УДК 004.056.53 (045)
DOI https://doi.org/10.32782/IT/2023-2-1

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:** 0000-0003-0016-1966,*
***Scopus Author ID:** 56029291400*

Роман КАРПЮК
аспірант кафедри кібербезпеки, Львівський національний університет імені Івана Франка, вул. Університетська, 1, Львів, Україна, 79000, roman.karpiuk@lnu.edu.ua,
***ORCID:** 0009-0001-0053-1608*

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

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:** 0000-0001-6798-5500*
***Scopus Author ID:** 57189702975*

Бібліографічний опис статті: Корченко, А, Карпюк, Р, Паращук, Т., Мацюк, С. (2023). Метод формування параметрів та оцінювання загроз в соціотехнічних системах. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 2, 3–11, doi: https://doi.org/10.32782/IT/2023-2-1

МЕТОД ФОРМУВАННЯ ПАРАМЕТРІВ ТА ОЦІНЮВАННЯ ЗАГРОЗ У СОЦІОТЕХНІЧНИХ СИСТЕМАХ

З кожним роком значна частина інформаційних технологій в соціотехнічних системах стрімко зростає. А розвиток відповідних систем безпосередньо залежить від відповідних інформаційних технологій, що використовуються в бізнес-процесах підприємств. Це впливає на появу нових загроз, уразливостей та атак, які пов'язані з інформаційною складовою. Рівень реалізації кібератак за останні роки стрімко зростає. Головною ціллю атак на соціотехнічні системи є персональні данні, облікові записи користувачів системи, комерційна таємниця, медична інформація, бази даних, переписка, дані платіжних карт тощо. Також, для попередження атак та виявлення потенційних загроз необхідно комплексно використовувати методи щодо оцінювання уразливостей та загроз, моделювання можливих впливів, а також світові практики та міжнародні стандарти і нормативні документи у галузі управління інформаційною безпекою. Проведений аналіз та розглянуті основні аспекти, які необхідні при формуванні параметрів для оцінювання загроз, створили базис для обґрунтування актуальності теми даної роботи. На основі сформованих аспектів було розроблено метод формування параметрів та оцінювання загроз в соціотехнічних системах. Метод враховує такі параметри, як: пріоритет, що показує ступень необхідності зменшення конкретної загрози; ступінь впливу на систему при реалізації певної загрози; ймовірність реалізації конкретної загрози в системі; чинник людської складової; чинник загрози, що характеризує на загальному рівні причини, які сприяють виникненню загрози. Також, відповідний метод, використовуючи отримані параметри повинен найбільш повно оцінити існуючі загрози в системі та може бути застосований при розробці методології профілювання співробітників.

Ключові слова: *соціотехнічні системи, загрози, ризики, бізнес-процеси, чинник загрози, ранжування, експертний метод, ймовірність подій, лінгвістичні параметри, параметри загрози, інформаційна безпека.*

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

Roman KARPIUK
Postgraduate Student Cyber Security Department, Franko National University of Lviv, Universytetska str., Lviv, Ukraine, 79000, roman.karpiuk@lnu.edu.ua
ORCID: *0009-0001-0053-1608*

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

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: *0000-0001-6798-5500*
Scopus Author ID: *57189702975*

To cite this article: Korchenko, A, Karpiuk, R, Paraschuk, T., Matsiuk, S. (2023). Metod formuvannia parametriv ta otsiniuvannia zahroz v sotsiotekhnichnykh systemakh [Method of formation of parameters and assessment of threats in sociotechnical systems]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 2, 3–11, doi: https://doi.org/10.32782/IT/2023-2-1

METHOD OF FORMATION OF PARAMETERS AND ASSESSMENT OF THREATS IN SOCIOTECHNICAL SYSTEMS

Every year a significant part of information technology in sociotechnical systems is growing rapidly. And the development of relevant systems directly depends on the relevant information technologies used in the business processes of enterprises. This affects the emergence of new threats, vulnerabilities and attacks that are associated with the information component. The level of implementation of cyberattacks in recent years is growing rapidly. The main target of attacks on sociotechnical systems is personal data, user accounts of the system, trade secrets, medical information, databases, correspondence, payment card data, etc. Also, in order to prevent attacks and identify potential threats, it is necessary to comprehensively use methods for assessing vulnerabilities and threats, modeling possible impacts, as well as world practices and international standards and regulations in the field of information security management. The analysis carried out and the main aspects that are necessary in the formation of parameters for threat assessment are considered, created the basis for substantiating the relevance of the topic of this work. On the basis of the formed aspects, a method of forming parameters and assessing threats in sociotechnical systems has been developed. The method takes into account such parameters as: priority, showing the degree of need to reduce a specific threat; the degree of influence on the system in the implementation of a certain threat; the likelihood of a specific threat in the system; factor of the human component; threat factor, characterizing at the general level the causes that contribute to the occurrence of the threat. Also, the appropriate method, using the obtained parameters, should most fully assess the existing threats in the system and can be applied in the development of a methodology for profiling employees.

