УДК 004.056.53(045)
DOI https://doi.org/10.32782/IT/2022-3-3

Анна КОРЧЕНКО
доктор технічних наук, професор, професор кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, Дніпро, Україна, 49005, annakor@ukr.net
***ORCID ID:** 0000-0003-0016-1966*
***Scopus Author ID:** 56029291400*

Сергій МАЦЮК
кандидат технічних наук, доцент, доцент кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, Дніпро, Україна, 49005, matsiuk.s.m@nmu.one
***ORCID ID:** 0000-0001-6798-5500*
***Scopus Author ID:** 57189702975*

Олександр ЧОБАЛЬ
канд. фіз.-мат. наук, доцент, кафедра твердотільної електроніки та інформаційної безпеки, ДВНЗ «Ужгородський національний університет», пл. Народна, 3, м. Ужгород 88000, Україна, oleksandr.chobal@uzhnu.edu.ua
***ORCID ID:** 0000-0002-8042-8052*
***Scopus Author ID:** 35241822900*

Олександр КРУЧІНІН
старший викладач кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, Дніпро, Україна, 49005, kruchinin.o.v@nmu.one
***ORCID ID:** 0000-0001-5523-948X*
***Scopus Author ID:** 55437732500*

Тарас ПАРАЩУК
аспірант кафедри безпеки інформаційних технологій, Національний авіаційний університет, просп. Космонавта Комарова, 1, Київ, Україна, 03058, taras1039@ukr.net
***ORCID ID:** 0000-0002-7014-761X*
***Scopus Author ID:** 56071538700*

Бібліографічний опис статті: Корченко, А., Мацюк, С., Чобаль, О., Кручінін, О., Паращук, Т. (2022). Метод формування параметрів функціональних обов'язків для оцінки загроз в соціотехнічних системах. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 19–26, doi: https://doi.org/10.32782/IT/2022-3-3

МЕТОД ФОРМУВАННЯ ПАРАМЕТРІВ ФУНКЦІОНАЛЬНИХ ОБОВ'ЯЗКІВ ДЛЯ ОЦІНКИ ЗАГРОЗ В СОЦІОТЕХНІЧНИХ СИСТЕМАХ

На сьогоднішній день рівень інформаційних атак, які включають в себе людський чинник значно збільшується. Велику їх частку складає збір інформації за допомогою фішингових і інсайдерських атак, соціального інжинірингу та інших видів кібератак. Ключова проблема ефективного виявлення відповідних атак, полягає в тому, що параметри, якими можна описати певні процеси мають велику кількість складно описуваних понять, відношень та специфічних особливостей. Також, як слідство, простежується відсутність необхідних методів і систем, орієнтованих на оцінку пов'язаних загроз і ризиків та виявлення відповідних атак. З урахуванням цього відбувається зростання зазначених атак, та потреба в системах оцінки загроз та ризиків, пов'язаних з людським чинником. А розробка відповідних засобів формування функціональних обов'язків для оцінки загроз є однією із складових даної теми, яка дозволить розглянути загрози в соціотехнічних системах з позицій функціональних обов'язків персоналу певної системи є актуальним науковим завданням. Виходячи з цього, метою роботи є розробка методу формування параметрів функ-

ціональних обов'язків для оцінки загроз в соціотехнічних системах. В статті визначено базову структуру профіля співробітника та ключові позиції запропонованого підходу, що включають загальні характеристики співробітника та специфічні компонент профіля. А з урахуванням базової структури профіля сформувано параметри, що відображають певні функціональні обов'язки для подальшої оцінки загроз в соціотехнічних системах.

Ключові слова: *загрози, ризики, атаки, соціотехнічні системи, система профілювання, лінгвістичні параметри, експертні методи, метод формування параметрів функціональних обов'язків, інформаційна безпека.*

Anna KORCHENKO
Doctor of Technical Sciences, Professor, Professor at the Department of Information Security and Telecommunications, National Technical University Dnipro Polytechnic, 19 Dmytra Yavornytskoho Avenue, Dnipro, Ukraine, 49005, annakor@ukr.net
ORCID ID: *0000-0003-0016-1966*
Scopus Author ID: *56029291400*

Sergii MATSIUK
Assistant Professor at the Department of Information Security and Telecommunications, National Technical University Dnipro Polytechnic, 19 Dmytra Yavornytskoho Avenue, Dnipro, Ukraine, 49005, matsiuk.s.m@nmu.one
ORCID ID: *0000-0001-6798-5500*
Scopus Author ID: *57189702975*

