© Vinogradov M., Ivanchenko Ye., Gnatyuk V. Method for efficiency assessment of cyberincidents processing by CSIRT // Ukrainian Scientific Journal of Information Security, 2017, vol. 23, issue 1, p. 56-62.

DOI: 10.18372/2225-5036.23.11580

МЕТОД ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ОБРОБКИ КІБЕРІНЦИДЕНТІВ ЦЕНТРАМИ CSIRT

Микола Віноградов, Євгенія Іванченко, Віктор Гнатюк

Національний авіаційний університет, Україна

ВІНОГРАДОВ Микола Анатолійович, д.т.н.

Рік та місце народження: 1946 рік, м. Київ, Україна.
Освіта: Київське вище інженерно авіаційне військове училище ВПС, 1969 рік.
Посада: професор кафедри комп'ютерних інформаційних технологій з 2007 року.
Наукові інтереси: інформаційна та авіаційна безпека, методи і моделі систем виявлення кібертерористичних атак.
Публікації: більше 80 наукових публікацій, серед яких монографії, наукові статті у вітчизняних та міжнародних фахових виданнях, матеріали і тези доповідей конференцій.
E-mail: icaocentre@nau.edu.ua

ІВАНЧЕНКО Євгенія Вікторівна, к.т.н.

Рік та місце народження: 1976 рік, м. Київ, Україна.
Освіта: Київський міжнародний університет цивільної авіації, 2000 рік.
Посада: професор кафедри безпеки інформаційних технологій з 2007 року.
Наукові інтереси: інформаційна та авіаційна безпека, методи і моделі систем виявлення кібертерористичних атак.
Публікації: більше 70 наукових публікацій, серед яких наукові та навчально-методичні праці, монографії, наукові статті у вітчизняних та міжнародних фахових виданнях, матеріали і тези доповідей конференцій, патенти.
E-mail: icaocentre@nau.edu.ua

ГНАТЮК Віктор Олександрович

Рік та місце народження: 1990 рік, м. Нетішин, Хмельницька область, Україна.
Освіта: Хмельницький національний університет, 2012 рік.
Посада: асистент кафедри телекомунікаційних систем з 2015 року.
Наукові інтереси: інформаційна безпека, управління інцидентами інформаційної безпеки.
Публікації: більше 20 наукових публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях, авторські свідоцтва.
E-mail: viktorgnatyuk@ukr.net

Анотація. *Обробка та управління кіберінцидентами – важливі завдання, розв'язанням яких займаються спеціалізовані центри типу CSIRT. Проте на сьогодні відсутні механізми оцінювання їх роботи. З огляду на це, у роботі пронаналізовано сучасні методи оцінювання роботи персоналу, проведено їх багатокритеріальний аналіз. Опираючись на результати аналізу, розроблено метод оцінювання ефективності обробки кіберінцидентів центрами CSIRT, який за рахунок визначення показників функціонування CSIRT, виділення серед них ключових показників ефективності використовуючи багаточинниковий кореляційно-регресійний аналіз, побудови панелі індикаторів, візуалізації залежності ключових показників ефективності та ефективності, дає можливість проводити аудит діяльності CSIRT та інших центрів технічного обслуговування інформаційно-телекомунікаційних систем. Цей метод та сформовані на його основі засоби будуть корисними керівникам центрів реагування на кіберінциденти для моніторингу, аналізу, оцінки та управління ефективністю роботи CSIRT. Розроблений метод можна застосувати в будь-якій компанії або державній установі з метою підвищення як рівня інформаційної безпеки, так і ефективності роботи працівника, відділу та організації в цілому.*

Ключові слова: *ключові показники ефективності, кіберінцидент, CSIRT, кореляційна матриця, панель індикаторів.*

Вступ

Сьогодні інформаційна безпеки особи, суспільства і держави є однією з головних складових національної безпеки в цілому, так як інформаційно-комунікаційні технології широко використовуються в усіх сферах життя. Проблема інформаційної безпеки не втрачає своєї актуальності в сучасному світі, а навпаки, починає носити глобальний характер – інциденти інформаційної безпеки (кіберінциденти) [5] стають все більш складними й частими. Реагуванням на кіберінциденти, як правило, займаються спеціалізовані центри (команди) типу CSIRT (Computer Security Incident Response Team), які з кожним роком отримують все більше завдань та викликів. Саме через це з'являється необхідність аналізувати та оцінювати ефективність роботи CSIRT – даний чинник, є одним з ключових для інформаційної безпеки як окремої організації, так і держави в цілому. Періодичне (щомісячне, щоквартальне тощо) оцінювання роботи цих центрів дозволить ідентифікувати сильні та слабкі сервіси, відділи, групи, окремих співробітників з метою врахування у майбутньому, а також виокремити певні тенденції на базі статистичних даних. Проведений аналіз показав, що оцінці ефективності роботи CSIRT не відводиться достатньо уваги, а це може негативно вплинути на рівень інформаційної безпеки.

