КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.691
УДК 004.94/.6-044.3-028.6:510.3

Дрейс Юрій Олександрович
к.т.н., доцент, доцент системного аналізу та інформаційних технологій
Маріупольський державний університет, Київ, Україна
ORCID ID: 0000-0003-2699-1597
y.dreis@mu.edu.ua

МОДЕЛЬ ПАРАМЕТРІВ ОЦІНЮВАННЯ НАСЛІДКІВ ВИТОКУ СЛУЖБОВОЇ ІНФОРМАЦІЇ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. Існує проблема між ефективністю забезпечення стійкого і безперервного функціонування об'єкта критичної інфраструктури у процесі надання ним основних послуг та/або життєво важливих функцій і ефективністю реалізованих методів, засобів та заходів, які не забезпечують достатнього рівня захисту об'єктів критичної інформаційної інфраструктури і, як наслідок, призводять до витоку інформації з обмеженим доступом, особливо, службової інформації. Для її вирішення було проведено аналіз видів відповідальності у разі розголошення службової інформації, класифікованих величиною нанесеної істотної шкоди або тяжких наслідків. Встановлені критерії обмеження доступу та класифікації видів інформації з обмеженим доступом, особливо, для службової інформації, як «трискладового тесту» на визначення відповідного інтересу, мети та її призначення, шкоди у разі розголошення та її противаги до суспільного інтересу у оприлюдненні. На основі проведеного дослідження переліку службової інформації окремого об'єкта критичної інфраструктури, розроблено базову модель, яка за рахунок інтегрованого теоретико-множинного представлення множин, що характеризують параметри обмеження у доступі, об'єкта відомостей, його сукупність чи окремі показники, гриф, строки та види маркування матеріальних носіїв службової інформації тощо, дозволяє відповідно до вимог чинного законодавства визначити множини вхідних та вихідних компонент для формування набору параметрів оцінювання наслідків її витоку. Також побудована ієрархічна структура даної кортежної моделі параметрів оцінювання наслідків витоку службової інформації об'єкта критичної інфраструктури для структуризації вхідних і вихідних даних. У подальшому, для проведення експериментального дослідження та практичної реалізації зазначеного вище процесу необхідно розробити метод оцінювання наслідків витоку службової інформації об'єкта критичної інфраструктури.

Ключові слова: об'єкт критичної інфраструктури; наслідки витоку службової інформації; модель параметрів оцінювання наслідків.

ВСТУП

Відповідно до закону [1], службовою інформацією (СлІ) є та, що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень, а також інформація зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці. Основною нормою, яка повинна застосовуватись в усіх без винятку випадках, коли обмежується доступ до публічної інформації, є частина друга статті 6 Закону України «Про доступ до публічної інформації», яка встановлює вимоги,

при дотриманні яких здійснюється обмеження доступу до публічної інформації, так званий «трискладовий тест» [1]:

- виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;
- розголошення інформації може завдати істотної шкоди цим інтересам;
- шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

«Трискладовий тест» обов'язково застосовується у таких випадках [2], [3]: при «первинному» віднесенні певних відомостей до таємної інформації; при «первинному» віднесенні певних відомостей до СлІ; при вирішенні питання надання чи відмови в доступі стосовно конкретної інформації (документу); при реєстрації в системі обліку публічної інформації з обмеженим доступом (ІзОД), якою розпорядник володів на момент набуття чинності Закону [2]; у всіх інших випадках, коли вирішується питання обмеження доступу до публічної інформації. Як наслідок, на основі використання даного «трискладового тесту», органи виконавчої влади мають затвердити переліки відомостей, що становлять службову інформацію (далі — ПСлІ), та оприлюднити їх в установленому порядку, згідно до Указу [4].

Щодо можливості урахування «*інтересів*» держави, наприклад, у сфері охорони ДТ під час проведення експертизи матеріальних носіїв інформації на наявність чи відсутність у них відомостей, що становлять державну таємницю, враховано у [5], [6].

Розмір «*істотної шкоди*», необхідної для притягнення до кримінальної відповідальності, відповідно до п.3 примітки до ст. 364 КК України визначається у сто і більше разів перевищує неоподатковуваний мінімум доходів громадян, а «*тяжких наслідків*» — у двісті п'ятдесят і більше разів перевищують неоподатковуваний мінімум доходів громадян (становить 17 грн., за винятком норм адміністративного та кримінального законодавства у частині кваліфікації злочинів або правопорушень, для яких сума неоподатковуваного мінімуму встановлюється на рівні податкової соціальної пільги, визначеної підпунктом 169.1.1 пункту 169.1 статті 169 розділу IV ПКУ для відповідного року, яка дорівнює 50 відсоткам розміру прожиткового мінімуму для працездатної особи). Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять СлІ, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, що призвело до розголошення такої інформації, також є адміністративним правопорушенням (ст. 212-5 КУпАП) та тягне за собою накладення штрафу на громадян від двадцяти до сорока неоподатковуваних мінімумів доходів громадян і на посадових осіб — від шістдесяти до ста шістдесяти неоподатковуваних мінімумів доходів громадян. Розміри штрафу, «*істотної шкоди*» та «*тяжких наслідків*» за видом відповідальності за розголошення СлІ у період з 2019 по 2024 рік, визначених згідно до законодавства, приведено у табл. 1 [7].