Oleksandr CHOBAL
Candidate of Physical and Mathematical Sciences, Associate Professor at the Department of Solid State Electronics and Information Security, Uzhhorod National University, 3 Narodna Square, Uzhhorod Ukraine, 88000, oleksandr.chobal@uzhnu.edu.ua
ORCID ID: *0000-0002-8042-8052*
Scopus Author ID: *35241822900*

Oleksandr KRUCHININ
Senior Lecturer at the Department Information Security And Telecommunications, National Technical University Dnipro Polytechnic, 19 Dmytra Yavornytskoho Avenue, Dnipro, Ukraine, 49005, kruchinin.o.v@nmu.one,
ORCID ID: *0000-0001-5523-948X*
Scopus Author ID: *55437732500*

Taras PARASCHUK
Postgraduate at the Student of Academic Department of IT-Security, National Aviation University, Kosmonavta Komarova Ave., 1, Kyiv, Ukraine, 03058, taras1039@ukr.net
ORCID ID: *0000-0002-7014-761X*
Scopus Author ID: *56071538700*

Бібліографічний опис статті: Korchenko, A., Matsiuk, S., Chobal, O., Kruchinin, O., Paraschuk, T. (2022). Metod formuvannia parametriv funktsionalnykh obov'iazkiv dlia otsinky zahroz v sotsiotekhnichnykh systemakh [The method of forming the parameters of functional responsibilities for assessing threats in sociotechnical systems]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 19–26, doi: https://doi.org/10.32782/IT/2022-3-3

THE METHOD OF FORMING THE PARAMETERS OF FUNCTIONAL RESPONSIBILITIES FOR ASSESSING THREATS IN SOCIOTECHNICAL SYSTEMS

Today, the level of information attacks, which include the human factor, is increasing significantly. A large part of them is information gathering with the help of phishing and insider attacks, social engineering and other types of cyber attacks. The key problem of effective detection of relevant attacks is that the parameters that can be used to describe certain processes have a large number of difficult to describe concepts, relations and specific features. Also, as an investigation, there is a lack of necessary methods and systems aimed at assessing related threats and risks and identifying relevant attacks. With this in mind, there is an increase in these attacks and the need for threat and risk assessment systems related to the human factor. And the development of appropriate means of forming functional

responsibilities for threat assessment is one of the components of this topic, which will allow considering threats in sociotechnical systems from the standpoint of functional responsibilities of the personnel of a certain system is an actual scientific task. Based on this, the goal of the work is to develop a method of forming the parameters of functional duties for the assessment of threats in sociotechnical systems. The article defines the basic structure of the employee's profile and the key positions of the proposed approach, which include the general characteristics of the employee and the specific component of the profile. And taking into account the basic structure of the profile, parameters reflecting certain functional duties for further assessment of threats in socio-technical systems were formed.

Key words: *threats, risks, attacks, sociotechnical systems, profiling system, linguistic parameters, expert methods, method of forming parameters of functional responsibilities, information security.*

Актуальність проблеми та наліз останніх досліджень і публікацій. Захист будь-якої системи починається не тільки з впровадження політики інформаційної безпеки, визначенням відповідальних осіб, документуванні всіх процесів і т.д., але й слід розглядати кожного працівника компанії, як потенційну точку доступу до інформаційної системи в цілому, а також складову системи, яку важко оцінити та задати конкретні межі впливу на частину системи або всю систему в цілому.

В даний час для вирішення проблеми виявлення атак та загроз пов'язаних з людським чинником приділяється багато уваги. Доказом цього можуть бути дослідження та звіти щодо можливих атак за 2018-2022 р.

Аналіз аналітичних досліджень (2020 Data Breach Investigations Report; Cisco Annual Cybersecurity Report, 2018; Cisco Annual Cybersecurity Report 2020; Систематизований досвід війни: актуальні питання IT та кібербезпеки в Україні - European Business Association; 5 актуальних тенденцій у галузі кібербезпеки в 2021 році. Кібербезпека у 2021 – чим запам'ятався цей рік? ESET) компаній InfoWatch, Cisco Systems Inc, DeviceLock, Verizon, Positive Technologies показав, що рівень інформаційних атак, які включають в себе людський чинник збільшується. Велику їх частку складає збір інформації за допомогою фішингових і інсайдерських атак, соціального інжинірингу та інших видів.

Відповідно до (The human factor is key to good security; David Lacey, 2009; Коцюк; Маслова; Ліпкан, Максименко, Желіховський, 2006; Hadnagy, 2018; Conheady, 2014; Zinatullin, 2016; Yevseiev, Laptiev, Lazarenko et al., 2021), можемо зробити висновки, що основна проблема ефективного виявлення атак, орієнтованих на людський чинник полягає в тому, що параметри, якими можна описати відповідні процеси мають велику кількість складно описуваних понять, відношень та специфічних особливостей. Також, як слідство, простежується відсутність необхідних методів і систем, орієнтованих на оцінку пов'язаних загроз і ризиків та виявлення відповідних атак.