Key words: *sociotechnical systems, threats, risks, business processes, threat factor, ranking, expert method, probability of events, linguistic parameters, threat parameters, information security.*

Актуальність проблеми та наліз останніх досліджень і публікацій. З кожним роком значна частина інформаційних технологій в соціотехнічних системах стрімко зростає, оскільки використання їх дозволяє автоматизувати інформаційні процеси, заощадити матеріальні та не матеріальні ресурси, зменшити фінансові ризики, збільшити конкурентоспроможність та інше.

Саме тому, подальший розвиток сучасних соціотехнічних систем безпосередньо залежить від інформаційних технологій (IT), що використ-

товуються в бізнес-процесах підприємств. Але, в свою чергу, це також впливає на появу нових загроз, уразливостей та атак, які пов'язані з інформаційною складовою.

Аналіз останніх аналітичних досліджень (2020 Data Breach Investigations Report; What Does IBM's Cost of a Data Breach…; DDoS Attack Trends for Q3 2021; DDoS Attack Trends for Q4 2021; Cisco Annual Cybersecurity Report 2018; Cisco Annual Cybersecurity Report 2018) від компаній Cisco Systems Inc, DeviceLock, Cloudflare, IBM, Positive Technologies, що займаються інформаційною безпекою або продуктами у цій сфері показують, що рівень кібератак за останні роки стрімко зростає. Головною ціллю атак на соціотехнічні системи є персональні данні, облікові записи користувачів системи, комерційна таємниця, медична інформація, бази даних, переписка, дані платіжних карт тощо.

В роботах (Lacey, 2009; Коцюк; Маслова; Ліпкан, Максименко, Желіховський, 2006; Кравченко, 2018) підтверджуються тенденції зростання кібератак на соціотехнічні системи, та зазначається, що для попередження атак, виявлення потенційних загроз необхідно комплексно використовувати методи щодо оцінювання уразливостей та загроз, моделювання можливих впливів, а також світові практики та міжнародні стандарти і нормативні документи у галузі управління інформаційною безпекою.

Також в роботах (Расторгуєв, Литвиненко, 2014; Дудатьєв, 2014; Методи оцінювання уразливостей та оптимізації інформаційних систем) розглядають особливості функціонування соціотехнічних систем у сучасному довкіллі. Напрям розвитку кожної із частин, соціальної та технічної складової показує, що зовнішні зміни інформаційного довкілля, які відбуваються з великою інтенсивністю, призводять до того, що швидкість зміни довкілля значно пришвидшується, порівняно зі змінами в самій системі. Як наслідок це призводить до появи різних інформаційних уразливостей у інформаційній та соціальній частині системи, якими можуть скористатися неавторизована сторона (НАС).

Виходячи з цього можна зазначити, що дане питання є актуальним і розгляд відповідного напрямку є обґрунтованим та потребує подальшого дослідження. Тому в даній роботі буде розглянуто формування загальних параметрів, які використовуються для опису конкретної загрози від НАС (порушника) в системі, а також за допомогою математичних і експертних методів та теорії множин буде сформовано метод параметрів та оцінювання можливих загроз для соціотехнічних систем.

Метою статті є розробка методу формування параметрів оцінки загроз в соціотехнічних системах. Перед розробкою або модифікацією систем інформаційного захисту важливо проаналізувати та оцінити можливі загрози в соціотехнічних системах. Оскільки визначення основних понять та аспектів дозволить створити параметри загроз та оцінити їх.

Класифікація загроз базується на основі досліджень атак на соціотехнічні системи, моделей порушника та ресурсів, сфери діяльності системи та її активи, організаційної структури та інше. Саме це дозволяє виділити декілька основних груп:

– загальні особливості діяльності та функціонування системи, її поточний стан (територіальне розміщення, особливості діяльності, поточний стан системи та довкілля в якому функціонує система);

– інформаційно-комунікаційні системи (засоби зв'язку, архітектура мережі, комунікаційні вузли, програмно-апаратні комплекси);

– матеріальні та не матеріальні активи системи (конфіденційна інформація, людські ресурси, фінансові активи);

– організаційна структура та процеси взаємодії між співробітниками (організація робочого процесу, бізнес-процеси, ієрархічні взаємозв'язки працівників).