Таблиця 1

Розміри штрафу, «*істотної шкоди*» та «*тяжких наслідків*» за видом відповідальності за розголошення СлІ у період з 2019 по 2024 рік

Розмір шкоди, наслідків та штрафу за видом відповідальності за розголошення СлІ (тис. грн.)		2019	2020	2021	2022	2023	2024
адміністративна	для громадян	19÷38	22÷44	24÷48	26÷52	27÷54	30÷60
	для посадових осіб	57÷154	66÷176	72÷190	78÷208	81÷215	90÷242
кримінальна	«*істотна шкода*»	>96	>110	>119	>130	>134	>151
	«*тяжкі наслідки*	>240	>275	>297	>325	>335,5	>378,5

Постановка проблеми. За останні роки стрімко зростають обсяги службової інформації (СлІ), що накопичуються, зберігаються та використовуються у професійній діяльності на ОКІ. При цьому надмірна концентрація СлІ спеціального призначення та приналежності, а також різке розширення кола користувачів, що мають безпосередній доступ до цієї інформації, породжує проблему забезпечення її захисту від можливої втрати чи розголошення. Підвищення рівня складності методів і засобів добування СлІ, а також існуючі способи використання інформаційних технологій призводять до появи реальних та потенційних загроз в інформаційній сфері для ОКІІ. Реалізація цих загроз може призвести до витоку СлІ та нанесення можливої шкоди ОКІ та/або державі. Величина такої шкоди зазвичай важко формалізована, нечітко визначена і, при необхідності визначення її у процедурі віднесення відомостей до СлІ, має містити набір базових ідентифікуючих та оціночних параметрів. Одним із підходів до вирішення такого завдання є використання відповідних моделей, методів та систем, які основі на використання нечітких множин, орієнтованих на обробку слабо структурованих даних з метою встановлення фактів нанесення шкоди, наприклад, від витоку таких видів ІзОД як таємної (ДТ), конфіденційної (у т.ч. персональних даних) або СлІ.

Однак існує *проблема* між ефективністю забезпечення стійкого і безперервного функціонування ОКІ у процесі надання ним основних послуг та/або життєво важливих функцій і ефективністю реалізованих методів, засобів та заходів, які не забезпечують достатнього рівня захисту ОКІІ, як наслідок, призводять до витоку ІзОД, особливо СлІ, на ОКІ. Вирішення цієї проблеми можливе шляхом розробки нових моделей, методів та засобів, які дозволяють формалізувати процес класифікації ІзОД за набором базових параметрів представлення можливої шкоди для ОКІ (установи, відомства) у разі витоку СлІ, оцінювання ризиків та можливих потенційних наслідків реалізації кібератаки на його ОКІІ за для своєчасної їх мінімізації та ліквідації, з метою своєчасного виявлення, запобігання і нейтралізацію загроз безпеці ОКІ та підтримки стану захищеності ОКІІ на такому рівні, за якого забезпечується безперервність функціонування і стійкість надання ОКІ основних послуг та/або життєво важливих функцій, що є однією з *найактуальніших науково-технічних задач сьогодення*.

Аналіз останніх досліджень і публікацій. У даному досліджені проведено аналіз наукових праць вітчизняних вчених у яких започатковано розв'язання проблеми з одного боку, — щодо методологічних, організаційних та юридичних засад забезпечення захисту СлІ, її класифікації (М. Лациба, О. Огданська, І. Касперський, Т. Ткачук, І. Гуменюк та ін.) [2], [3], [7] – [11], а з іншого, — щодо побудови систем, методів, засобів та заходів забезпечення захисту ІзОД та оцінювання ризиків (О. Корченко, С. Казмірчук, Є. Іванченко, В. Мохор, С. Гончар, С. Гнатюк та ін.) [5], [6], [12] – [25], а також інших законодавчих актів [1] та указів [4], правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах [26], деякі питання ОКІ [27] та ОКІІ [28], окремих переліків СлІ на ОКІ [29], типової

інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію [30].

Метою роботи є розробка моделі параметрів оцінювання наслідків витоку СлІ на ОКІ для своєчасної їх мінімізації та ліквідації, як способу попередження, виявлення, запобігання і нейтралізації загроз безпеці ОКІ та підтримки стану захищеності ОКІІ на рівні, за якого забезпечується безперервність функціонування і стійкість надання основних послуг та/або життєво важливих функцій.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Модель параметрів оцінювання наслідків витоку СлІ на ОКІ

Для вирішення поставленого завдання розроблено модель формування параметрів оцінювання наслідків витоку СлІ на ОКІ, як базову кортежну модель, основу якої становить кортеж, що складається з ідентифікатора виду ІзОД, на прикладі СлІ, а також інші компоненти, як підмножини з: нечітких (лінгвістичних) еталонів, поточних значень нечітких параметрів, базових детекційних правил у т. ч. і класифікації інформації, можливих ідентифікаційних та оціночних параметрів тощо.

Так відповідно до законодавства [1], [26], інформація (*Information*) *I* за порядком доступу поділяється на відкриту та ІзОД, тобто в її основні міститься ідентифікатори як:

$$\boldsymbol{I} = \langle \boldsymbol{I}_1, ..., \boldsymbol{I}_i, ..., \boldsymbol{I}_n \rangle, \quad (1)$$

де $I_i \subseteq I \ \ (i = \overline{1,n})$ — компонент кортежу, що відображає *i*-й ідентифікатор видів інформації, де *n* - їх кількість, а для всіх членів I характерна властивість порядку.

Наприклад, відповідно до [1], [11], [17], [26], формування переліку існуючих видів інформації в Україні, при *n* = 2 визначимо кортеж (1) як:

$$\boldsymbol{I} = \langle \boldsymbol{I}_1, \boldsymbol{I}_2 \rangle = \langle \boldsymbol{PI}, \boldsymbol{RI} \rangle,$$

де $I_1 = PI$ (множина ідентифікаторів відкритої інформації (*Public Information*)); $I_2 = RI$ (множина ідентифікаторів ІзОД (*Restricted Information*)).