Аналіз досліджень і публікацій

У вітчизняній та зарубіжній науково-технічній літературі описана велика кількість методів оцінки роботи персоналу [16], проте характерними для них є не комплексність, еклектичний підхід, коли результати оцінки здобувають з допомогою конгломерату не пов'язаних між собою оцінювальних методів; брак систематичності та регулярності у застосуванні процедур оцінювання, орієнтація на спрощені процедури оцінки, брак конструктивного зворотного зв'язку між об'єктом і суб'єктами оцінювання тощо.

Проведено аналіз сучасних методів оцінки роботи персоналу [2, 4, 6, 8, 12, 15, 16] за такими критеріями: врахування особистісних якостей окремого працівника (PF), врахування результатів діяльності окремого працівника (PR), врахування результатів діяльності групи працівників (PG), самодостатність методу (SS), потреба в значних часових витратах на обробку результатів (TS), складність у застосуванні (DA), якісна оцінка (QA), кількісна оцінка (Q), висока вартість застосування (HC), об'єктивність оцінки (OE). Результати проведеного аналізу відображені у табл. 1, де «+» означає повну відповідність критерію, «-» – не відповідність, а «+/-» – часткову відповідність.

Багатокритеріальний аналіз методів оцінки роботи персоналу Таблиця 1

№	Назва методу	Базові критерії									
		PF	PR	PG	SS	TS	DA	QA	Q	HC	OE
1.	Описовий	+	-	-	-	+/-	-	+	-	-	-
2.	Класифікації	+	+	-	+/-	+/-	-	+	-	-	-
3.	Оцінки нормативом роботи	+/-	+	-	+/-	+/-	+/-	+	+	-	+
4.	Моделювання ситуації	+	-	-	+/-	+/-	+/-	+	-	-	-
5.	Порівняльних анкет	+	+/-	-	+/-	-	-	+	-	-	-
6.	Тестування	+	+	-	+/-	-	-	+	+	-	-
7.	Порівняння	+	+	-	+/-	-	-	+	-	-	-
8.	Алфавітно-числової шкали	+	+	-	+/-	-	-	+	-	-	-
9.	Інтерв'ю	+	-	-	+/-	+/-	-	+	-	-	-
10.	Комітетів	+	+	-	+/-	-	-	+	-	-	+/-
11.	360 градусів	+	+	-	+/-	+/-	-	+	-	-	+/-
12.	Незалежних сусідів	+/-	+/-	-	+/-	+/-	-	+	+/-	-	-
13.	«Центр оцінки»	+	+/-	-	+	+	+/-	+	+/-	+	+
14.	Ділових ігор	+	-	+	+/-	-	-	+	-	-	-
15.	Управління за цілями	+/-	+	+/-	+/-	+/-	-	+	+/-	-	+/-
16.	Управління досягненнями	+	+	+	+	+/-	+/-	+	+	-	+
17.	Стандартних оцінок	+	+/-	-	+/-	-	-	+	-	-	-
18.	Вирішальних ситуацій	+	-	-	+/-	-	-	+	-	+	-
19.	Рейтингових поведінкових установок	+	-	-	+/-	+	+/-	+	-	+	-
20.	Шкали спостереження за поведінкою	+	-	-	+/-	+	+/-	+	-	+	-
21.	Заданого розподілу	+	-	-	-	-	-	+	-	-	+/-

Проаналізувавши існуючі методи оцінки роботи персоналу (табл.1) можна зробити висновок, що: переважна їх більшість спрямована на оцінку особистісних якостей працівника, вони є самодостатніми, близько половини з розглянутих методів враховують результати діяльності окремого працівника та для всіх є характерним якісна оцінка. Також, слід відмітити, що лише декілька методів дають можливість оцінити роботу групи працівників.

З огляду на результати аналізу (табл. 1), найбільш ефективним методом оцінювання роботи персоналу є метод управління досягненнями (Performance Management), що являє собою концепцію управління організацією, яка базується на низці теорій та практик управління. Обраний ме-

тод базується на принципах в яких досягнення цілей співробітниками оцінюється за допомогою показників (Key Performance Indicators — KPI). Ключові показники ефективності – система оцінок, яка застосовується при вирішенні стратегічних і тактичних завдань, що виникають в складних технічних системах [1, 11, 14]. Використання ключових показників ефективності дає можливість оцінити стан і допомогти в оцінці реалізації методів управління. Для терміну KPI найчастіше використовується переклад «ключові показники ефективності» (КПЕ), проте це не зовсім вірно [11]. Справа в тому, що слово «performance» має багато трактувань. Правильне формулювання можна знайти в стандарті ISO 9000: 2008. Він розділяє слово «performance» на два терміни: результативність і ефективність. За стандартом, результативність – це ступінь досягнення запланованих результатів (здатність системи орієнтуватися на результат), а ефективність – співвідношення між досягнутими результатами і витраченими ресурсами (здатність системи до реалізації своїх цілей і планів із заданим якісним рівнем, вираженим певними вимогами – часом, витратами, ступенем досягнення мети). Слово «performance» об'єднує в собі і результативність, і ефективність. Таким чином, правильним перекладом терміна KPI був би «ключовий показник результатів функціонування», так як результат функціонування містить в собі і ступінь досягнення, і витрати на отримання результату [11]. Тому, надалі у цій роботі будемо дотри-муватися такого трактування терміну KPI.