Виходячи з класифікації можна визначити основні складові, які необхідно враховувати при оцінці загроз в соціотехнічних системах:

– імовірність виникнення конкретної загрози;

– ступінь впливу на систему в результаті реалізації загрози;

– критичні ресурси та активи, що є в системі;

– поточний стан соціотехнічної системи;

– бізнес-процеси, що закладені в основі функціонування системи;

– складність реалізації атаки порушником;

– модель порушника;

– структура соціотехнічної системи, її складові та взаємозв'язки між ними.

Основна частина. На базі проведеного аналізу видів загроз і чинників, які можуть впливати при проведенні оцінювання та визначивши основні аспекти загроз в соціотехнічних системах сформуємо параметри та оцінки.

Базуючись на введеній множині оціночних інтервалів ***EI*** для значень параметрів та визначених коефіцієнтах для кожного з інтервалів, які були описанні в (Корченко, Мацюк, Чобаль, 2022), сформуємо таблицю можливих значень всіх оціночних інтервалів *EI*, які експерт буде використовувати при оцінюванні сформованих параметрів загроз (див. табл. 1).

Таблиця 1

Можливі значення оціночного інтервалу

Числові значення	Лінгвістичні значення частоти	Лінгвістичні значення рівня	Коефіцієнт
1–2	Рідко	Дуже низький	0,05
3–4	Іноді	Низький	0,1
5–6	Досить часто	Середній	0,125
7–8	Часто	Вище середнього	0,175
9-10	Дуже часто або завжди	Високий	0,25

Опишемо в загальному виді загрозу $\boldsymbol{T}_i^t$ за допомогою кортежу з параметрами:

$$\boldsymbol{T}_i^t = TN_i, PT_i, DIS_i, FPT_i, HCF_i, TF_i, \quad (1)$$

в якому:

TN_i – назва та опис загрози;

PT_i – пріоритет, що показує ступінь необхідності зменшення конкретної загрози відносно всіх можливих загроз пов'язаних з бізнес-процесами (шкала оцінки від 1 до 10);

DIS_i – ступінь впливу на систему, що характеризує можливість впливу при реалізації конретної загрози (шкала оцінки від «Дуже низький» до «Високий»);

FTP_i – ймовірність реалізації чи реалізація загрози в системі (шкала оцінки від «Дуже низький» до «Високий»);

HCF_i – чинник людської складової (шкала оцінки від «Дуже низький» до «Високий»);

TF_i – чинник, що сприяють виникненню загрози (значення «Контрольовані» чи «Неконтрольовані»).

Оцінки параметрів визначаються експертом або групою експертів на основі проведеного аналізу всіх можливих загроз компанії, що пов'язанні з основними бізнес-процесами. Визначенні експертами оцінки для конкретної загрози повинні відповідати шкалі оцінювання для даної загрози, також процес оцінювання повинен відбуватися максимально об'єктивно.

Пріоритет. Визначення даного параметру відбувається на основі комплексного аналізу всіх загроз, що пов'язанні з бізнес-процесами компанії. Він характеризує ступінь необхідності зменшення конкретної загрози з урахування поточного стану системи, тобто впровадження засобів та методів щодо мінімізації загроз.

Наприклад, при оцінюванні експертом певної загрози, він може аргументувати значення пріоритету:

– впливом зовнішнього довкілля в якому функціонує дана система, тобто економічний, соціальний, екологічний, політичний стан і т. д.;

– внутрішнім станом системи, тобто складом та структурою персоналу їх функціональними обов'язками, поточними бізнес-процесами, критичними ресурсами системи, поточною інформаційною структурою, технічним чи програмним забезпеченням (ПЗ) системи і т. д.

Ймовірність реалізації загрози НАС. Для визначення точної оцінки для даного параметру необхідно проаналізувати систему захисту, провести аналіз критичності ресурсів соціотехнічної системи, можливі загрози з урахуванням моделі порушника та побудувати між ними математичні залежності. На основі аналізу (Ймовірність усвідомлення потенційним зловмисником реальної загрози безпеці) розглянемо поняття моделі порушника, складності реалізації загрози та її оцінки, що дозволить визначити ймовірність реалізації загрози для конкретної системи.