Далі, для формалізації процесу формування ідентифікаторів *RI*, введемо множину можливих видів ІзОД, витік (втрата чи розголошення) якої може нанести шкоду національній безпеці України як [11], [17]:

$$\boldsymbol{RI} = \langle \boldsymbol{RI}_1, \boldsymbol{RI}_2, ..., \boldsymbol{RI}_i, ..., \boldsymbol{RI}_n \rangle, \quad (2)$$

де $RI_i \subseteq RI \ \ (i = \overline{1,n})$ — компонент кортежу, що відображає *i*-й ідентифікатор видів ІзОД, де *n* їх кількість, а для всіх членів I характерна властивість порядку.

Наприклад, відповідно до [1], [11], [17], [26], формування переліку існуючих видів ІзОД в Україні, при *n* = 3 кортеж (2) визначимо як:

$$\boldsymbol{RI} = \langle \boldsymbol{RI}_1, \boldsymbol{RI}_2, \boldsymbol{RI}_3 \rangle = \langle \boldsymbol{CI}, \boldsymbol{OI}, \boldsymbol{IS} \rangle,$$

де $RI_1 = CI$ (множина ідентифікаторів конфіденційної інформації (*Confidential Information*)); $RI_2 = OI$ (множина ідентифікаторів СлІ (*Official Information*)); $RI_3 = IS$ (множина ідентифікаторів таємної інформації (*Secret Information*), наприклад, ДТ [6], [12], [17] – [19]).

Далі для формалізації процесу формування параметрів СлІ, введемо множину можливих ідентифікаторів, які використовуються для її класифікації і оцінювання як:

$$\boldsymbol{OI} = \langle \boldsymbol{OI}_1, \boldsymbol{OI}_2, ..., \boldsymbol{OI}_i, ..., \boldsymbol{OI}_n \rangle, \quad (3)$$

де $OI_i \subseteq OI \ \ (i = \overline{1,n})$ — компонент кортежу, що відображає *i*-й ідентифікатор параметру, *n* їх кількість, а для всіх членів *OI* характерна властивість порядку.

Наприклад, для формування переліку параметрів СлІ відповідно до [за [1] – [3], [11], [17], при *n* = 5 вираз (3) визначимо наступний кортеж як:

$$\boldsymbol{OI} = \langle \boldsymbol{OI}_1, \boldsymbol{OI}_2, \boldsymbol{OI}_3, \boldsymbol{OI}_4, \boldsymbol{OI}_5, \boldsymbol{OI}_6 \rangle = \langle \boldsymbol{L}, \boldsymbol{R}, \boldsymbol{T}^e, \boldsymbol{DR}^l, \boldsymbol{P}_{\boldsymbol{T}}^{\tau_f}, \boldsymbol{V} \rangle, \quad (4)$$

де $\boldsymbol{OI}_1 = \boldsymbol{L}$ — множина можливих ідентифікаторів, що характеризує наявність СлІ на ОКІ; $\boldsymbol{OI}_2 = \boldsymbol{R}$ — множина можливих параметрів, що використовуються для визначення СлІ, наприклад, «трискладовий тест»; $\boldsymbol{OI}_3 = \boldsymbol{T}^e$ — множина можливих нечітких (лінгвістичних) еталонів, що відображають судження експерта відносно наявності базових параметрів можливої шкоди (по типу процедури віднесення відомостей до IS) із підмножини R для обмеження доступу; $\boldsymbol{OI}_4 = \boldsymbol{DR}^l$ — множина базових детекційних правил, причинно-наслідкових і просторово-часових характеристик та ознак для СлІ; $\boldsymbol{OI}_5 = \boldsymbol{P}_{\boldsymbol{T}}^{\tau_f}$ — множина поточних значень нечітких параметрів, сформованих на основі T_i^e у момент часу τ_f ($f = \overline{1,max_\tau}$) за часовий проміжок $\tau_h = \tau_f - \tau_{f-1}$; $\boldsymbol{OI}_6 = \boldsymbol{V}$ — множина ідентифікаторів, що використовуються для обмеження доступу до СлІ.

Перший компонент кортежу $\boldsymbol{L}$ — перелік (*List*) СлІ ОКІ може бути представлений у вигляді множини розділів і множини статей у них, сформованих за тематикою як:

$$L = \{\bigcup_{i=1}^{r_1} \{L_i\}\} = \{\{L_1\}, \{L_2\}, .., \{L_{r_1}\}\}, \quad (5)$$

де $L_i \subseteq L \ \ (i = \overline{1,r_1})$ — *i*-та підмножина ідентифікаторів розділів у переліку СлІ ОКІ, а r_1 — загальна кількість груп.