З урахуванням цього та на основі проаналізованих джерел можна зробити висновок про неухильне зростання зазначених атак, та наявність невеликої кількості систем оцінки загроз та ризиків, пов'язаних з людським чинником, дозволяє стверджувати, що дана тема є актуальною, обґрунтованою та потребує подальшого дослідження. А в свою чергу метод формування параметрів функціональних обов'язків для оцінки загроз є однією із складових даної теми, яка дозволить розглянути загрози в соціотехнічних системах з позицій зору функціональних обов'язків персоналу певної системи.

Однією із задач при розробці методів та моделей для покращення систем на базі методології оцінки загроз, є збір статистичних даних, аналіз бізнес процесів, визначення критичних активів та конфіденційної інформації, формування профіля співробітника, підвищення інформаційної обізнаності працівників для можливості протидії інформаційним загрозам.

Метою даної статті є створення методу формування параметрів функціональних обов'язків для оцінки загроз в соціотехнічних системах.

Викладення основного матеріалу дослідження. Визначмо базову структуру профіля співробітника та ключові позиції даного підходу. Базовий профіль персоналу можна розділити на два функціональних компонента:

1. Загальний компонент профіля:

− дані про особу (прізвище, ім'я, по батькові, вік, місце проживання чи прописки, освіта, попереднє місце роботи та посада, стаж роботи, заробітна плата та тощо);

− посада та відділ;

− кількість підлеглих всіх рівнів ієрархічної структури відділу/організації;

2. Специфічний компонент профіля:

− функціональні обов'язки;

− залежність функціональних обов'язків від можливих загроз в компанії;

− взаємозв'язки з іншими співробітниками;

− додаткові параметри.

Перший компонент профіля відповідає за загальні характеристики співробітника, вплив на очікувану величину загрози для певного профіля і за необхідності може бути визначений експертом. Тобто, якщо певна властивість із загального компонента профіля на судження експерта, є важливою і може збільшити або зменшити ступінь очікуваної величини загрози,

тоді він формує певний параметр (коефіцієнт) впливу, що враховується при оцінюванні.

Другий компонент профіля враховує специфіку роботи відділу та займаної посади. Саме даний компонент відповідає за формування основних параметрів та значень (кількісних та якісних), які дозволяють:

1. Оцінити ступінь значимості конкретного профіля для системи, не тільки з точки зору можливої загрози, а і активу;

2. Визначити можливий вплив профіля на певні бізнес процеси, що базуються на функціональних обов'язках;

3. Встановити залежність функціональних обов'язків від можливих загроз в компанії та визначити середню очікувану величину по кожному із них;

4. Визначити взаємозв'язки між співробітниками та відділами та побудувати аналітичні залежності між ними;

5. Побудувати математичні моделі та візуально продемонструвати залежності між параметрами та їх значеннями;

6. Описати кількісно та/або якісно можливість впливу людського чинника на підсистеми та систему в цілому.

З урахуванням базової структури профіля сформовано параметри, що відображають певні функціональні обов'язки для подальшої оцінки загроз в соціотехнічних системах.

Введемо множину оціночних інтервалів $\boldsymbol{EI}$ для можливих значень параметрів, які будуть використовуватись експертом (Корченко, 2006; Корченко, 2019; 18. Akhemetov, Korchenko, Akhmetova et al., 2016; Zhumangaliyeva, Korchenko, Doszhanova, 2019; Korchenko, Breslavskyi, Yevseiev, 2021) при оцінці функціональних обов'язків та загроз:

$$\boldsymbol{EI} = \{\cup_{i=1}^{n_e} \boldsymbol{EI}_i\} = \{EI_1, EI_2, EI_3, \dots, EI_{n_e}\}, (i = \overline{1, n_e}), \quad (1)$$

де n_e визначає кількість всіх оціночних інтервалів.

Можливі значення всіх оціночних інтервалів $\boldsymbol{EI}$, які експерт буде використовувати при оцінці функціональних обов'язків та загроз, визначмо у вигляді таблиці 1.

Таблиця 1

Можливі значення оціночного інтервалу

Числові значення	Лінгвістичні значення частоти	Лінгвістичні значення рівня
1–2	Рідко	Дуже низький
3–4	Іноді	Низький
5–6	Досить часто	Середній
7–8	Часто	Вище середнього
9-10	Дуже часто або завжди	Високий

Далі, визначмо множину коефіцієнтів впливу:

$$\boldsymbol{K} = \{\cup_{i=1}^{n_k} \boldsymbol{K}_i\} = \{K_1, K_2, K_3, \dots, K_{n_k}\}, (i = \overline{1, n_k}), \quad (2)$$

при цьому n_k визначає кількість всіх можливих коефіцієнтів.