Складність реалізації загрози характеризується тим на скільки довго зможе знаходитись система в стані, коли загроза безпеці є реальною і є можливість для проведення атаки. Щодо урахування аспекту, який описує мінімально необхідну кількість матеріальних та не матеріальних ресурсів (ПЗ, обладнання, час та ресурси необхідні для проведення атаки, практичні навички, фінанси тощо), що необхідні НАС для реалізації атаки. Його оцінка є складною, оскільки наразі активно розвивається нелегальний ринок послуг та засобів реалізації загроз атак і доволі складно оцінити можливості потенційного порушника.

Рівень складності реалізації загрози може характеризуватись мірою невизначеності для потенційного порушника та наявності загрози системі. Математичною основою для такої міри є поняття інформаційної ентропії визначеної К. Шенноном (Николайчук, Воронич, 2010), в свою чергу даний аспект дозволив автору сформувати математичну залежність між складністю реалізації і даним поняттям (Ймовірність усвідомлення потенційним зловмисником реальної загрози безпеці):

$$CTR_i = -\log_2(1 - PSR_i), \quad (2)$$

де PSR_i – величина надійності захисту ресурсу системи, або ймовірність відсутності загрози реалізації атаки в соціотехнічній системі.

В свою чергу, значення можна сформувати та визначити по різному. Для даної роботи пропонується розглянути ймовірність надійності системи захисту ресурсу системи PSR_i, як узагальнюючий параметр на основі:

– цінності ресурсу для соціотехнічної системи з урахуванням моделі порушника та його можливих цілей при доступі в систему;

– надійності системи захисту конкретного ресурсу, тобто ступінь захищеності ресурсу від можливих атак, які були визначанні при побудові політики безпеки соціотехнічної системи.

Позначимо цінність ресурсу як *RV* і, відповідно, ступінь захищеності ресурсу *RP*. При оцінці *RV* та *RP* експерту слід враховувати шкалу оцінки, наприклад, від 1 до 10 для цих параметрів. Далі встановимо залежності між ними у вигляді формули:

$$PSR = \frac{RV}{RP}. \quad (3)$$

Описана залежність між даними параметрами, при яких ймовірність загрози реалізації атаки в соціотехнічній системі була б мінімальною. Це можна показати лінійно, тобто чим цінніший ресурс, тим відповідний захист повинен бути більшим. Розглянемо всі можливі варіанти залежності:

1. При $PV = RP$, поточний стан захищеності ресурсу знаходиться на границі мінімально можливого захисту від реалізації загрози НАС;
2. При $PV < RP$, поточний стан захищеності ресурсу знаходиться в стані, коли чим більше значення *RP* відносно *PV* тим менше вірогідність реалізації загрози;
3. При $PV > RP$, поточний стан захищеності ресурсу знаходиться в стані, коли чим більше значення *PV* відносно *RP* тим більша можливість реалізації загрози НАС.

На основі залежностей сформуємо відповідні формули обрахування ймовірності відсутності загрози реалізації атаки в соціотехнічній системі:

1. При $PV_i \le RP_i$:

$$PSR_i = 1 - PSR_{const} * \frac{RV_i}{RP_i}, \quad (4)$$

де PRS_{const} – гранична ймовірність загрози реалізації атаки в системі (PRS_{const} = 0,5).

2. При $PV_i > RP_i$:

$$PSR_i = PSR_{const} * \frac{RP_i}{RV_i}, \quad (5)$$

де PRS_{const} – гранична ймовірність загрози реалізації атаки в системі (PRS_{const} = 0,5).

Тоді, з урахуванням формул (4) та (5) можна подати формулу (2) як:

1. При $PV_i \ge RP_i$:

$$CTR_i = -\log_2\left(PSR_{const} * \frac{RV_i}{RP_i}\right). \quad (6)$$

2. При $PV_i > RP_i$:

$$CTR_i = -\log_2\left(1 - PSR_{const} * \frac{RP_i}{RV_i}\right). \quad (7)$$

Базуючись на [16] та з урахуванням описаного в цій роботі, ймовірність реалізації загрози порушником *PTR* може бути визначена через складність реалізації певної загрози безпеці НАС на основі виразу (2), що можна записати у вигляді:

$$PTR_i = \frac{1}{2^{CTR_i}}. \quad (8)$$

Розглянемо два приклади формування *PTR.* Нехай оцінки експерта, що описують низку параметрів для першої загрози будуть $RV_1 = 6$ та $PR_1 = 8$, а для другої загрози $RV_2 = 7$ та $PR_2 = 4$.