Наприклад, з урахуванням [29] при $r_1 = 6$ $(i = \overline{1,6})$ на основі (5) L представимо як:

$$L = \{\bigcup_{i=1}^{6} \{L_i\}\} = \{\{L_1\}, \{L_2\}, \{L_3\}, \{L_4\}, \{L_5\}, \{L_6\}\} =$$

$$= \{\{"1"\}, \{"2"\}, \{"3"\}, \{"4"\}, \{"5"\}, \{"6"\}\} =$$

$$= \{\{"Загальні відомості"\}, \{"Відомості з питань національної безпеки, освіти і економіки"\}, \{"Відомості з питань науки і технологій"\}, \{"Відомості з питань мобілізаційної підготовки і мобілізації"\}, \{"Відомості з питань режимно-секретної діяльності"\}, \{"Відомості з питань технічного захисту інформації"\}\}.$$

Для *i*-ї підмножини L_i визначимо як:

$$L_i = \{\bigcup_{j=1}^{r_{1i}} L_{ij}\} = \{L_{i1}, L_{i2}, ..., L_{i_{n_i}}\}, \quad (6)$$

де $L_{i.j} \subseteq L_i \ \ (j = \overline{1,r_{1_i}})$ — ідентифікатори статей *i*-го розділу, а r_{1_i} — їх кількість. З урахуванням (6) вираз (5) можна представити у такому вигляді:

$$L = \{\bigcup_{i=1}^{r_1} L_i\} = \{\bigcup_{i=1}^{r_1}\{\bigcup_{j=1}^{r_{1_i}} L_{i.j}\}\} = \{\{L_{1.1}, L_{1.2}, ..., L_{1.r_{11}}\}, \{L_{2.1}, L_{2.2}, ..., L_{2.r_{12}}\}, ..., \{L_{r_1.1}, L_{r_1.2}, ..., L_{r_1.r_{1_1}}\}\}, (i = \overline{1, r_1}), (j = \overline{1, r_{1_i}}). \quad (7)$$

Наприклад, з урахуванням [29] при $r_1 = 1$ $(i = 4)$ та $r_{1_4} = 6$ $(j = \overline{1,6})$ на основі (7) L представимо як:

$$L = \{\bigcup_{i=4}^{4}\{\bigcup_{j=1}^{6} L_{4.j}\}\} = \{\{L_{4.1}\}, \{L_{4.2}\}, \{L_{4.3}\}, \{L_{4.4}\}, \{L_{4.5}\}, \{L_{4.6}\}\} =$$

$$= \{\{"4.1."\}, \{"4.2."\}, \{"4.3."\}, \{"4.4."\}, \{"4.5."\}, \{"4.6."\}\} =$$

={{"Відомості за окремими показниками про заходи мобілізаційної підготовки та мобілізації в цілому щодо Міністерства освіти і науки України"}, {"Відомості за окремими показниками про організацію оповіщення, зв'язку, управління мобілізацією, порядку, термінів виконання заходів мобілізації щодо Міністерства"}, {"Відомості за сукупністю всіх показників про заходи мобілізаційної підготовки та мобілізації в цілому щодо закладу освіти, підприємства, установи, організації"}, {"Відомості за окремими показниками щодо розпорядження бюджетними коштами для фінансуванням заходів мобілізаційної підготовки, розголошення яких може завдати шкоди інтересам національної безпеки та оборони держави, в цілому щодо закладу освіти, підприємства, установи, організації"},{"Відомості про військовозобов'язаних, забронюваних за галуззю освіти і науки України"}, {"Відомості про мобілізаційні завдання, визначені для галузі освіти і науки України, у цілому щодо Міністерства освіти і науки України, обласної, Київської міської державних адміністрацій"}.

Наступний компонент кортежу ***R*** — множина можливих параметрів, що використовуються для визначення СлІ, наприклад, "трискладовий тест" у вигляді як:

$$R = \{\bigcup_{i=1}^{r_2}\{R_i\}\} = \{\{R_1\}, \{R_2\}, ..., \{R_{r_2}\}\}, \quad (8)$$

де $R_i \subseteq R$ $(i = \overline{1, r_2})$ — ідентифікатор законної вимоги на обмеження доступу до публічної інформації, а r_2 — кількість таких вимог. Відповідно до [1], в Україні наявні три вимоги на обмеження доступу до публічної інформації, тобто це вимоги «трискладового тесту».

Наприклад, при $r_2 = 3$ $(i = \overline{1,3})$ з урахуванням [1] формула (8) набуде вигляду:

$$R = \{\bigcup_{i=1}^{3}\{R_i\}\} = \{\{R_1\}, \{R_2\}, \{R_3\}\} =$$

$$= \{\{"1"\}, \{"2"\}, \{"3"\}\} =$$

={{"виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя"}, {"розголошення інформації може завдати істотної шкоди цим інтересам"}, {"шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні"}.

Третій компонент кортежу T^e — множина можливих нечітких (лінгвістичних) еталонів, що відображають судження експерта відносно застосування вимог R та наявності базових параметрів можливої шкоди (по типу процедури віднесення відомостей до IS [6], [12]) для обмеження доступу цієї інформації і відображається як:

$$T^e = \{\bigcup_{i=1}^{r_3}\{T_i^e\}\} = \{\{T_1^{e_1}\},\{T_2^{e_2}\},\ldots,\{T_{r_3}^{e_{r_2}}\}\}, \quad (9)$$

де $T_i^e \subseteq T^e$ $(i=\overline{1,r_3})$ — ідентифікатор нечітких (лінгвістичних) еталонів, що відображають *i*-те судження експерта відносно вимоги *R*, а r_3 — їх кількість для $e = r_2$.

Наприклад, з урахуванням [1] для $r_2 = 3$ $(i=\overline{1,3})$, при $r_3 = 1$ $(i=1)$ та $e = r_2$ формула (9) набуде вигляду:

$$T = \{\bigcup_{i=1}^{r_3}\{T_i^{R_i}\}\} = \{\{T_1^{R_1}\},\{T_1^{R_2}\},\{T_1^{R_3}\}\} =$$

= {{"*наявний, відповідають* вимозі R_1"},{"*завдає* за вимогою R_2"},{"*значно та/або суттєво* за вимогою R_3"}} = {{"*наявний* інтерес національної безпеки, територіальної цілісності або громадського порядку), а мета та призначення *відповідають* для запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя)"}, {"її розголошення *завдає* істотної шкоди цим інтересам"}, {"шкода від оприлюднення такої інформації *значно та/або суттєво* переважає суспільний інтерес в її отриманні"}.