Метою роботи є розробка методу оцінювання ефективності обробки кіберінцидентів центрами CSIRT, який дасть можливість проводити аудит діяльності CSIRT та інших центрів технічного обслуговування інформаційно-телекомунікаційних систем.

Основна частина дослідження

Розроблений метод складається з таких етапів: визначення показників функціонування CSIRT, визначення ключових показників ефективності роботи CSIRT, побудова панелі індикаторів та візуалізація залежності *KPI* та *E*.

Етап 1 – Визначення показників функціонування CSIRT. При функціонуванні CSIRT здійснюється запис до бази даних (БД) інформації про кіберінциденти. Серед базових показників функціонування CSIRT [3, 7], що мають кількісні значення варто виділити наступні (табл. 2).

Показники функціонування CSIRT Таблиця 2

Позначення	Назва
E	Ефективність
LRI	Рівень вирішення інциденту
INAI	Кількість некоректних призначень інциденту
DRI	Тривалість вирішення інциденту
ECS	Оцінка задоволеності клієнтів
PRI	Пріоритет інциденту
DIR	Тривалість реєстрації інциденту
CII	Повнота наданої інформації про інцидент

Для реалізації цього етапу задамо множину показників функціонування CSIRT $\boldsymbol{PI}$:

$$\boldsymbol{PI} = \{\bigcup_{q=1}^{p} PI_q\} = \{PI_1,\ PI_2,...,PI_p\}, \quad (1)$$

де $PI_q \subseteq \boldsymbol{PI}$, $(q = \overline{1, p})$, p – кількість показників функціонування CSIRT.

Для перевірки адекватності методу будемо розглядати різні варіанти вхідних даних для кожного з етапів (статистика кіберінцидентів за II та III квартал 2016 року відповідно).

Варіант 1

Наприклад, використовуючи БД з показниками функціонування CSIRT вітчизняного оператора стільникового зв'язку (за II квартал 2016 року) сформуємо табл. 3.

Значення показників діяльності CSIRT за II квартал 2016 р. Таблиця 3

№	E	LRI	INAI	DRI	ECS	PRI	DIR	CII
1	90	4	3	1539	4	3	2	40
2	115	1	0	2502	8	4	6	80
…	…	…	…	…	…	…	…	…
600	171	1	0	37	6	1	6	85

Використовуючи (1) та дані з табл. 2 при $p = 8$, отримаємо:

$$\boldsymbol{PI}_{celprov\_ua2} = \{\bigcup_{q=1}^{8} PI_q\} = \{PI_1,\ PI_2,...,PI_8\} =$$

$$\{PI_E,\ PI_{LRI}, PI_{INAI}, PI_{DRI}, PI_{ECS}, PI_{PRI}, PI_{DIR}, PI_{CII}\} =$$

$$\{E,\ LRI, INAI, DRI, ECS, PRI, DIR, CII\},$$

де $PI_1 = PI_E = E$, $PI_2 = PI_{LRI} = LRI$,…, $PI_8 = PI_{CII} = CII$ – показники функціонування CSIRT.

На виході цього етапу маємо матрицю з показниками функціонування CSIRT та їх значеннями, які беремо з табл. 3.

Варіант 2

Наприклад, використовуючи БД з показниками функціонування CSIRT вітчизняного оператора стільникового зв'язку (за III квартал 2016 року) сформуємо табл. 4.

Значення показників діяльності CSIRT за III квартал 2016 р. Таблиця 4

№	E	LRI	INAI	DRI	ECS	PRI	DIR	CII
1	109	1	0	55	5	1	5	70
2	86	4	2	560	4	2	4	60
…	…	…	…	…	…	…	…	…
600	150	1	0	40	8	1	4	60

Використовуючи (1) та дані з табл. 2 при $p = 8$, отримаємо:

$$\boldsymbol{PI}_{celprov\_ua3} = \{\bigcup_{q=1}^{8} PI_q\} = \{PI_1,\ PI_2,...,PI_8\} =$$

$$\{PI_E,\ PI_{LRI}, PI_{INAI}, PI_{DRI}, PI_{ECS}, PI_{PRI}, PI_{DIR}, PI_{CII}\} =$$

$$\{E,\ LRI, INAI, DRI, ECS, PRI, DIR, CII\},$$

де $PI_1 = PI_E = E$, $PI_2 = PI_{LRI} = LRI$,…, $PI_8 = PI_{CII} = CII$ – показники функціонування CSIRT.