Сформувавши множини $\boldsymbol{EI}$ та $\boldsymbol{K}$, визначмо бієктивну підмножину відповідності $\boldsymbol{M}$ для $\boldsymbol{EI}$ та $\boldsymbol{K}$, яка однозначно асоціює один елемент множини $\boldsymbol{EI}$ з одним і тільки одним елементом множини $\boldsymbol{K}$.

При $n_e = 5$ та $n_k = 5$ для множини з п'яти оціночних інтервалів

$$\boldsymbol{EI} = \{EI_1, EI_2, EI_3, EI_4, EI_5\} = \{[1;2], [3;4], [5;6], [7;8], [9;10]\}$$

та відповідною їм множиною з коефіцієнтами

$$\boldsymbol{K} = \{K_1, K_2, K_3, K_4, K_5\} = \{0,05; 0,1; 0,125; 0,175; 0,25\}$$

сформуємо підмножину $\boldsymbol{M}$:

$$\boldsymbol{M} = \left\{ \begin{matrix} (EI_1, K_1), (EI_2, K_2), \\ (EI_3, K_3), (EI_4, K_4), (EI_5, K_5) \end{matrix} \right\} = \left\{ \begin{matrix} ([1;2]; 0,05), ([3;4]; 0,1), \\ ([5;6]; 0,125), ([7;8]; 0,175), \\ ([9;10]; 0,25) \end{matrix} \right\}. \quad (3)$$

Розглянуту в прикладі множину $\boldsymbol{M}$ можна подати у більш зручному вигляді для подальшого аналізу разом з відповідними коефіцієнтами (див. табл. 2).

Аналогічні дані до таблиці 2 можна сформувати також для оціночних інтервалів описаних в таблиці 1 (від «Дуже низький» до «Високий»; від «Рідко» до «Дуже часто») з відповідними коефіцієнтами.

Також, визначенні коефіцієнти є лише рекомендованими для використання експертом і є оптимальними при конвертації оціночного значення в заданий коефіцієнт. Тому в даній

Таблиця 2

Інтерпретація залежності між оціночними інтервалами та відповідними коефіцієнтами

Елемент множини, *M*	Значення оціночного інтервалу, *EI*	Коефіцієнт, *K*
(EI_1, K_1)	1–2	0,05
(EI_2, K_2)	3–4	0,1
(EI_3, K_3)	5–6	0,125
(EI_4, K_4)	7–8	0,175
(EI_5, K_5)	9-10	0,25

роботі при обрахунках будуть використовуватись коефіцієнти з таблиці 2.

Розглядаючи певну компанію, слід зазначити, що кожен співробітник має список чітко закріплених функціональних обов'язків (посадових обов'язків), за якими є закріпленні визначенні бізнес процеси.

Для формалізації процесу формування зазначених вище компонент, спочатку введемо множину CE, яка описує співробітників компанії працюючих в певний часовий проміжок t:

$$\boldsymbol{CE}^t = \{\cup_{i=1}^{n_c} \boldsymbol{CE}_i^t\} = \{CE_1^t, CE_2^t, \dots, CE_{n_c}^t\}, (i = \overline{1, n_c}), \quad (4)$$

де n_c – кількість всіх співробітників, що можуть працювати в компанії в певний період часу t.

Далі, визначмо множину всі функціональних обов'язків WR, які можуть виникати в процесі функціонування бізнес процесів компанії в певний часовий проміжок t та можуть бути спільними для декількох співробітників одного або різних відділів:

$$\boldsymbol{WR}^t = \{\cup_{i=1}^{n_w} \boldsymbol{WR}_i^t\} = \{WR_1^t, WR_2^t, \dots, WR_{n_w}^t\}, (i = \overline{1, n_w}), \quad (5)$$

де n_w – визначає кількість функціональних обов'язків, що можуть бути у співробітників компанії в певний період часу t.

Далі, для CE^t та WR^t визначмо математичну залежність, тобто відповідність між даними множинами як кортеж (CE^t, WR^t, ER^t), де ER^t – підмножина відповідності між CE^t та WR^t.

Підмножину ER^t можна описати графом відповідності (див. рис. 1).