Четвертий компонент кортежу DR^l — множина базових детекційних правил, причинно-наслідкових ознак і просторово-часових характеристик для СлІ, показано як:

$$DR^l = \{\bigcup_{i=1}^{r_4}\{DR_i^l\}\} = \{\{DR_1^{l_1}\},\{DR_2^{l_2}\},\ldots,\{DR_{r_4}^{l_{r_1 i}}\}\}, \quad (10)$$

де $DR_i^l \subseteq DR^l$ $(i=\overline{1,r_4})$ — ідентифікатор базових детекційних правил, причинно-наслідкових ознак і просторово-часових характеристик *OI*, а r_4 — їх кількість для $l = r_{1_{i.j}}$.

Як відомо з [29], що за кожною статтею L_i у переліку чи зводу відомостей, що становлять СлІ наявний об'єкт цих відомостей, його характеристики, або/та його окремі показники чи їх сукупність тощо. Наприклад, з урахуванням [29] при $r_{1_i} = 1$ $(i=4)$ та $r_{1_{4.j}} = 1$ $(j=1)$ та $l = r_{1_{4.1}}$ для $r_4 = 4$ $(i=\overline{1,4})$, формула (10) набуде вигляду:

$$DR = \{\bigcup_{i=1}^{4}\{DR_i^{r_{1i.j}}\}\} = \{\{DR_1^{r_{14.1}}\},\{DR_2^{r_{14.1}}\},\{DR_3^{r_{14.1}}\},\{DR_4^{r_{14.1}}\}\} = \{\{Ob\},\{In\},\{Op\},\{Co\}\},$$

де *Ob* = {"*object*"} = {"про заходи мобілізаційної підготовки та мобілізації"}; *In* = {{"*indicators*"} = {"щодо Міністерства освіти і науки"}; *Op* = {"*options for Ob*"} = {"за окремими показниками"}; *Co* = {"*conditions for In*"} = {"в цілому"}.

Наступний компонент кортежу $\boldsymbol{P}^{l}_{\tau_f}$ — множина параметрів часового обмеження у доступі до L_i, сформованих на основі T^e_i як встановлений строк експертною комісією τ_f ($f=\overline{1,max_\tau}$), що відображається як:

$$P^l_{\tau_f}=\{\bigcup_{i=1}^{r_5}\{P^l_{\tau_f i}\}\}=\{\{P^{l_1}_{\tau_f 1}\},\{P^{l_2}_{\tau_f 2}\},...,\{P^{l_{ni}}_{\tau_f r_5}\}\}, \quad (11)$$

де $P^l_{\tau_f i}\subseteq P^l_{\tau_f}$ $(i=\overline{1,r_5})$ — ідентифікатор строку обмеження доступу до *ОІ* за кожною статею у переліку L_i, а r_5 — їх кількість. Якщо відомо з [6], [12], [17] – [19], що строк, протягом якого діє рішення про віднесення інформації до державної таємниці, який встановлюється державним експертом з питань таємниць, не може перевищувати для інформації із ступенем секретності «особливої важливості» — 30 років, для інформації «цілком таємно» — 10 років, для інформації «таємно» — 5 років. То строк, що встановлюється експертною комісією для СлІ, може складати до 5 років.

Наприклад, з урахуванням [29] при $r_{1i}=1$ $(i=4)$, $r_{1_{4.j}}=6$ $(j=\overline{1,6})$ та $l=r_{1_{4.1}}\div r_{1_{4.6}}$ для $r_5=1$ $(i=1)$, формула (11) набуде вигляду:

$$P^l_{\tau_f}=\{\bigcup_{i=1}^{r_5}\{P^l_{\tau_f i}\}\}=\{\{P^{r_{14.1}}_{\tau_f 1}\},\{P^{r_{14.2}}_{\tau_f 1}\},\{P^{r_{14.3}}_{\tau_f 1}\},\{P^{r_{14.4}}_{\tau_f 1}\},\{P^{r_{14.5}}_{\tau_f 1}\},\{P^{r_{14.6}}_{\tau_f 1}\}\}=$$

$$=\{\{"4"\},\{"4"\},\{"3"\},\{"4"\},\{"2"\},\{"2"\}\}=$$

$$=\{\{"для статті 4.1. — 4 роки"\},\{"для статті 4.2. — 4 роки"\},\{"для статті 4.3. — 3 роки"\},\{"для статті 4.4. — 4 роки"\},\{"для статті 4.5. — 2 роки"\},\{"для статті 4.6. — 2 роки"\}\}.$$

Останній параметр кортежу $\boldsymbol{V}$ — множина ідентифікаторів, що присвоюється документам та матеріальним носіям службової інформації (МНСлІ) і визначається як:

$$V=\{\bigcup_{i=1}^{r_6}\{V_i\}\}=\{\{V_1\},\{V_2\},...,\{V_{r_6}\}\}, \quad (12)$$

де $V_i\subseteq V$ $(i=\overline{1,r_6})$ — ідентифікатори відміток, що присвоюється документам та матеріальним носіям інформації, що містять *ОІ*, а r_6 — їх кількість. Відповідно до [30], [31] для *ОІ* наявні чотири відмітки, що присвоюється документам та МНСлІ: гриф «Для службового користування»; відмітка «Літер «М»; відмітка «Літер «К»; відмітка «СІ».