За аналогією, на виході цього етапу маємо матрицю з показниками функціонування CSIRT та їх значеннями, які беремо з табл. 4.

Етап 2 – Визначення ключових показників ефективності роботи CSIRT. Щоб визначити з множини показників функціонування CSIRT *PI* ключові показники ефективності *KPI* використаємо процедуру множинного кореляційно-регресійного аналізу [9], яка включає наступні кроки:

Крок 1. Вибір всіх можливих чинників (обираються чинники, які впливають на показник (або процес), що досліджується, якщо деякі чинники неможливо кількісно чи якісно визначити або для них недоступна статистика, то їх вилучають з подальшого розгляду).

Крок 2. Вибір вигляду регресійної чи багаточинникової моделі (знаходження аналітичного виразу, який найкраще відображував би зв'язок чинникових ознак з результативною).

Крок 3. Перевірка адекватності отриманої моделі (розрахунок: розбіжності між спостереженими та розрахунковими значеннями; відносної похибки між спостереженими та розрахунковими значеннями; середньоквадратичної помилки дисперсії збурень; коефіцієнта детермінації; коефіцієнта множинної кореляції).

Крок 4. Перевірка адекватності моделі за допомогою статистики Фішера (критичне значення знаходиться за таблицями Фішера).

Крок 5. Перевірка значущості коефіцієнтів рівняння регресії (перевірка здійснюється за допомогою t-статистики).

Крок 6. Обчислення коефіцієнта еластичності (для усунення відмінностей в одиницях вимірювання чинників використаємо часткові коефіцієнти еластичності).

Крок 7. Визначення довірчих інтервалів для параметрів регресії (довірчий інтервал при рівні надійності (1-α) є інтервал з випадково визначеними межами, що з рівнем довіри (1-α) накриває істинне значення коефіцієнта рівняння регресії).

Нехай маємо m випадкових величин $x_1, x_2, \ldots, x_i, \ldots, x_m$ (параметрів, що досліджуються) представлених вибірками по n значень $x_i = \{x_{i1}, x_{i2}, \ldots, x_{ik}, \ldots, x_{in}\}$. Для кожної пари випадкових величин x_i та x_j по рівнянню можна оцінити значення емпіричного коефіцієнта лінійної кореляції r_{ij}. Отримані значення коефіцієнтів записуються в матрицю розміром $m \times m$:

$$\begin{pmatrix} 1 & r_{12} & \ldots & r_{1j} & \ldots & r_{1m} \\ r_{21} & 1 & \ldots & r_{2j} & \ldots & r_{2m} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ r_{i1} & r_{i2} & \ldots & 1 & \ldots & r_{im} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ r_{m1} & r_{m2} & \ldots & r_{mj} & \ldots & 1 \end{pmatrix}.$$

Всі значення коефіцієнта кореляції r належать інтервалу від -1 до 1. Знак коефіцієнта показує «напрямок» зв'язку: додатне значення свідчить про «прямий» зв'язок, від'ємне значення – про «зворотний» зв'язок, а значення «0» – про відсутність лінійного кореляційного зв'язку. При r =1 або r =-1 маємо функціональний зв'язок між ознаками. Множинний коефіцієнт кореляції є основною характеристикою тісноти взаємозв'язку між результативною ознакою PI_1 та сукупністю чинникових ознак $PI_2, PI_3, ..., PI_p$. При оцінюванні сили зв'язку використовується шкала Чеддока [13].

Отже, за допомогою наведеної розрахункової процедури множинного кореляційно-регресійного аналізу можна оцінити міру впливу на досліджуваний результативний показник (PI_1) кожного із введених у модель чинників ($PI_2, PI_3, ..., PI_p$) та визначити множину ключових показників ефективності ***KPI*** :

$$\boldsymbol{KPI} = \{\bigcup_{w=1}^{v} KPI_w\} = \{KPI_1, KPI_2, ..., KPI_v\}, \qquad (2)$$

де $KPI_w \subseteq \boldsymbol{KPI}$, $(w = \overline{1,v})$, v – кількість ключових показників ефективності.

Варіант 1

Наприклад, на вхід цього етапу подаємо матрицю з показниками функціонування CSIRT та їх значеннями (табл. 3). Далі, застосовуючи вищеописану процедуру множинного кореляційно-регресійного аналізу отримуємо кореляційну матрицю (табл. 5).

