.V. Ivanchenko, S.O. Hnatiuk, and N.A. Sieilova, "Method for cyberincidents network-centric monitoring in modern information & communication systems", *Zahist ìnformacìï*, vol. 18, iss. 3, pp. 229-247, 2016. doi: 10.18372/2410-7840.18.10852.

[7] A.I. Hizun, V.O. Hnatiuk, and O.M. Suprun, "Formalized model of construction heuristic rules to identify incidents", *Journal of Engineering Academy of Ukraine*, no. 1, pp. 110-115, 2015.

[8] A.O. Korchenko, A.I. Hizun, V.V. Volianska, and O.V. Havrylenko, "Heuristic rules based on logical & linguistic connection to detect and identify information security intruders", *Zahist ìnformacìï*, vol. 15, iss. 3, pp. 251-257, 2013. doi: 10.18372/2410-7840.15.4862.

[9] KDD CUP99 [Online]. Available: https://kdd.ics.uci.edu/databases/kddcup99/task.html. Accessed on: Aug., 28, 2016.
[10] A.H. Korchenko, *Construction of information security systems on fuzzy sets. Theory and practical solutions.* Kyiv, Ukraine: MK-Press, 2006.
[11] V.A. Olutayo, and A.A. Eludire, "Traffic Accident Analysis Using Decision Trees and Neural Networks", *International Journal of Information Technology and Computer Science (IJITCS)*, vol. 6, № 2, pp. 22-28, 2014.
doi: 10.5815/ijitcs.2014.02.03.
[12] A.O. Korchenko, V.A. Kozachok, and A.I. Hizun, "Method of criticality level assessment for crisis management systems", *Zahist ìnformacìï*, vol. 17, iss. 1, pp. 86-98, 2015.
doi: 10.18372/2410-7840.17.8349.
[13] K.K. Sindhu, B.B. Meshram, "Digital Forensic Investigation Tools and Procedures", *International Journal of Computer Network and Information Security (IJCNIS)*, vol. 4, № 4, pp. 39-48, 2012.
doi: 10.5815/ijcnis.2012.04.05.

ПЕТР ПАВЛЕНКО,
НИКОЛАЙ ВИНОГРАДОВ,
СЕРГЕЙ ГНАТЮК,
АНДРЕЙ ГИЗУН,
ВИКТОР ГНАТЮК

МЕТОД ФОРМИРОВАНИЯ ПРАВИЛ ЭКСТРАПОЛЯЦИИ ИНЦИДЕНТОВ ДЛЯ СЕТЕЦЕНТРИСТСКОГО МОНИТОРИНГА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Инциденты могут нарушить штатный режим функционирования информационно-телекоммуникационной системы и привести к значительным материальным и имиджевым убыткам предприятия. Одним из подходов к инцидент-менеджменту является применение сетецентрической теории управления для мониторинга инцидентов, однако недостаточно формализованным является этап формирования множеств базовых правил. Учитывая это, в работе разработан метод формирования множеств правил экстраполяции инцидентов для сетецентрического мониторинга информационно-телекоммуникационных систем, который за счет определения возможных типов кибератак и категорий инцидентов, формирования вектор-матриц вероятностей реализации инцидентов, ранжирования инцидентов по их важности и определение предельных значений вероятностей, формирования показателей возможности появления инцидентов, а также формирования и установления правил экстраполяции инцидентов, позволяет автоматизировать и повысить точность работы систем сетецентрического мониторинга информационно-телекоммуникационных систем.

Ключевые слова: инцидент, сетецентрический мониторинг, информационная безопасность, кибератака, информационно-телекоммуникационная система.

PETRO PAVLENKO,
MYKOLA VINOHRADOV,
SERHII HNATIUK,
ANDRII HIZUN,
VIKTOR HNATIUK

METHOD FOR RULES FORMING OF INCIDENTS EXTRAPOLATION FOR NETWORK-CENTRIC INFORMATION AND TELECOMMUNICATION SYSTEMS MONITORING

Security incidents and effective response have become an important component of information and telecommunication standards and guidances. Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires

substantial planning and resources. Incidents can disrupt regular mode of information and telecommunication systems functioning and cause substantial material and image losses for the company. The main task of incident management is consequense impact containment, quick response and backslide prevention. One of the modern approaches in incident management is usage of network-centric (continuously-evolving, complex community of people, devices, information and services interconnected by a communications network to achieve optimal benefit of resources and better synchronization of events and their consequences) management theory for incidents monitoring. Known method of network-centric incident management provides some advantages in influence forecasting, criticality evaluation and prioritizing. This method combines a set of stages but stage of forming basic rules set is not formalized. In this regard, in this work developed method for forming rule set of incidents extrapolation for network-centric information and telecommunication systems monitoring, which by determining possible types of cyberattacks and incidents categories, forming vector-matrix of incidents probability, incidents ranging by their importance and determining limit values of probability, forming incidents possibility indicators, and also development and establishment of incidents extrapolation rules, allows to automate and increase accuracy operation of network-centric systems for information and telecommunication systems monitoring.