Наприклад, при $r_6=4$ $(i=\overline{1,4})$ з урахуванням [30] формула (12) набуде вигляду:

$$V=\{\bigcup_{i=1}^{4}\{V_i\}\}=\{\{V_1\},\{V_2\},\{V_3\},\{V_4\}\}=$$

$$=\{\{"ДСК"\},\{"Літер «М»"\},\{"Літер «К»"\},\{"«СІ»"\}\}=$$

$$=\{\{"документам та МНСлІ присвоюється гриф «Для службового користування»"\},\{"документам та МНСлІ з мобілізаційних питань, додатково проставляється відмітка “Літер «М»"\},\{"документам та МНСлІ з питань криптографічного захисту СлІ, — відмітка «Літер «К»"\},\{"документам та МНСлІ з питань спеціальної інформації, — відмітка «СІ»"\}.$$

Загальну ієрархічну структуру розробленої моделі (з урахуванням наведених прикладів) представлено на рис. 1.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

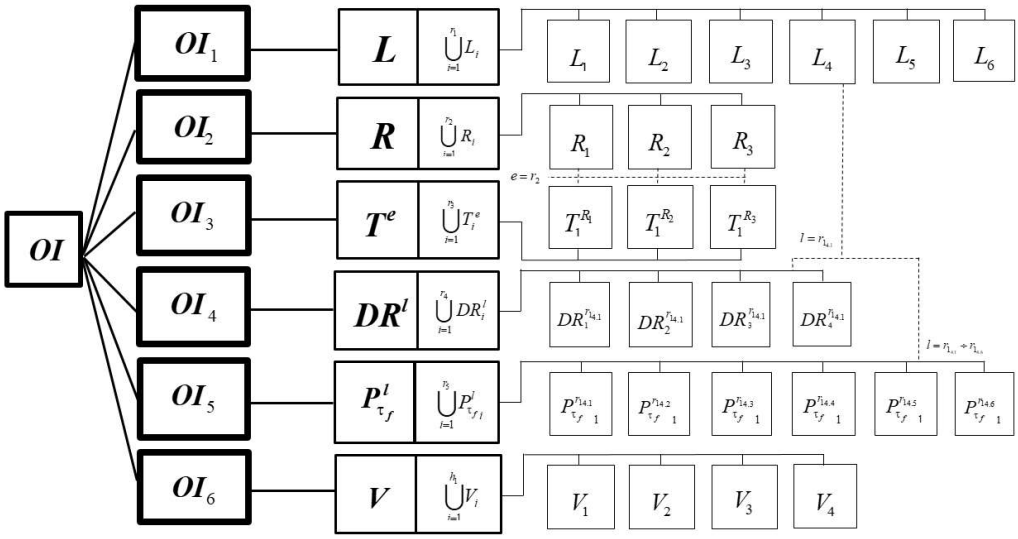

Рис. 1. Ієрархічна структура кортежної моделі параметрів оцінювання наслідків витоку службової інформації об'єкта критичної інфраструктури

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Таким чином, запропонована кортежних модель формування набору базових параметрів оцінювання наслідків витоку СлІ на ОКІ, яка за рахунок формалізації процедури обмеження доступу до ІзОД, дозволяє сформувати кортеж, що відображає процес класифікації СлІ та становлення базових параметрів для оцінювання наслідків та можливої шкоди у разі її витоку відповідно до затвердженого на ОКІ переліку СлІ.

У подальшому, для проведення експериментального дослідження та практичної реалізації, необхідно розробити метод оцінювання наслідків витоку СлІ на ОКІ, який за рахунок розробленої моделі дозволить розрахувати наслідки і величину нанесеної шкоди від можливого витоку СлІ на ОКІ з метою своєчасного попередження, виявлення, запобігання і нейтралізації такої загрози безпеці ОКІ та підтримки стану захищеності ОКІІ на такому рівні, за якого забезпечується безперервність функціонування і стійкість надання ОКІ основних послуг та/або життєво важливих функцій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про доступ до публічної інформації, Закон України №2939-VI (2023). https://zakon.rada.gov.ua
2. Лациба, М., та ін. (2011). *Методичні рекомендації щодо практичного впровадження Закону України «Про доступ до публічної інформації». Методичні рекомендації*. https://www.president.gov.ua
3. Огданська, О., та ін. (2014). Службова інформація: порядок віднесення та доступу. *Практичний посібник*. http://za.inf.ua/bo/slizkonis_dsk.pdf
4. Питання забезпечення органами виконавчої влади доступу до публічної інформації, Указ Президента України №547/2011 (2011). https://zakon.rada.gov.ua
5. Дрейс, Ю. (2012). Врахування інтересів держави в методиці оцінювання шкоди у сфері охорони державної таємниці. *V міжнародна конференція Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2012)*, 316–318.
6. Корченко, О., та ін. (2014). *Оцінювання шкоди національній безпеці України у разі витоку державної таємниці. Монографія*. https://repository.mu.edu.ua/jspui/handle/123456789/5221
7. Касперський, І. (2014). Класифікаційні ознаки службової інформації. *Інформаційна безпека людини, суспільства, держави, 3(16)*, 104–109.