Кореляційна матриця для II кварталу 2016 року Таблиця 5

E	1							
LRI	-0,37	1						
INAI	-0,79	0,35	1					
DRI	-0,49	0,36	0,66	1				
ECS	0,82	-0,47	-0,57	-0,51	1			
PRI	-0,91	0,57	0,47	0,67	-0,63	1		
DIR	0,19	-0,52	-0,52	-0,63	0,43	-0,60	1	
CII	0,89	-0,62	-0,52	-0,45	0,72	-0,58	0,29	1
	E	LRI	INAI	DRI	ECS	PRI	DIR	CII

Аналізуючи дані з табл. 5 та використовуючи шкалу Чеддока, можна зробити висновок, що найбільш впливають на ефективність такі чинники: пріоритет інциденту (PRI), кількість некоректних призначень інциденту (INAI), оцінка задоволеності клієнтів (ECS) та повнота наданої інформації про інцидент (CII).

На виході цього етапу, згідно (2), при $w = 4$ отримуємо множину ключових показників ефективності ***KPI*** :

$$\boldsymbol{KPI}_{\boldsymbol{CSIRT\,2Q}} = \{\bigcup_{w=1}^{4} KPI_w\} = \{KPI_1, KPI_2, KPI_3, KPI_4\} =$$

$$\{KPI_{PRI}, KPI_{INAI}, KPI_{ECS}, KPI_{CII}\} = \{PRI, INAI, ECS, CII\},$$

де $KPI_1 = KPI_{PRI} = PRI$, $KPI_2 = KPI_{INAI} = INAI$, $KPI_3 = KPI_{ECS} = ECS$ та $KPI_4 = KPI_{CII} = CII$ – ключові показники ефективності: пріоритет інциденту, кількість некоректних призначень інциденту, оцінка задоволеності клієнтів та повнота наданої інформації про інцидент відповідно.

Варіант 2

Аналогічно, для прикладу, на вхід цього етапу подаємо матрицю з показниками функціонування CSIRT та їх значеннями (табл. 4). Далі, застосовуючи вищеописану процедуру множинного кореляційно-регресійного аналізу отримуємо кореляційну матрицю (табл. 6).

Кореляційна матриця для ІІІ кварталу 2016 року Таблиця 6

E	1							
LRI	-0,35	1						
INAI	-0,83	0,43	1					
DRI	-0,43	0,38	0,62	1				
ECS	0,64	-0,57	-0,52	-0,41	1			
PRI	-0,89	0,53	0,43	0,57	-0,53	1		
DIR	0,23	-0,47	-0,56	-0,53	0,53	-0,45	1	
CII	0,81	-0,54	-0,55	-0,55	0,62	-0,39	0,34	1
	E	LRI	INAI	DRI	ECS	PRI	DIR	CII

Аналізуючи дані з табл. 6 та використовуючи шкалу Чеддока, можна зробити висновок, що найбільш впливають на ефективність такі чинники: пріоритет інциденту (PRI), кількість некоректних призначень інциденту (INAI), повнота наданої інформації про інцидент (CII).

На виході цього етапу, згідно (2), при $w=3$ отримуємо множину ключових показників ефективності ***KPI*** :

$$\boldsymbol{KPI}_{\boldsymbol{CSIRT\,3Q}} = \{\bigcup_{w=1}^{3} KPI_w\} = \{KPI_1, KPI_2, KPI_3\} =$$

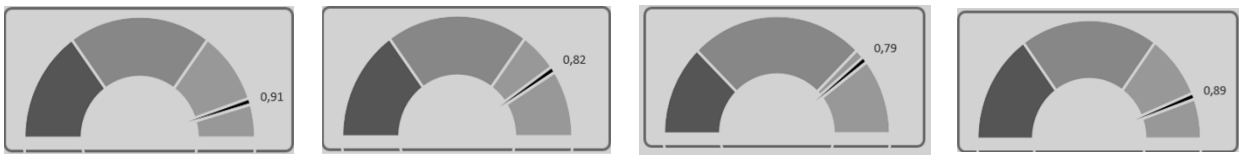
$$\{KPI_{PRI},\ KPI_{INAI}, KPI_{CII}\} = \{PRI,\ INAI, CII\},$$

де $KPI_1 = KPI_{PRI} = PRI$, $KPI_2 = KPI_{INAI} = INAI$, $KPI_3 = KPI_{CII} = CII$ – ключові показники ефективності: пріоритет інциденту, кількість некоректних призначень інциденту та повнота наданої інформації про інцидент відповідно.

Етап 3 – Побудова панелі індикаторів та візуалізація залежності *KPI* та *E*. Наступним етапом розробленого методу є побудова панелі індикаторів (ПІ), за допомогою якої і буде проходити моніторинг, аналіз та управління ефективністю роботи CSIRT. Панель індикаторів – це інструмент для візуалізації та аналізу інформації про бізнес-процеси і їх ефективність. Дані, що виводяться на ПІ, зазвичай представлені у вигляді ***KPI***. Сама система ПІ може бути складовою частиною корпоративної інформаційної системи, або виступати як самостійний застосунок [10]. Використання ПІ дозволить представити отримані дані в зручній формі – діаграмах, графіках або схемах даних. Для кожної організації, в залежності від її оперативних, планових та стратегічних цілей дана панель складається індивідуально.