Оскільки $RV_1 \le PR_1$, тоді формула визначення CTR_1 буде:

$$CTR_1 = -\log_2\left(PSR_{const} * \frac{RV_1}{RP_1}\right) =$$

$$= -\log_2\left(\frac{6}{16}\right) = -\log_2 0,375 = 1,415.$$

В свою чергу $RV_2 > RP_2$, тоді формула визначення CTR_2 буде мати вигляд:

$$CTR_2 = -\log_2\left(1 - PSR_{const} * \frac{RP_2}{RV_2}\right) =$$

$$= -\log_2\left(1 - \frac{4}{14}\right) = -\log_2 0,714 = 0,486.$$

З розрахунків видно, що реалізація успішної атаки на першу загрозу в 2,91 рази складніша, чим на другу. Тепер, визначимо значення PTR_1 та PTR_2:

$$PTR_1 = \frac{1}{2^{CTR_1}} = \frac{1}{2^{1,415}} = 0,375,$$

$$PTR_2 = \frac{1}{2^{CTR_2}} = \frac{1}{2^{0,486}} = 0,714.$$

Дані значення можна також інтерпретувати лінгвістично [18–19] PTR_1 = «Низький», а PTR_2 = «Вище середнього».

Ступінь впливу на систему. Визначення оцінки для певного параметру відбувається на основі можливого впливу на систему після реалізації загрози, що була спричинена порушником.

Сформуємо кортеж параметрів (ймовірність реалізації загрози, складність інфраструктури), які будуть впливати на оцінювання експертом ступеня впливу на систему:

$$DIS_i = CS_i, PSR_i, \quad (9)$$

де CS_i **–** поточний стан системи, ресурсу або активу відносно якого може бути реалізована загроза в певний момент часу;

PSR_i – величина надійності захисту ресурсу системи.

При оцінці CS_i експерту слід враховувати такі складові, як:

1. Бізнес-процеси, що можуть бути пов'язанні або впливати на CS_i, оперуючи поняттями складності процесу, захищеності та доступності;
2. Складність побудови та функціонування соціотехнічної системи й суміжних процесів;
3. Персонал, що обслуговує чи використовує систему, ресурс або актив;
4. Інформаційні ресурси та активи, що можуть стати ціллю НАС;
5. Загальний поточний стан системи.

Мінімальне значення оцінки CS_i на шкалі означає, що поточний стан системи, ресурсу або активу знаходиться в найгіршому положенні за всіма вище описаним складовим і система або її складова потребує максимального вдосконалення. Відповідно до цього, чим вища оцінка тим поточний стан є кращим, шкала оцінки від 1 до 10.

Описавши основні параметри, визначимо ступінь впливу на систему DIS_i і сформуємо в загальному вигляді вираз для певної загрози:

$$DIS_i = CS_i * (1 - PSR_i). \quad (10)$$

Використаємо значення оцінки експерта, що розглядались при ймовірності реалізації загрози. Для першої загрози $RV_1 = 6$, $RP_1 = 8$ та $CS_1 = 5$, а для другої – $RV_2 = 7$, $RP_2 = 4$, та $CS_2 = 8$, тоді:

$$DIS_1 = CS_1 * \left(PSR_{const} * \frac{RV_1}{RP_1} \right) =$$

$$= 5 * \frac{6}{16} = 5 * 0{,}375 = 1{,}875$$

або «Дуже низький»;

$$DIS_2 = CS_2 * \left(1 - PSR_{const} * \frac{RP_2}{RV_2} \right) =$$

$$= 8 * \left(1 - \frac{4}{14} \right) = 5{,}714$$

або «Середній».

З обрахунків видно, що вплив атаки при реалізації другої загрози в 3,05 рази вищий, чим при реалізації першої.

Чинник людської складової. Параметр показує залежність конкретної загрози від людського чинника, яка може бути використана НАС або може впливати на ймовірність реалізації конкретної загрози чи ступінь впливу на систему. Під людською складовою (чинником) розглядається конкретний працівник соціотехнічної системи, що має або може отримати доступ до ресурсів системи, з якими в подальшому буде пов'язана дана загроза.

Значення, які набуває цей параметр є якісними і їх визначає експерт, враховуючи структуру та особливості бізнес-процесів, що можуть бути пов'язаними з відповідною загрозою. Також слід зазначити, що така оцінка є лише загальною й в подальшому спрямована допомогти експерту в ефективному визначенні взаємозалежності між функціональними обов'язками та загрозами, якщо це необхідно.