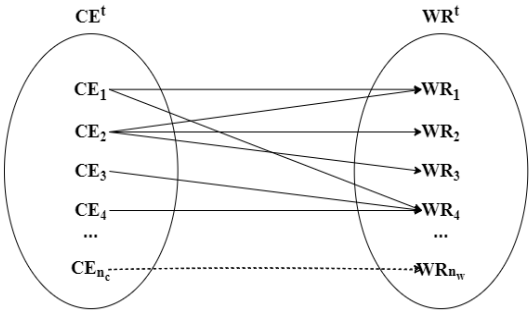

Рис. 1. Граф відповідності між множинами CE^t та WR^t

На основі проілюстрованого графа, маємо що дане відображення є несюр'єктивним та неін'єктивним, тобто кожний елемент WR^t множини асоціюється щонайменше з одним або більше елементів CE^t множини або дані асоціації можуть бути відсутні. Також дану підмножину ER^t можна подати в вигляді:

$$\boldsymbol{ER}^t = \left\{\bigcup_{i=1}^{n_c}\bigcup_{j=1}^{n_w}(\boldsymbol{CE}_i^t, \boldsymbol{WR}_j^t)\right\} = \left\{\begin{matrix}(CE_{n_c}^t, WR_1^t) \dots (CE_{n_c}^t, WR_{n_w}^t), \\ (CE_2^t, WR_1^t) \dots (CE_2^t, WR_{n_w}^t), \\ \dots, \\ (CE_2^t, WR_1^t) \dots (CE_2^t, WR_{n_w}^t)\end{matrix}\right\}, \quad (6)$$

$$\left(i = \overline{1, n_c}\right), \left(j = \overline{1, n_w}\right).$$

Слід зазначити що кожному співробітнику може відповідати декілька функціональних обов'язків, а один функціональний обов'язок може мати відношення до декількох співробітників одночасно.

Далі введемо множину функціональних обов'язків для конкретного співробітника:

$$\boldsymbol{WR}(\boldsymbol{CE}_j^t)^t = \{\cup_{i=1}^{m} \boldsymbol{WR}_i^t\} = \{WR_1^t, WR_2^t, \dots, WR_n^t\}, \left(i = \overline{1, m}\right), \quad (7)$$

де m – кількість всіх функціональних обов'язків для конкретного співробітника CE_j^t в певний період часу t.

Далі визначмо та опишемо загальні параметри функціональних обов'язків. Для цього опишемо в загальному виді обов'язок WR_i^t з формули (7), за допомогою кортежу з параметрами:

$$\boldsymbol{WR}_i^t = \boldsymbol{WRN}_i, \boldsymbol{PR}_i, \boldsymbol{FPR}_i, \boldsymbol{LC}_i, \boldsymbol{DDR}_i, \quad (8)$$

в якому:

– WRN_i – назва певного функціонального обов'язку;

– PR_i – ступінь важливості обов'язку в структурі бізнес процесів компанії (шкала оцінки від 1 до 10);

– FPR_i – частота виконання певного обов'язку відносно всіх обов'язків конкретного профілю (шкала оцінки від «рідко» до «дуже часто»);

– LC_i – рівень компетентності конкретного співробітника (профілю) для виконання певного обов'язку (шкала оцінки від «дуже низький» до «високий»);

– DDR_i – ступінь залежності обов'язку від критичних активів та конфіденційної інформації в компанії (шкала від 1 до 10).

Оцінки параметрів визначаються експертом на основі проведеного аналізу певного співробітника компанії. Всі оцінки повинні відповідати визначеній шкалі оцінок та процес оцінювання повинен відбуватися максимально об'єктивно. Тепер перейдемо до детального розгляду кожного із параметрів з формули WR_i^t.

Пріоритет. Оцінка для даного параметру відбувається на основі комплексного аналізу всіх бізнес процесів, де визначається ступінь впливу даного обов'язку при його виконанні певним профілем, визначається ступінь залежності від інших бізнес процесів, структурна складність обов'язку і кількість використаних ресурсів та активів досліджуваної компанію в цілому.

Частота виконання конкретного обов'язку. Визначення оцінки для даного параметру відбувається на основі проаналізованих бізнес процесів в яких бере участь досліджуваний профіль, також повинні враховуватись всі обов'язки, які повинен виконувати даний співробітник.

Рівень компетентності. Для визначення точної оцінки необхідно проаналізувати якість

виконуваних обов'язків певним профілем та його компетентності визначенні більш компетентною відповідальною особою в компанії.

Ступінь залежності обов'язку від критичних активів та конфіденційної інформації. Оцінка для даного параметру відбувається на основі аналізу процесів з визначення активів та інформації пов'язаної з виконанням певного обов'язку конкретним співробітником компанії.