8. Касперський, І. (2020). Проблеми правової регламентації змісту службової інформації в Україні. *Інформаційна безпека людини, суспільства, держави, 1–3 (28–30)*, 83–89.
9. Ткачук, Т., & Марчук, В. (2012). Актуальні теоретичні та практичні проблеми визначення правової природи службової інформації. *Інформаційна безпека людини, суспільства, держави, 3(10)*, 51–56.
10. Гуменюк, І. (2012). Проблеми охорони державної таємниці та службової інформації у трудоправовому аспекті. *Актуальні проблеми управління інформаційною безпекою держави*, тези конф., 12–15.
11. Falchenko, S., et al. (2020). Method of Fuzzy Classification of Information with Limited Access. *IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT)*, 255–259. https://doi.org/10.1109/ATIT50783.2020.9349358
12. Корченко, О., & Дрейс, Ю. (2011). *Охорона конфіденційної інформації підприємства. Навчальний посібник*.
13. Корченко, О., & Дрейс, Ю. (2012). Модель складної орієнтованої інформаційної мережі службової інформації у сфері оборони – Переліку службової інформації Збройних Сил України. *Захист інформації і безпека інформаційних систем*, 10–11.
14. Дрейс, Ю., & Корченко, О. (2014). Проблема формування переліку відомостей, що становлять службову інформацію. *Актуальні проблеми управління інформаційною безпекою держави*, 168–169.
15. Дрейс, Ю. (2021). Службова інформація: розмір істотної шкоди у разі розголошення. *XI міжнародна конференція ITSec*, 7–8.
16. Dreis, Yu., et al. (2022). Restricted Information Identification Model. In: *Cybersecurity Providing in Information and Telecommunication Systems*, *Vol. 3288*, 89–95.
17. Корченко, О., & Дрейс, Ю. (2022). Кортежна модель формування бази даних первинних параметрів для оцінювання стану охорони державної таємниці. *Безпека інформації*, *28(1),* 35–42. https://doi.org/10.18372/2225-5036.28.16911
18. Dreis, Yu., et al. (2024). Model to Formation Data Base of Internal Parameters for Assessing the Status of the State Secret Protection. In: *Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3654*, 277–289.
19. Dreis, Yu., et al. (2024). Model to Formation Data Base of Secondary Parameters for Assessing Status of the State Secret Protection. In: *Cyber Security and Data Protection*, *Vol. 3800*. 1–11.
20. Дрейс, Ю. (2024). Метод оцінювання наслідків втрати об'єкта критичної інформаційної інфраструктури за узагальненими критеріями. *Кібербезпека: освіта, наука і техніка, 1(25)*, 487–504. https://doi.org/10.28925/2663-4023.2024.25.487504
21. Korchenko, O., et al. (2017). Analysis problems in the field of state's critical infrastructure. *Projekt interdyscyplinarny projektem XXI wieku: Monografia, 1*, 397–402.
22. Корченко, О. та ін. (2013). Методологія синтезу та програмна реалізація системи оцінювання шкоди національній безпеці у сфері охорони державної таємниці. *Захист інформації*, *15(1),* 14–20. https://doi.org/10.18372/2410-7840.15.4210
23. Корченко, О., Казмірчук, С., & Ахметов, Б. (2017). *Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія*.
24. Мохор, В., & Гончар, С. (2019). Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури. *Електронне моделювання, 41(6)*, 65–76.
25. Гнатюк, С., та ін. (2020). Базові аспекти захисту конфіденційної інформації на об'єктах критичної інформаційної інфраструктури. *Кібербезпека: освіта, наука і техніка, 1(9)*, 170–181.
26. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, Постанова КМУ, правила №373 (2021). https://zakon.rada.gov.ua
27. Деякі питання об'єктів критичної інфраструктури, Кабінет Міністрів України, Постанова №1109 (2024). https://zakon.rada.gov.ua
28. Деякі питання об'єктів критичної інформаційної інфраструктури, Кабінет Міністрів України, Постанова №943 (2022). https://zakon.rada.gov.ua
29. Про затвердження Переліку відомостей, що містять службову інформацію в Міністерстві освіти і науки України, Міністерство освіти і науки України, Наказ №1 (2019). https://mon.gov.ua
30. Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, Постанова КМУ №736 (2023). https://zakon.rada.gov.ua
31. Гулак, Г. М., Жильцов, О. Б., Киричок, Р. В., Коршун, Н. В., & Складанний, П. М. (2024). *Інформаційна та кібернетична безпека підприємства.* Підручник. Львів : Видавець Марченко Т. В.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Yurii Dreis
PhD in Eng. (Information security), Associate Professor, Associate Professor of System Analysis & Information Technologies Academic Department
Mariupol State University, Kyiv, Ukraine
ORCID ID: 0000-0003-2699-1597
y.dreis@mu.edu.ua

MODEL OF PARAMETERS FOR ASSESSING CONSEQUENCES OF LEAKAGE OFFICIAL INFORMATION FROM OBJECT OF CRITICAL INFRASTRUCTURE

Abstract. There is a problem between the effectiveness of ensuring the stable and continuous functioning of a critical infrastructure facility in the process of providing it with basic services and/or vital functions and the effectiveness of the implemented methods, means and measures that do not provide a sufficient level of protection of critical information infrastructure facilities and, as a result, lead to the leakage of information with limited access, especially official information. To solve it, an analysis of the types of liability in case of disclosure of official information, classified by the amount of significant damage caused or serious consequences, was conducted. Criteria for restricting access and classifying types of information with limited access, especially for official information, were established as a "three-part test" to determine the relevant interest, purpose and its purpose, harm in case of disclosure and its counterbalance to the public interest in disclosure. Based on the conducted study of the list of service information of a separate critical infrastructure object, a basic model was developed, which, due to the integrated set-theoretic representation of sets characterizing the parameters of access restrictions, the information object, its set or individual indicators, the stamp, terms and types of marking of material carriers of service information, etc., allows, in accordance with the requirements of current legislation, to determine the sets of input and output components for forming a set of parameters for assessing the consequences of its leakage. Also, a hierarchical structure of this tuple model of the parameters for assessing the consequences of a leak of service information of a critical infrastructure object was built for the structuring of input and output data. In the future, to conduct experimental research and practical implementation of the above process, it is necessary to develop a method for assessing the consequences of the leakage of official information from object of critical infrastructure.