Чинник загрози. Даний параметр визначає базис, який лежить в основі певної загрози, що в подальшому дозволить більш повно оцінити чинники походження загрози та здатність на них впливати. Значення параметру повинно визначатись на основі попередніх етапів оцінки параметрів і піддаватися контролю за допомогою вживання необхідних заходів по попередженню чи протидії загрозам.

Якщо вживання відповідних заходів не достатньо для зменшення чинників появи загрози або причини її виникнення є випадковими, тоді слід визначати, що чинники загрози є не контрольовані. Також, до випадкових чинників належать ті, для яких необхідні математичні очікування і дисперсії для визначення даних випадкових величин.

В свою чергу чинники, появи загрози, які можна визначити, описати та в подальшому оцінити називаються контрольовані. При створенні і оцінці загроз системи необхідно кожному експерту максимально точно описувати чинники, що лежать в основі загроз, тобто максимальна кількість існуючих загроз повинна бути визначена параметром «Контрольовані».

Саме вище описанні параметри дозволять максимально точно та об'єктивно провести оцінювання складової кортежу $\boldsymbol{T}_i^t$. Розглянемо множину можливих загроз, яку визначмо у вигляді:

$$\boldsymbol{T}^t = \left\{ \bigcup_{i=1}^{n} \boldsymbol{T}_i^t \right\} =$$

$$\left\{ \boldsymbol{T}_1^t, \boldsymbol{T}_2^t, \boldsymbol{T}_3^t, \ldots, \boldsymbol{T}_n^t \right\}, \ \left(i = \overline{1,n} \right), \quad (11)$$

де n **–** визначає кількість всіх можливих загроз для певної соціотехнічної системи.

Відповідно до формули (11) при m = 11 розглянемо список загроз для певної компанії:

$$\boldsymbol{T}^t = \left\{ \bigcup_{i=1}^{11} \boldsymbol{T}_i^t \right\} = \left\{ \boldsymbol{T}_1^t, \boldsymbol{T}_2^t, \boldsymbol{T}_3^t, \ldots, \boldsymbol{T}_{11}^t \right\}.$$

Далі, опишемо кожну загрозу $\boldsymbol{T}_i^t$ з використанням формули (1) у вигляді кортежу з параметрами *TN*, *PT*, *DIS*, *PTR*, *HCF*, *TF* враховуючи межі шкал кожного із параметрів:

– $\boldsymbol{T}_1^t = TN_1, PT_1, DIS_1, PTR_1, HCF_1, TF_1 =$
$\langle TN_1, 5, «Вище середнього», «Низький», «Низький», «Контрольовані» \rangle$;

– $\boldsymbol{T}_2^t = TN_2, PT_2, DIS_2, PTR_2, HCF_2, TF_2 =$
$\langle TN_2, 7, «Високий», «Середній», «Високий», «Контрольовані» \rangle$;

– $\boldsymbol{T}_3^t = TN_3, PT_3, DIS_3, PTR_3, HCF_3, TF_3 =$
$\langle TN_3, 7, «Низький», «Вище середнього», «Середній», «Контрольовані» \rangle$;

– $\boldsymbol{T}_4^t = TN_4, PT_4, DIS_4, PTR_4, HCF_4, TF_4 =$
$\langle TN_4, 8, «Високий», «Середній», «Високий», «Не контрольовані» \rangle$;

– $\boldsymbol{T}_5^t = TN_5, PT_5, DIS_5, PTR_5, HCF_5, TF_5 =$
$\langle TN_5, 9, «Вище середнього», «Середній», «Високий», «Контрольовані» \rangle$;

– $\boldsymbol{T}_6^t = TN_6, PT_6, DIS_6, PTR_6, HCF_6, TF_6$

$\boldsymbol{T}_8^t = TN_8, PT_8, DIS_8, PTR_8, HCF_8, TF_8 =$
$\langle TN_8, 7, «СЕРЕДНІЙ», «Середній», «Середній», «Контрольовані» \rangle$;

– $\boldsymbol{T}_9^t = TN_9, PT_9, DIS_9, PTR_9, HCF_9, TF_9 =$
$\langle TN_8, 7, «Дуже низький», «Середній», «Високий», «Контрольовані» \rangle$;

– $\boldsymbol{T}_{10}^t = TN_{10}, PT_{10}, DIS_{10}, PTR_{10}, HCF_{10}, TF_{10} =$
$\langle TN_{10}, 4, «Вище середнього», «Низький», «Середній», «Контрольовані» \rangle$;

– $\boldsymbol{T}_{11}^t = TN_{11}, PT_{11}, DIS_{11}, PTR_{11}, HCF_{11}, TF_{11} =$
$\langle TN_{11}, 3, «Вище середнього», «Дуже низький», «Низький», «Не контрольовані» \rangle$.