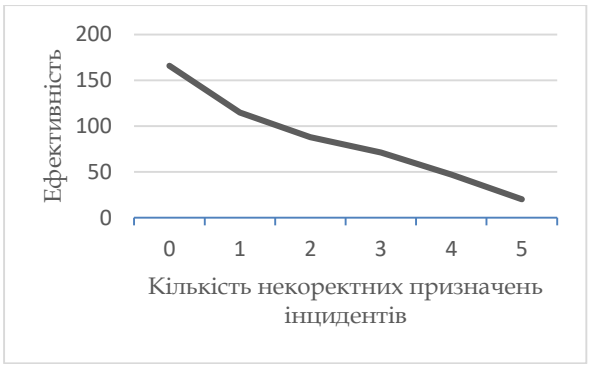
Варіант 1

Наприклад, використовуючи вихідні дані попереднього етапу, візуалізуємо отримані результати (рис. 1, 2).

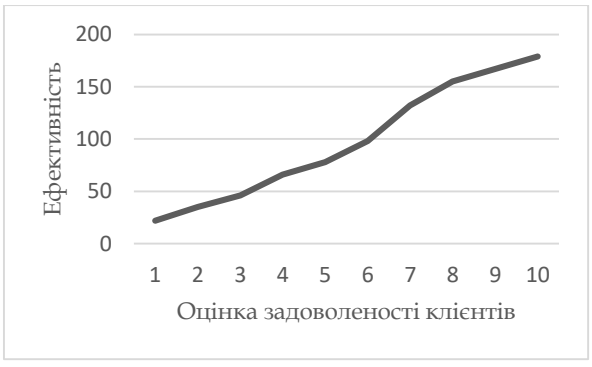


а) б) в) г)

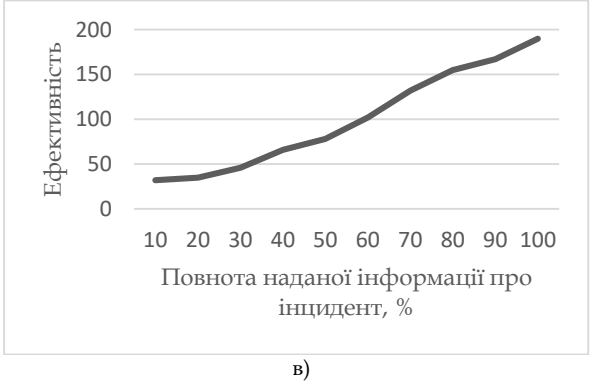
Рис. 1. Значення коефіцієнтів кореляції: а) пріоритет інциденту; б) оцінка задоволеності клієнтів; в) кількість некоректних призначень інциденту; г) повнота наданої інформації про інцидент



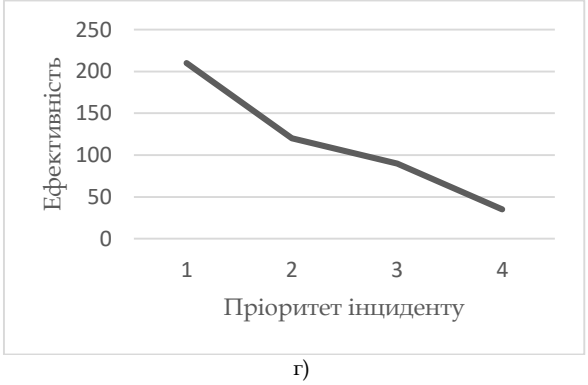
а)



б)



в)



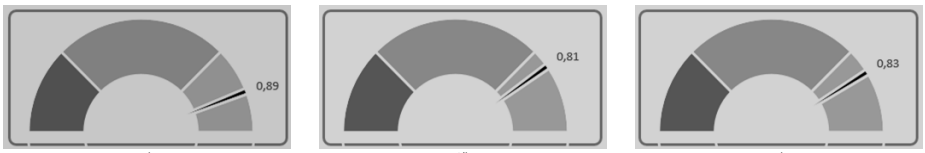
г)

Рис. 2. Графік залежності ефективності від: а) кількості некоректних призначень інцидентів; б) оцінки задоволеності клієнтів; в) повноти наданої інформації про інцидент; г) пріоритету інциденту

Провівши аналіз отриманих результатів (рис. 1,2), можна зробити висновок про залежність ефективності від кожного з визначених KPI та сформувати обмеження: якщо INAI > 1, то E < 100; якщо ECS < 7, то E < 100; якщо CII < 60, то E < 100; якщо PRI < 2, то E < 100.