Keywords: incident, network-centric monitoring, information security, cyberattack, information and telecommunication system.

Петро Миколайович Павленко, доктор технічних наук, професор, професор кафедри засобів захисту інформації, Національний авіаційний університет, Київ, Україна.
E-mail: petrpav@nau.edu.ua.
Микола Анатолійович Віноградов, доктор технічних наук, професор, професор кафедри комп'ютерних інформаційних технологій, Національний авіаційний університет, Київ, Україна.
E-mail: vl43@yandex.ru.
Сергій Олександрович Гнатюк, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій, Національний авіаційний університет, Київ, Україна.
E-mail: s.gnatyuk@nau.edu.ua.
Андрій Іванович Гізун, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій, Національний авіаційний університет, Київ, Україна.
E-mail: caesar07@meta.ua.
Віктор Олександрович Гнатюк, асистент кафедри телекомунікаційних систем, Національний авіаційний університет, Київ, Україна.
E-mail: viktorgnatyuk@ukr.net.

Петр Николаевич Павленко, доктор технических наук, профессор, профессор кафедры средств защиты информации, Национальный авиационный университет, Киев, Украина.
Николай Анатольевич Виноградов, доктор технических наук, профессор, профессор кафедры компьютерных информационных технологий, Национальный авиационный университет, Киев, Украина.
Гнатюк Сергей Александрович, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий, Национальный авиационный университет, Киев, Украина.
Гизун Андрей Иванович, кандидат технических наук, доцент кафедры безопасности информационных технологий, Национальный авиационный университет, Киев, Украина.
Гнатюк Виктор Александрович, ассистент кафедры телекоммуникационных систем, Национальный авиационный университет, Киев, Украина.

Petro Pavlenko, doctor of technical science, professor, professor at information security means academic department, National aviation university, Kyiv, Ukraine.

Mykola Vinohradov, doctor of technical science, professor, professor at computer information technologies academic department, National aviation university, Kyiv, Ukraine.

Serhii Hnatiuk, candidate of technical sciences, associate professor, associate professor of IT-Security academic departament, National aviation university, Kyiv, Ukraine.

Andrii Hizun, candidate of technical sciences, associate professor of IT-security academic departament, National aviation university, Kyiv, Ukraine.

Viktor Hnatiuk, assistant of telecommunication systems academic departament, National aviation university, Kyiv, Ukraine.

УДК 006.034:658.562.4

ЮЛІЯ КОЖЕДУБ,
ТЕТЯНА ЛІСНІЧЕНКО

ЗБІР, ОБРОБКА, ЗАСТОСУВАННЯ ТА ЗАХИСТ ІНФОРМАЦІЇ В ДОКУМЕНТАХ ВИСОКОЇ СОЦІАЛЬНОЇ ЗНАЧИМОСТІ

У статті розглянуто актуальне питання щодо збору, обробки, застосування та захисту інформації, що міститься у нормативно-правових актах і нормативних документах, використовуваних у сферах діяльності, що відповідають соціально важливим сферам промисловості й сфери послуг, зокрема, це проаналізовано на прикладах, що відповідають проектуванню й будівництву автомобільних доріг загального користування. Визначено, що первинні дані, отримані з практичного досвіду спеціалістів, фахівців, зокрема проектувальників та будівельників автомобільних доріг, перетворено у параметри, характеристики, які покладено в основу, створюваних документів для забезпечення безпеки, серед іншого й користування автомобільними дорогами й прилеглою до них інфраструктурою. Проаналізовано потенційну потребу у застосуванні інформації, що її використано для створення нормативно-правових актів та нормативних документів. Визначено переліки кількісних даних і відповідні статистичні методи, наведені в стандартах, для застосування організаціями, що упровадили системи управління для підтвердження дієвості управління. Висвітлено сферу застосування найвідоміших статистичних методів для оброблення кількісних даних сучасних нормативно-правових і нормативних документів для подальшого їх використання. Встановлено, що беззаперечне дотримання числових значень параметрів і характеристик є запорукою створення безпеки у соціально важливих сферах діяльності людини. Викладено результати дослідження та перспективи подальших пошуків у цьому напрямі.

Ключові слова: інформація, кількісні дані, нормативний документ, нормативно-правовий акт, статистичні методи.

Постановка проблеми. Наявність інформації та потреба її використовувати складають основу не лише повсякденного життя людей і їх спілкування на побутовому рівні. Задіяність інформації, зокрема опрацювання наявних кількісних даних, потрібно, насамперед, у виробничий сфері під час виконання суспільно-корисної праці, у сфері побуту, а тому питання регулювання інформаційних відносин щодо створення, збирання, одержання, зберігання, використання, поширення, охорони й захисту інформації є важливою частиною різних сфер діяльності людини й стосується питань життєво необхідних для буття людини. Є певні соціально значимі сфери діяльності людини, що стосуються безпекових питань, і тому вважаємо, що питання дотримання вимог нормативно-правових актів та нормативних