Таблиця 2

Приклад можливих загроз

Номер загрози (*i*)	Назва загрози (*TN*)	Пріоритет (*PT*)	Ступінь впливу на систему (*DIS*)	Ймовірність реалізації загрози НАС (*PTR*)	Чинник людської складової (*NCF*	Чинник загрози (*TF*)
1	Отримання доступу до внутрішньої поштової системи	5	Вище середнього	Низький	Низький	Контрольовані
2	Отримання доступу до інформації (документів, носіїв, засобів зберігання) пов'язаних з КІ	7	Високий	Середній	Високий	Контрольовані
3	Отримання доступу до робочого телефону	7	Низький	Вище середнього	Середній	Контрольовані
4	Соціальний інжиніринг персоналу	8	Високий	Середній	Високий	Не контрольовані
5	Отримання доступу до знищених документів чи ресурсів	9	Вище середнього	Середній	Високий	Контрольовані
6	Отримання доступу до внутрішньої системи документообігу та суміжних ресурсів	4	Високий	Низький	Середній	Контрольовані
7	Витік інформації про систему через відкриті інформаційні ресурси	6	Низький	Середній	Високий	Контрольовані
8	Отримання інформації про структуру, особливості функціонування системи	7	Середній	Середній	Середній	Контрольовані
9	Викрадення чи отримання дублікату ключа карти	7	Дуже низький	Середній	Високий	Контрольовані
10	Викрадення персональних даних персоналу системи	4	Вище середнього	Низький	Середній	Контрольовані
11	Втрата інформації через стихійні лиха природнього чи техногенного характеру	3	Вище середнього	Дуже низький	Низький	Не контрольовані

Описані приклади кортежів загроз для даної компанії визначмо в таблиці додавши назву/ описання кожної із них (див. табл. 2).

Описана таблиця дозволяє отримати характеристику певної загрози на базі описаних параметрів, показати відношення між загрозами та встановити певні залежності між параметрами і типом загрози.

Висновки. Оцінка загроз та ризиків в соціотехнічних системах є питанням не новим, але важливим оскільки на даний момент кількість атак на інформаційні системи, що пов'язані з існуючими загрозами та ризиками зростає. Тому запропонований метод формування параметрів та оцінювання загроз повинен найбільш повно оцінити існуючі загрози системі (встановити чинник загрози, ступінь впливу на соціотехнічну систему, пріоритет, ймовірність реалізації загрози, чинник людської складової). Даний метод може використовуватись при розробці методології профілювання співробітників.

ЛІТЕРАТУРА:

1. 2020 Data Breach Investigations Report. URL: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf (дата звернення: 22.12.2022).

2. What Does IBM's Cost of a Data Breach Report 2021 Mean for Businesses? URL: https://www.transpere.com/blog/ibm-data-breach-report-2021/ (дата звернення: 22.12.2021).

3. DDoS Attack Trends for Q3 2021. URL: https://blog.cloudflare.com/ddos-attack-trends-for-2021-q3/ (дата звернення: 26.12.2022).

4. DDoS Attack Trends for Q4 2021. URL: https://blog.cloudflare.com/ddos-attack-trends-for-2021-q4/ (дата звернення: 26.12.2022).

5. Cisco Annual Cybersecurity Report 2018. URL: https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf (дата звернення: 28.12.2022).

6. Cisco Annual Cybersecurity Report 2018. URL: https://www.cisco.com/c/dam/m/en_hk/ciscolive/2020-ciso-benchmark-cybersecurity-series.pdf (дата звернення: 28.12.2022).

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

8. 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: 20.09.2022).

9. 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: 20.09.2022).

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

11. Кравченко С. І. Безпека соціотехнічних систем. *НБІ технології*. 2018.

12. Расторгуєв В.П., Литвиненко М.В. Інформаційні операції в мережі / В.П. Расторгуєв, М.В. Литвиненко. АНО ЦСОІП, 2014. 128 с.

13. Дудатьєв А.В. Теоретичні аспекти та технології керованого хаосу для реалізації комплексного інформаційного захисту соціотехнічних систем. *Інформаційні технології та комп'ютерна інженерія*. 2014. № 2 (30). С. 28–32.