Відповідно до формули (7) при $m = 9$ розглянемо список з функціональних обов'язків, для голови юридичного відділу абстрактної компанії:

$$\boldsymbol{WR}(\boldsymbol{CE}_1^t)^t = \left\{\cup_{i=1}^{9} \boldsymbol{WR}_i^t\right\} = \{WR_1^t, WR_2^t, WR_3^t, \dots, WR_9^t\}.$$

Далі опишемо кожен функціональний обов'язок $\boldsymbol{WR}_i^t$ з формули (7) у вигляді кортежу з параметрами *WRN*,*PR*,*FPR*,*LC*,*DDR* (враховуючи визначену шкалу оцінки), які визначив експерт використовуючи формулу (8):

$$WR_1^t = WRN_1, PR_1, FPR_1, LC_1, DDR_1 = WRN_1, 4, "\text{Дуже часто}", "\text{Середній}", 1;$$

$$WR_2^t = WRN_2, PR_2, FPR_2, LC_2, DDR_2 = WRN_2, 9, "\text{Досить часто}", "\text{Високий}", 9;$$

$$WR_3^t = WRN_3, PR_2, FPR_2, LC_2, DDR_2 = WRN_3, 7, "\text{Часто}", "\text{Вище середнього}", 6;$$

$$WR_4^t = WRN_4, PR_2, FPR_2, LC_2, DDR_2 = WRN_4, 7, "\text{Досить часто}", "\text{Високий}", 6;$$

$$WR_5^t = WRN_5, PR_2, FPR_2, LC_2, DDR_2 = WRN_5, 6, "\text{Часто}", "\text{Вище середнього}", 2;$$

$$WR_6^t = WRN_6, PR_2, FPR_2, LC_2, DDR_2 = WRN_6, 8, "\text{Часто}", "\text{Високий}", 8;$$

$$WR_7^t = WRN_7, PR_2, FPR_2, LC_2, DDR_2 = WRN_7, 6, "\text{Часто}", "\text{Високий}", 8;$$

$$WR_8^t = WRN_8, PR_2, FPR_2, LC_2, DDR_2 = WRN_8, 8, "\text{Досить часто}", "\text{Високий}", 6;$$

$$WR_9^t = WRN_9, PR_2, FPR_2, LC_2, DDR_2 = WRN_9, 5, "\text{Іноді}", "\text{Середній}", 5.$$

Описані кортежі функціональних обов'язків відобразимо в таблиці 3, де зазначено назва кожного параметру $\boldsymbol{WRN}_i$.

Описана таблиця та розглянутий метод формування параметрів для функціональних обов'язків дозволяє продемонструвати ряд важливих параметрів та методологію їх оцінки. Також важливо значити, що даний метод є важливим етапом перед визначенням залежності

Таблиця 3

Приклад функціональних обов'язків з визначними параметрами

Номер обов'язку (*i*)	Назва обов'язку (*WRN*)	Пріоритет (*PR*)	Частота виконання конкретного обов'язку (*FPR*)	Рівень компетентності (*LC*)	Ступінь залежності обов'язку від критичних активів (*DDR*)
1	Робота з відкритими джерелами та інформаційними ресурсами	4	Дуже часто	Середній	1
2	Взаємодія з конфіденційною інформацією, що циркулює в організації	9	Досить часто	Високий	9
3	Управління та прийняття юридичних документів	7	Часто	Вище середнього	6
4	Створення та контроль бізнес процесів, що пов'язанні з юридичною стороною	7	Досить часто	Високий	6
5	Контроль поточного законодавства та стандартизація процесів під поточне законодавство	6	Часто	Вище середнього	2
6	Контроль за виконаною роботою підлеглих та формування робочих процесів у відділі	8	Часто	Високий	8
7	Контроль за документування процесів пов'язаних з юридичною діяльністю у відділі та компанії в цілому	6	Часто	Високий	8
8	Надання консультацій підлеглим та іншим відділам, які залежні від юридичного відділу	8	Досить часто	Високий	6
9	Проведення співбесід з працівниками при виникненні юридичних питань	5	Іноді	Середній	5

між обов'язками та всіма загрозами, що є наявними в компанії.

Висновки. На даному етапі виявлення атак, оцінка загроз в соціотехнічних системах є важливим питанням, особливо з точки зору людської складової. Тому запропонований метод формування параметрів для функціональних обов'язків є ключовим етапом розробки методології профілювання співробітників певної компанії. Даний метод дозволяє оцінити функціональні обов'язки конкретного співробітника та встановити залежності між співробітником та обов'язками за допомогою параметрів.

ЛІТЕРАТУРА:

1. 2020 Data Breach Investigations Report. URL: https://enterprise.verizon.com /resources/reports/2020-data-breach-investigations-report.pdf (Дата звернення: 02.09.2022).

