КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.487504
УДК 004.02-044.3-021-028.43(004)

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

МЕТОД ОЦІНЮВАННЯ НАСЛІДКІВ ВТРАТИ ОБ'ЄКТА КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ЗА УЗАГАЛЬНЕНИМИ КРИТЕРІЯМИ

Анотація. На основі проведеного аналізу та дослідження критеріїв визначення і оцінки секторів критичної інфраструктури, критичності об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури, об'єктів інформаційної діяльності, соціальної, суспільної, економічної значущості цих об'єктів критичної інфраструктури, взаємозв'язку між ними, у т.ч. для забезпечення національної безпеки та обороноздатності країни, враховуючи категорії складності об'єкта за класами наслідків (відповідальності) будівель і споруд, надання життєво важливих функцій та/або основних послуг, рівнів можливих надзвичайних або кризових ситуацій у разі втрати тощо, розроблено метод оцінювання наслідків втрати об'єкта критичної інформаційної інфраструктури за запропонованими узагальненими критеріями (міжнародного та національного впливу; функцій та/або послуг, значущості, відповідальності, інформації, кіберзахисту, захисту і гарантій, кіберстійкості). Даний метод є одним із способів попередження, виявлення, запобігання і нейтралізації загроз безпеці об'єкта критичної інфраструктури та підтримки стану захищеності об'єкта критичної інформаційної інфраструктури на рівні, за якого забезпечується безперервність функціонування і стійкість надання основних послуг та/або життєво важливих функцій за для своєчасної мінімізації та ліквідації оцінених наслідків. У подальшому для проведення експериментального та практичної реалізації необхідно розробити метод оцінки ризику втрати об'єкта критичної інформаційної інфраструктури.

Ключові слова: об'єкт критичної інформаційної інфраструктури; наслідки втрати; метод оцінювання; критерії наслідків.

ВСТУП

У сучасному світі розвиток будь-якої демократичної країни визначається здатністю до забезпечення надання якомога більшої кількості послуг та функцій, необхідних для комфортного і безпечного життя її громадян. Висока затребуваність у отриманні окремих таких послуг та функцій, викликана різними сферами існування людини, суспільства, держави, призвела до надання їм статусу як «основних» та/або «життєво важливих». Тому об'єкти, які здатні надавати ці основні послуги та/або життєво важливі функції для кожної країни є критичними. Сукупність таких критичних об'єктів у межах однієї сфери визначає відповідний сектор критичної інфраструктури, а сукупність всіх секторів за усіма сферами формує критичну інфраструктуру держави. Реалізація процесу надання більшості основних послуг та/або життєво важливих функцій на об'єкті критичної інфраструктури (ОКІ) відбувається в основному за допомогою використання комунікаційних або технологічних систем, що робить їх об'єктами критичної інформаційної інфраструктури (ОКІІ). Здійснення ОКІІ управління технологічних

процесів та/або забезпечення електронних комунікацій на ОКІ відбувається в цілому у кіберпросторі, який передбачає використанням мережі Інтернет та/або інших глобальних мереж передачі даних, а тому такі системи є цілями для кібератак. Саме тому метою кібератаки на ОКІІ є виведення із ладу або функціонування (тобто їх втрати) за для порушення штатного режиму функціонування ОКІ і завдання безпосереднього впливу на стійкість та безперебійність надання ним основних послуг та/або життєво важливих функцій, а її успішність реалізації призведе до швидких негативних наслідків для економіки, національної безпеки та оборони, порушення функціонування яких завдають шкоди життєво важливим національним інтересам людини, суспільства, держави.

Постановка проблеми. Наразі Україна перебуває у воєнному стані, а тому досить гостро постає питання у забезпеченні безпеки її критичної інфраструктури від можливих загроз, інцидентів, кібератак, несанкціонованого втручання та кризових ситуацій (КС), тобто у підтримці такого стану захищеності, за якого забезпечуються її функціональність, безперервність роботи, відновлюваність, цілісність і стійкість до надання ОКІ основних послуг та/або життєво важливих функцій, порушення яких призведе до негативних наслідків для національної безпеки України. Головною вимогою до ОКІІ є ефективне забезпечення стійкого і безперервного функціонування ОКІ для надання ним основних послуг та життєво важливих функцій, реалізовуючи при цьому захист критичної інформаційної інфраструктури. Ефективність захисту ОКІІ визначається її здатністю до своєчасного виявлення, запобігання і нейтралізації загроз безпеці ОКІ, а також мінімізацію та ліквідацію наслідків у разі їх реалізації. Тобто виконувати функції захищеності від подій або ряду несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки несанкціонованого втручання в функціонування ОКІ, які становлять загрозу його безпеці, системі управління технологічними процесами, створюють ймовірність порушення штатного режиму функціонування такого об’єкта (у тому числі зриву та/або блокування роботи, функціонування та/або несанкціонованого управління його ресурсами, витоку інформації), ставлять під загрозу його захищеність. Недостатнє забезпечення захисту ОКІІ від реалізації кібератак, може призвести до порушення стійкого і безперервного його функціонування, що матиме негативні наслідки для безпеки критичної інфраструктури держави, тобто і для національної безпеки України.