14. Методи оцінювання уразливостей та оптимізації інформаційних систем в умовах інформаційних впливів. URL: https://er.nau.edu.ua/bitstream/NAU/14308/1/Диссер.pdf (дата звернення: 23.09.2022).

15. Метод формування параметрів функціональних обов'язків для оцінки загроз в соціотехнічних системах / А. Корченко, С. Мацюк, О. Чобаль, О. Кручінін, Т. Паращук. Information Technology: Computer Science. *Software Engineering and Cyber Security*. 2022. № 3. С. 19–26.

16. Ймовірність усвідомлення потенційним зловмисником реальної загрози безпеці. URL: https://studme.org/180232/informatika/veroyatnost_realizatsii_potentsialnym_narushitelem_realnoy_ugrozy_bezopasnosti.

17. Николайчук, Я.М., Воронич А. Р. Теоретичні основи мір ентропії їх застосування в інформаційних технологіях формування та опрацювання сигналів. *Оптико-електронні інформаційно-енергетичні технології*. 2010. № 1. С. 50–63.

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

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

REFERENCES:

1. 2020 Data Breach Investigations Report. URL: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf (data zvernennia: 22.12.2022).

2. What Does IBM's Cost of a Data Breach Report 2021 Mean for Businesses? URL: https://www.transpere.com/blog/ibm-data-breach-report-2021/ (data zvernennia: 22.12.2021).

3. DDoS Attack Trends for Q3 2021. URL: https://blog.cloudflare.com/ddos-attack-trends-for-2021-q3/ (data zvernennia: 26.12.2022).

4. DDoS Attack Trends for Q4 2021. URL: https://blog.cloudflare.com/ddos-attack-trends-for-2021-q4/ (data zvernennia: 26.12.2022).

5. Cisco Annual Cybersecurity Report 2018. URL: https://www.cisco.com/c/dam /m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf (data zvernennia: 28.12.2022).

6. Cisco Annual Cybersecurity Report 2018. URL: https://www.cisco.com/c/dam /m/en_hk/ciscolive/2020-ciso-benchmark-cybersecurity-series.pdf (data zvernennia: 28.12.2022).

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

8. 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: 20.09.2022).

9. 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: 20.09.2022).

10. 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).

11. Kravchenko S. I. Bezpeka sotsiotekhnichnykh system. *NBI tekhnolohii*. 2018. T. 12. № 2.

12. Rastorhuiev V.P., Lytvynenko M.V. Informatsiini operatsii v merezhi / V.P. Rastorhuiev, M.V. Lytvynenko. *ANO TsSOIP.* 2014. 128 s.

13. Dudatiev A.V. Teoretychni aspekty ta tekhnolohii kerovanoho khaosu dlia realizatsii kompleksnoho informatsiinoho zakhystu sotsiotekhnichnykh system. *Informatsiini tekhnolohii ta kompiuterna inzheneriia.* 2014. № 2 (30). S. 28–32.

14. Metody otsiniuvannia urazlyvostei ta optymizatsii informatsiinykh system v umovakh informatsiinykh vplyviv. URL: https://er.nau.edu.ua/bitstream/NAU/14308/1/Диссер.pdf (data zvernennia: 23.09.2022).

15. Korchenko A. Metod formuvannia parametriv funktsionalnykh oboviazkiv dlia otsinky zahroz v sotsiotekhnichnykh systemakh / A. Korchenko, S. Matsiuk, O. Chobal, O. Kruchinin, T. Parashchuk. Information Technology: Computer Science. *Software Engineering and Cyber Security*. 2022. № 3. S. 19–26.

16. Ymovirnist usvidomlennia potentsiinym zlovmysnykom realnoi zahrozy bezpetsi. URL: https://studme.org/180232/informatika/veroyatnost_realizatsii_potentsialnym_narushitelem_realnoy_ugrozy_bezopasnosti.

17. Nykolaichuk, Ya.M. Teoretychni osnovy mir entropii yikh zastosuvannia v informatsiinykh tekhnolohiiakh formuvannia ta opratsiuvannia syhnaliv. *Optyko-elektronni informatsiino-enerhetychni tekhnolohii*. 2010. № 1. S. 50–63.

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

19. Anna Korchenko, Metody identyfikatsii anomalnykh staniv dlia system vyiavlennia vtorhnen : Monohrafiia, Kyiv : TsP "Komprynt", 2019. 361 s.