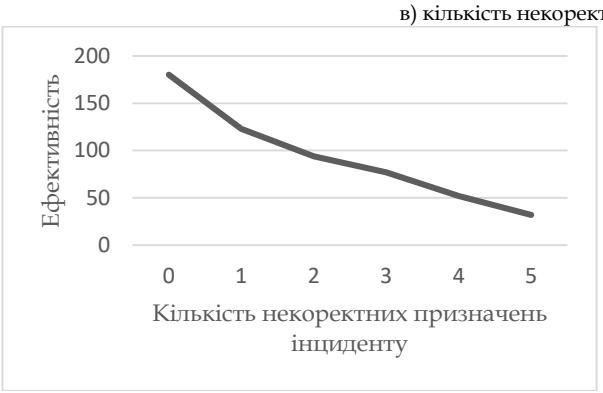
Варіант 2

Наприклад, аналогічно використовуючи вихідні дані попереднього етапу, візуалізуємо отримані результати (рис. 3, 4).

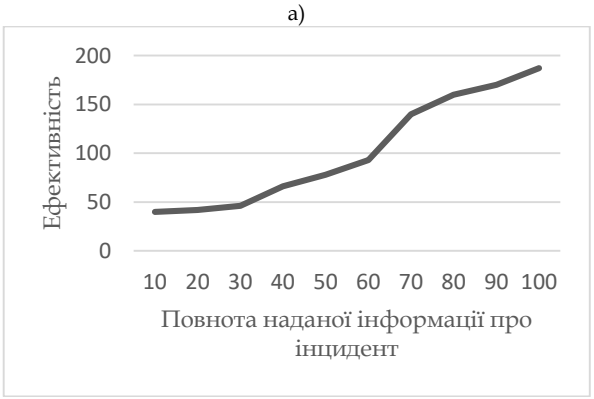


а) б) в)

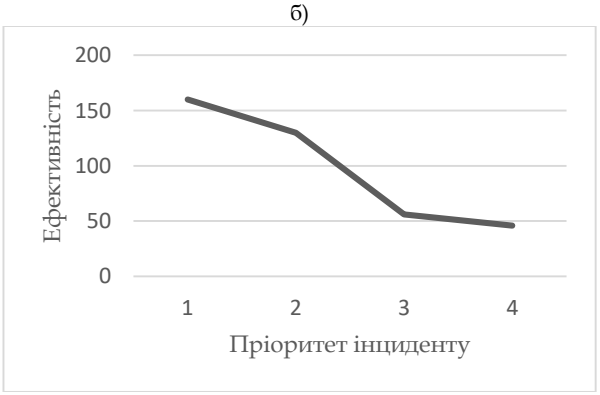
Рис. 3. Значення коефіцієнтів кореляції: а) пріоритет інциденту; б) повнота наданої інформації про інцидент; в) кількість некоректних призначень інциденту



а)



б)



в)

Рис. 4. Графік залежності ефективності від: а) кількості некоректних призначень інцидентів; б) повноти наданої інформації про інцидент; в) пріоритету інциденту

Провівши аналіз отриманих результатів (рис. 3, 4), можна зробити висновок про залежність ефективності від кожного з визначених KPI та сформувати обмеження: якщо INAI > 1 то E < 100; якщо CII < 70 то E < 100; якщо PRI < 2 то E < 100.

Висновки

Таким чином, у роботі розроблено метод оцінювання ефективності обробки кіберінцидентів центрами CSIRT, який за рахунок визначення показників функціонування CSIRT, виділення серед них ключових показників ефективності, використовуючи багаточинниковий кореляційно-регресійний аналіз, побудови панелі індикаторів, візуалізації залежності KPI та E, дає можливість проводити аудит діяльності CSIRT та інших центрів технічного обслуговування інформаційно-телекомунікаційних систем.

Цей метод та сформовані на його основі засоби будуть корисними керівникам центрів реагування на інциденти для моніторингу, аналізу, оцінки та управління ефективністю роботи CSIRT. Так як метод є універсальним, його можна застосувати в будь-якій компанії або державній установі, з метою підвищення як рівня інформаційної безпеки, так і ефективності роботи працівника, відділу та організації в цілому.

Література

[1] Kreher R. UMTS Performance Measurement: A Practical Guide to KPIs for the UTRAN Environment. - John Wiley & Sons, Ltd, 2006. – 227 pp.

[2] Балабанова Л.В. Управління персоналом: Навч. посібник / Л.В. Балабанова, О.В. Сардак. – К.: Професіонал, 2006. – 512 с.

[3] Бон Я.В. ИТ Сервис-менеджмент, введение / под ред. Яна Ван Бона; пер. с англ. осуществлен компанией «IT Expert», 2003. – 240 с.

[4] Головатий М.Ф. Управлінські аспекти соціальної роботи. Курс лекцій / М.Ф. Головатий, М.П. Лукашевич, Г.А. Дмитренко та ін. — К.: МАУП, 2004. — 368 с.