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 його втрати. Вирішення цієї проблеми можливе шляхом розробки нових моделей, методів та засобів оцінювання ризиків та можливих потенційних наслідків втрати ОКІ у разі реалізації кібератаки на його ОКІІ 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 [1] – [13], у яких започатковано розв’язання проблеми з одного боку, — щодо методологічних та організаційних засад забезпечення стійкого і безперервного функціонування ОКІ (О. Суходоля, С. Іванюта, С. Кондратов, Д. Бобро, О. Єрменчук та ін.) [1] – [3], а з іншого, — щодо побудови системи, методів,

засобів та заходів забезпечення кібербезпеки, інформаційної безпеки та захисту інформації, оцінювання ризиків, кіберзахисту ОКІІ (О. Корченко, С. Казмірчук, Є. Іванченко; В. Мохор, С. Гончар, М. Комаров; С. Гнатюк, О. Юдін, В. Сидоренко) [4] – [11], а також інших міжнародних і державних стандартів [14] – [17], законодавчих та нормативних актів у сфері кібербезпеки та захисту інформації, критичної інфраструктури, деяких питань ОКІІ та ОКІ, загальних вимог до кіберзахисту ОКІ, правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, методичних рекомендацій щодо категоризації ОКІ, порядку класифікації надзвичайних ситуацій за їх рівнями, та критеріїв, відповідно до яких об'єкти включаються до переліку окремих особливо важливих об'єктів права державної власності, охорона яких здійснюється виключно державними підприємствами та організаціями на підставі договорів про надання охоронних послуг [18] – [32].

Метою роботи є розробка методу оцінювання наслідків втрати ОКІІ за узагальненими критеріями 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

Метод оцінювання наслідків втрати ОКІІ за узагальненими критеріями

Дослідивши та узагальнивши більшість доступних у [1] – [32] критеріїв визначення переліків, режимів, класів, рівнів, категорій, оцінки захищеності, критичності ОКІ та/або ОКІІ, ОІД, складності об'єктів, особливо важливих об'єктів, об'єктів підвищеної небезпеки, інших об'єктів і систем, які враховують характеристики можливих негативних наслідків у разі їх втрати, припинення функціонування або відмови, запропоновано ***перелік узагальнених критеріїв наслідків втрати ОКІІ***, а саме як:

- *секторальні критерії:*
  1) за наслідком оцінки міжнародного впливу важливості сектору (галузі) на критичну інфраструктуру держави (*критерій міжнародного впливу*);
  2) за наслідком оцінки національного впливу важливості сектору на критичну інфраструктуру держави (*критерій національного впливу*);
  3) за наслідками порушення надання ОКІ життєво важливих функцій та/або основних послуг у разі знищення, пошкодження або порушення функціонування ОКІІ для національної безпеки України (*критерій функцій та/або послуг*);
- *міжсекторальні критерії:*
  1) за наслідками оцінки рівня негативного впливу соціальної, суспільної, економічної значущості ОКІ, взаємозв'язку між ОКІ, значущості ОКІ для забезпечення національної безпеки та обороноздатності країни, встановленого категорією критичності (критерій значущості);
  2) за оцінкою характеристик наслідків відмови або припиненням функціонування ОКІ, визначених категорією складності об'єкта, рівнем потенційних надзвичайних ситуацій та класом наслідків (відповідальності) будівель і споруд, спричинених втратою ОКІІ (критерій відповідальності);

3) за наслідками витоку критичної інформації (певного виду інформації за порядком доступу), яка обробляється на ОКІІ визначених категорією ОІД та/або категорією критичності ОКІ і за рівнем можливої кризової ситуації (критерій інформації);

– *об'єктові критерії:*

1) за наслідком втрати ефективності способів виконання кіберзахисту ОКІІ, визначених переліком базових і загальними вимогами до організаційно-методологічних, технічних та технологічних умов кіберзахисту ОКІ (критерій кіберзахисту);
2) за рівнем наслідків порушення конфіденційності, цілісності і доступності інформації, недоступності служб та функцій захисту (як функціональних послуг безпеки (ФПБ)), визначених функціональним профілем захищеності на КСЗІ і рівнем гарантій (критерій захисту і гарантій);
3) за наслідком втрати кіберстійкості ОКІІ до здатності виконання цільового призначення підтримки безперервності і стійкості надання основних послуг та/або життєво важливих функцій ОКІ, забезпечення режимів роботи та стану захищеності ОКІ в умовах здійснення деструктивних інформаційних впливів (критерій кіберстійкості).