2. Cisco Annual Cybersecurity Report 2018. URL: https://www.cisco.com /c/dam/m/hu_hu/ campaigns/ security-hub/pdf/acr-2018.pdf (Дата звернення: 11.09.2022).

3. Cisco Annual Cybersecurity Report 2018. URL: https://www.cisco.com /c/dam/m/en_hk/ciscolive/2020-ciso-benchmark-cybersecurity-series.pdf (Дата звернення: 11.09.2022).

4. Систематизований досвід війни: актуальні питання IT та кібербезпеки в Україні - European Business Association URL: https://eba.com.ua/ systematyzovanyj-dosvid-vijny-aktualni-pytannya-it-ta-kiberbezpeky-v-ukrayini/ (Дата звернення: 22.04.2023).

5. 5 актуальних тенденцій у галузі кібербезпеки в 2021 році URL: https://www.kliksolutions.com.ua/great-info/5-aktualnyh-tendenczij-u-galuzi-kiberbezpeky-v-2021-roczi/ (Дата звернення: 22.04.2023).

6. Кібербезпека у 2021 – чим запам'ятався цей рік? ESET | ESET URL: https://www.eset.com/ua/about/newsroom/press-releases/malware/itogi-goda-kakim-byl-2021-dlya-kiberbezopasnosti/ (Дата звернення: 22.04.2023).

7. The human factor is key to good security. URL: https://www.computerweekly.com/opinion/The-human-factor-is-key-to-good-security (Дата звернення: 11.09.2021).

8. David Lacey (2009). Managing the Human Factor in Information Security, How to win over staff and influence business managers, Chichester, John Wiley & Sons Ltd.

9. Коцюк Ю. А. Роль людського чинника у питаннях захисту інформаційних систем. URL: https://psj.oa.edu.ua/articles/2012/n20/%D0%9A%D0%BE %D1%86%D1%8E%D0%BA.pdf (Дата звернення: 20.09.2021).

10. Маслова Ю.Ю. Інформаційна безпека і людський фактор. URL: http://webcache.googleusercontent.com/search?q=cache:XmsbYCGJ78gJ:journals.dut.edu.ua/index.php/dataprotect/article/view/2462/2362+&cd=6&hl=uk&ct=clnk&gl=ua (Дата звернення: 20.09.2021).

11. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. К.: КНТ, 2006. 280 с. (Серія: Національна і міжнародна безпека).

12. Christopher Hadnagy. Social Engineering: The Science of Human Hacking. John Wiley & Sons, 2018. 320 pages.

13. Sharon Conheady. Social Engineering in IT Security: Tools, Tactics, and Techniques: Testing Tools, Tactics & Techniques. McGraw Hill Professional, 2014. 272 pages.

14. Leron Zinatullin. The Psychology of Information Security: Resolving conflicts between security compliance and human behaviour. IT Governance Publishing. 2016. 116 pages.

15. Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Model the protection of personal data from trust and the amount of information on social networks. Eureka: Physics and Engineering, 2021. Vol.32. №.1. – Pp. 24-31.

16. Корченко О.Г. Побудова систем захисту інформації на нечітких множинах: теорія та практичні рішення. К. : МК-Прес, 2006. 320 с.

17. Анна Корченко, Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт». 2019 361 с.

18. Akhemetov Bakhytzhan, Korchenko Anna, Akhmetova Sanzira, Zhumangalieva Nazym. Improved method for the formation of linguistic standards for of intrusion detection systems. Journal of Theoretical and Applied Information Technology, 2016. Vol.87. №.2. pp. 221-232.

19. Nazym Zhumangaliyeva, Anna Korchenko, Aliya Doszhanova, Aigul Shaikhanova, Shangytbayeva Gulmira Avkurova Zhadyra. Detection environment formation method for anomaly detection systems. Journal of Theoretical and Applied Information Technology, 2019. Vol.97. № 16. Pp. 4239-4250.

20. A. Korchenko, V. Breslavskyi, S. Yevseiev, N Zhumangalieva, A. Zvarych, S. Kazmirchuk, O. Kurchenko, O. Laptiev, O. Sievierinov, S. Tkachuk. Development of a method for constructing linguistic standards for

multi-criterial assessment of honeypot efficiency. Eastern-European Journal of Enterprise Technologies. 2021. Vol.109. №.1/2. Pp. 14-23.

REFERENCES:

1. 2020 Data Breach Investigations Report. URL: https://enterprise.verizon.com /resources/reports/2020-data-breach-investigations-report.pdf (Data zvernennia: 02.09.2022).

2. Cisco Annual Cybersecurity Report 2018. URL: https://www.cisco.com /c/dam/m/hu_hu/ campaigns/ security-hub/pdf/acr-2018.pdf (Data zvernennia: 11.09.2022).