Keywords: object of critical infrastructure; consequences of leakage official information; model of parameters for assessment consequences.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. On Access to Public Information, Law of Ukraine No. 2939-VI (2023). https://zakon.rada.gov.ua.
2. Latsyba, M., et al. (2011). *Methodological Recommendations on Practical Implementation of the Law of Ukraine 'On Access to Public Information'. Methodological recommendations.* https://www.president.gov.ua.
3. Ogdanska, O., et al. (2014). Official information: the procedure of classification and access. A practical guide. http://za.inf.ua/bo/slizkonis_dsk.pdf.
4. Issues of Ensuring Access to Public Information by Executive Bodies, Decree of the President of Ukraine No. 547/2011 (2011). https://zakon.rada.gov.ua
5. Drais, Y. (2012). Taking into account the interests of the state in the methodology of damage assessment in the field of protection of state secrets. *V International Conference on Integrated Intelligent Robotic Systems (IIRTC-2012),* 316–318.
6. Korchenko, O., et al. (2014). *Assessment of damage to the national security of Ukraine in case of leakage of state secrets. Monograph.* https://repository.mu.edu.ua/jspui/handle/123456789/5221.
7. Kasperskyi, I. (2014). Classification features of proprietary information. *Information security of a person, society, state, 3(16),* 104–109.
8. Kasperskyi, I. (2020). Problems of legal regulation of the content of proprietary information in Ukraine. *Information security of a person, society, state, 1–3 (28–30),* 83–89.

9. Tkachuk, T., & Marchuk, V. (2012). Actual theoretical and practical problems of determining the legal nature of official information. *Information security of a person, society, state, 3(10),* 51–56.
10. Gumeniuk, I. (2012). Problems of protection of state secrets and proprietary information in the labour law aspect. *Actual problems of managing the information security of the state, abstracts of the conference, 12–15.*
11. Falchenko, S., et al. (2020). Method of Fuzzy Classification of Information with Limited Access. *IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT),* 255–259. https://doi.org/10.1109/ATIT50783.2020.9349358
12. Korchenko, O., & Dreis, Y. (2011). *Protection of confidential information of the enterprise. Study guide.*
13. Korchenko, O., & Dreis, Y. (2012). Model of a complex orientated information network of proprietary information in the defence sector - the List of proprietary information of the Armed Forces of Ukraine. *Information Protection and Security of Information Systems,* 10–11.
14. Dreis, Y., & Korchenko, O. (2014). The problem of forming a list of data constituting proprietary information. *Actual problems of information security management of the state,* 168–169.
15. Dreis, Y. (2021). Proprietary information: the amount of material damage in case of disclosure. *XI International ITSec Conference,* 7–8.
16. Dreis, Yu., et al. (2022). Restricted Information Identification Model. In: *Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3288,* 89–95.
17. Korchenko, O., & Dreis, Y. (2022). A tuple model for the formation of a database of primary parameters for assessing the state of protection of state secrets. *Information Security, 28(1),* 35–42. https://doi.org/10.18372/2225-5036.28.16911
18. Dreis, Yu., et al. (2024). Model to Formation Data Base of Internal Parameters for Assessing the Status of the State Secret Protection. In: *Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3654*, 277–289.
19. Dreis, Yu., et al. (2024). Model to Formation Data Base of Secondary Parameters for Assessing Status of the State Secret Protection. In: *Cyber Security and Data Protection*, *Vol. 3800*, 1–11.
20. Dreis, Yu. (2024). Method for assessing consequences of los a critical information infrastructure object by generalized criteria. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 1(25),* 487–504. https://doi.org/10.28925/2663-4023.2024.25.487504
21. Korchenko, O., et al. (2017). Analysis problems in the field of state's critical infrastructure. *Projekt interdyscyplinarny projektem XXI wieku: Monograph, 1*, 397–402.
22. Korchenko, O., et al. (2013). Synthesis methodology and software implementation system evaluation harm to national security in protection of state secrets. *Ukrainian Journal of Information Security Research*, *15(1),* 14–20. https://doi.org/10.18372/2410-7840.15.4210
23. O. Korchenko, et al. (2017). *Applied information security risk assessment systems. Monograph*.
24. Mohor, V., & Honchar, S. (2019). Assessment of cyber security risks of information systems of critical infrastructure objects. *Electronic Modeling*, *41(6)*, 65–76.
25. Gnatyuk, S., et al. (2020). Basic aspects of confidential information security in critical information infrastructure objects. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 1(9)*, 170–181.
26. On Approval of the Rules for Ensuring the Protection of Information in Information, Electronic Communication and Information and Communication Systems, CMU Resolution, Rules No. 373 (2021). https://zakon.rada.gov.ua.
27. Some Issues of Critical Infrastructure Objects, Cabinet of Ministers of Ukraine, Resolution No. 1109 (2024). https://zakon.rada.gov.ua
28. Some issues of critical information infrastructure, Cabinet of Ministers of Ukraine, Resolution No. 943 (2022). https://zakon.rada.gov.ua
29. On Approval of the List of Data Containing Proprietary Information in the Ministry of Education and Science of Ukraine, Ministry of Education and Science of Ukraine, Order No. 1 (2019). https://mon.gov.ua
30. On Approval of the Standard Instruction on the Procedure for Keeping Records, Storage, Use and Destruction of Documents and Other Material Media Containing Proprietary Information, CMU Resolution No. 736 (2023). https://zakon.rada.gov.ua
31. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise.* Textbook. Lviv: Publisher Marchenko T. V.