[5] Гнатюк В.О. Аналіз дефініцій поняття «інцидент» та його інтерпретація у кіберпросторі // В.О. Гнатюк / Безпека інформації. − №3 (19). – 2013. − С. 175-180.

[6] Данюк В.М. Менеджмент персоналу: Навч. посіб. / В.М. Данюк, В.М. Петюх, С.О. Цимбалюк та ін.; За заг. ред. В.М. Данюка, В.М. Петюха. – К.:КНЕУ, 2004. – 398 с.

[7] Кінзерявий В.М. Базові показники ефективності роботи команд реагування на кіберінциденти / В.М. Кінзерявий, В.О. Гнатюк // Безпека інформації. – Том 20, №2. – 2014. – С. 193-196.

[8] Колот А.М. Мотивація персоналу: Підручник. / А.М. Колот – К.: КНЕУ, 2002. - 337 с.

[9] Мармоза А.Т. Теорія статистики / А.Т. Мармоза // Підручник для студентів вищих навчальних закладів. – К. 2013. – С. 333-397.

[10] Панели индикаторов как инструмент управления: ключевые показатели эффективности, мониторинг деятельности, оценка результатов / Уэйн У. Эккерсон; Пер. с англ. — М.: Альпина Бизнес Букс, М., 2007. — 396 с.

[11] Панов М.М. Оценка деятельности и система управления компанией на основе KPI / М.М. Панов. – М.: Инфра-М, 2012. – 255 с.

[12] Савченко В.А. Управління розвитком персоналу : навч. посіб. / В.А. Савченко. – Київ : КНЕУ,2002. – 351 с.

[13] Сизова Т.М. Статистика: Учебное пособие. – СПб.: СПб ГУИТМО, 2005. – 80 с.

[14] Система KPI (Key Performance Indicator): разработка и применение показателей бизнес-процесса. Показатели эффективности. – [Електронний ресурс]. – Режим доступу: http://www.businesstudio.ru/procedures/business/ kpi (25.01.2017).

[15] Сучасні методи оцінки персоналу – [Електронний ресурс]. – Режим доступу: http://dspace.nuft.edu.ua/jspui/bitstream/123456789/10385/1/Mordeen%20methods%20of%20evaluation%20personnel.pdf (25.01.2017).

[16] Сучасні методи оцінки персоналу – [Електронний ресурс]. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=776 (25.01.2017).

УДК 004.054 (045)

Виноградов Н.А., Иванченко Е.В., Гнатюк В.А. Метод оценивания эффективности обработки киберинцидентов центрами CSIRT

Аннотация. *Обработка и управления киберинцидентамы - важные задачи, решением которых занимаются специализированные центры типа CSIRT. Однако на сегодня отсутствуют механизмы оценивания их работы. Учитывая это, в работе пронанализовано современные методы оценивания работы персонала, проведения их многокритериальный анализ. Опираясь на результаты анализа, разработан метод оценивания эффективности обработки киберинцидентив центрами CSIRT, который за счет определения показателей функционирования CSIRT, выделение среди них ключевых показателей эффективности используя многофакторный корреляционно-регрессионный анализ, построения панели индикаторов, визуализации зависимости ключевых показателей эффективности и эффективности, дает возможность проводить аудит деятельности CSIRT и других центров технического обслуживания информационно-телекоммуникационных систем. Этот метод и сформированные на его основе средства будут полезными руководителям центров реагирования на киберинциденты для мониторинга, анализа, оценивания и управления эффективностью работы CSIRT. Разработанный метод можно применить в любой компании или государственном учреждении с целью повышения как уровня информационной безопасности, так и эффективности работы сотрудника, отдела и организации в целом.*

Ключевые слова: *ключевые показатели эффективности, киберинцидент, CSIRT, корреляционная матрица, панель индикаторов.*

Vinogradov M., Ivanchenko Ye., Gnatyuk V. Method for efficiency assessment of cyberincidents processing by CSIRT

Abstract. *Cyberincidents processing and managing are important problems, solving of which involved specialized centers such as CSIRT. However, nowadays there are no mechanisms for assessment their work. In this regard in this paper are analyzed modern methods for estimation personnel work, conducted their multicriterial analysis. Based on analysis developed a method of efficiency estimation of processing cyberincidents by CSIRT centers, that by definition CSIRT performance indices, selection among them key performance indicators using multivariate correlation-regression analysis, indicators panel construction, dependence visualization of key performance indicators and efficiency, makes it possible to conduct audit for CSIRT activities and for other service centers of information and telecommunication systems. This method and formed on its basis tools will be useful for heads of responding on cyberincidents centers for monitoring, analysis, evaluation and management of CSIRT performance. Developed method can be applied at any company or government agency in order to increase information security level and effectiveness of the employee, department and organization.*

Key words: *key performance indicators, cyberincidents, CSIRT, correlation matrix, indicators panel.*

Отримано *3 квітня 2017 року*, затверджено редколегією *17 квітня 2017 року*