3. Cisco Annual Cybersecurity Report 2018. URL: https://www.cisco.com /c/dam/m/en_hk/ciscolive/2020-ciso-benchmark-cybersecurity-series.pdf (Data zvernennia: 11.09.2022).

4. Systematyzovanyi dosvid viiny: aktualni pytannia IT ta kiberbezpeky v Ukraini - European Business Association URL: https://eba.com.ua/ systematyzovanyj-dosvid-vijny-aktualni-pytannya-it-ta-kiberbezpeky-v-ukrayini/ (Data zvernennia: 22.04.2023).

5. 5 aktualnykh tendentsii u haluzi kiberbezpeky v 2021 rotsi URL: https://www.kliksolutions.com.ua/great-info/5-aktualnyh-tendenczij-u-galuzi-kiberbezpeky-v-2021-roczi/ (Data zvernennia: 22.04.2023).

6. Kiberbezpeka u 2021 – chym zapamiatavsia tsei rik? ESET | ESET URL: https://www.eset.com/ua/about/ newsroom/press-releases/malware/itogi-goda-kakim-byl-2021-dlya-kiberbezopasnosti/ (Data zvernennia: 22.04.2023).

7. The human factor is key to good security. URL: https://www.computerweekly.com/opinion/The-human-factor-is-key-to-good-security (Data zvernennia: 11.09.2021).

8. David Lacey (2009). Managing the Human Factor in Information Security, How to win over staff and influence business managers, Chichester, John Wiley & Sons Ltd.

9. Kotsiuk Yu. A. Rol liudskoho chynnyka u pytanniakh zakhystu informatsiinykh system. URL: https:// psj.oa.edu.ua/articles/2012/n20/%D0%9A%D0%BE %D1%86%D1%8E%D0%BA.pdf (Data zvernennia: 20.09.2021).

10. Maslova Yu.Iu. Informatsiina bezpeka i liudskyi faktor. URL: http://webcache.googleusercontent.com/ search?q=cache:XmsbYCGJ78gJ:journals.dut.edu.ua/index.php/dataprotect/article/view/2462/2362+&cd=6&hl=uk&ct=clnk&gl=ua (Data zvernennia: 20.09.2021).

11. Lipkan V. A., Maksymenko Yu. Ye., Zhelikhovskyi V. M. Informatsiina bezpeka Ukrainy v umovakh yevrointehratsii: Navchalnyi posibnyk. K.: KNT, 2006. 280 s. (Seriia: Natsionalna i mizhnarodna bezpeka).

12. Christopher Hadnagy. Social Engineering: The Science of Human Hacking. John Wiley & Sons, 2018. 320 pages.

13. Sharon Conheady. Social Engineering in IT Security: Tools, Tactics, and Techniques: Testing Tools, Tactics & Techniques. McGraw Hill Professional, 2014. 272 pages.

14. Leron Zinatullin. The Psychology of Information Security: Resolving conflicts between security compliance and human behaviour. IT Governance Publishing. 2016. 116 pages.

15. Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Model the protection of personal data from trust and the amount of information on social networks. Eureka: Physics and Engineering, 2021. Vol.32. №.1. – Pp. 24-31.

16. Korchenko O. H. Pobudova system zakhystu informatsii na nechitkykh mnozhynakh: teoriia ta praktychni rishennia. K. : MK-Pres, 2006. 320 s.

17. Anna Korchenko, Metody identyfikatsii anomalnykh staniv dlia system vyiavlennia vtorhnen. Monohrafiia, Kyiv, TsP «Komprynt», 2019 – 361 s.

18. Akhemetov Bakhytzhan, Korchenko Anna, Akhmetova Sanzira, Zhumangalieva Nazym. Improved method for the formation of linguistic standards for of intrusion detection systems. Journal of Theoretical and Applied Information Technology, 2016. Vol.87. №.2. Pp. 221-232.

19. Nazym Zhumangaliyeva, Anna Korchenko, Aliya Doszhanova, Aigul Shaikhanova, Shangytbayeva Gulmira Avkurova Zhadyra. Detection environment formation method for anomaly detection systems. Journal of Theoretical and Applied Information Technology, 2019. Vol.97. №.16. Pp. 4239-4250.

20. A. Korchenko, V. Breslavskyi, S. Yevseiev, N Zhumangalieva, A. Zvarych, S. Kazmirchuk, O. Kurchenko, O. Laptiev, O. Sievierinov, S. Tkachuk. Development of a method for constructing linguistic standards for multi-criterial assessment of honeypot efficiency. Eastern-European Journal of Enterprise Technologies, 2021. Vol.109. №.1/2. Pp. 14-23.