Під ***наслідками втрати ОКІІ*** у цьому дослідженні слід розуміти кількісну міру, що визначає величину можливих негативних наслідків (шкоди/збитків) нанесених для власника ОКІІ та/або оператора критичної інфраструктури у разі можливого виводу з ладу або функціонування, відмови ОКІІ, спричинених реалізацією кібератак, яка показує потенційний вплив на безперервність та стійкість надання цим ОКІ основних послуг та/або життєво важливих функцій, розрахованого за узагальненими критеріями таких наслідків.

Функціональну залежність *наслідків втрати* ОКІІ (*Consequences of Loss*) від їх узагальнених критеріїв можна подати за допомогою наступного виразу:

$$CL = \frac{\sum_{i=1}^{n} cl_i}{n}, \qquad (1)$$

де n — кількість узагальнених критеріїв наслідків втрати ОКІІ; cl_i — коефіцієнт, який характеризує кількісну міру наслідків втрати ОКІІ за i-м критерієм.

Таблиця 1

Наслідки втрати ОКІІ за узагальненими критеріями

Оцінка наслідків втрати ОКІІ (*CL*)	Класифікація наслідків	Умовне позначення наслідку	Рівень негативного впливу	Категорія наслідків	Грошова шкала (€)
< 0,1	незначні	синій	1 бал	перша	< 100 тис.
0,11 ÷ 0,20	середні	зелений	2 бали	друга	100 тис.–1 млн.
0,21 ÷ 0,30	значні	жовтий	3 бали	третя	1–100 млн.
> 0,3	тяжкі	червоний	4 бали	четверта	> 100 млн.

Секторальні критерії

1) *За наслідком оцінки міжнародного впливу важливості сектору (галузі) на критичну інфраструктуру держави* (*критерій міжнародного впливу*). За даним критерієм передбачається ранжування та визначення наслідків втрати ОКІІ у секторі критичної інфраструктури, важливість якого визначається за наявністю його у більшості країн світу як критичного [1] – [7], у світовому стандарті галузей промисловості (GICS) [14],

міжнародному (NACE, МСГК 4) [15] і національному класифікаторі видів економічної діяльності України ДК 009:2010 [16].

Коефіцієнт, який характеризує наслідки оцінки міжнародного впливу важливості сектору (галузі) на критичну інфраструктуру держави, спричинених втратою ОКІІ, cl_1 складається з двох рівнозначних коефіцієнтів $cl_{1.1}$ та $cl_{1.2}$, а його значення є їх середнім арифметичним як:

$$cl_1 = \frac{cl_{1.1} + cl_{1.2}}{n}, \quad (2)$$

де n — кількість коефіцієнтів; $cl_{1.1}$ — коефіцієнт, що характеризує важливість сектору, віднесеного у більшості країн світу до критичного та за GICS; $cl_{1.2}$ — коефіцієнт, що характеризує важливість сектору (галузі) за NACE, МСГК 4, КВЕД ДК 009:2010.

Для отримання коефіцієнта, що характеризує важливість сектору, віднесеного у більшості країн світу до критичного та за GICS, $cl_{1.1}$ використаємо вираз:

$$cl_{1.1} = \frac{f_i}{\sum_{i=1}^{n} f_i}, \quad (3)$$

де n — кількість секторів; f_i — коефіцієнт, який характеризує частоту віднесення i-го сектору до критичної інфраструктури держави.

Методом ранжування отримано коефіцієнт $cl_{1.2}$, що характеризує важливість сектору (галузі) за NACE, МСГК 4, КВЕД ДК 009:2010 за наступним виразом:

$$cl_{1.2} = \frac{r_i}{\sum_{i=1}^{n} r_i}, \quad (4)$$

де n — кількість секторів; r_i — коефіцієнт, який показує рейтинг i-го сектору (галузі).

Результати розрахунку наслідків за *критерієм міжнародного впливу* приведені у табл. 2.

Таблиця 2

Наслідки впливу важливості сектору (галузі) на критичну інфраструктуру держави (міжнародний вплив)

№	Назва сектору	Код сектору/ групи за GICS	Код секції / групи за КВЕД, NACE, МСГК 4	f_i	$cl_{1.1}$	r_i	$cl_{1.2}$	cl_1
1	Сектор безпеки та оборони	20/201010	O/84.22	1	0,109	6	0,136	**0,123**
2	Паливно-енергетичний сектор	10, 15/1510	B, D	1	0,109	6	0,136	**0,123**
3	Банківсько-фінансовий сектор	40, 60	K, L	0,9	0,099	5	0,114	**0,107**
4	Сектор державного управління (сектори державної влади та місцевого самоврядування; соціального захисту; виборів та референдуму; правосуддя; державного матеріального резерву)	20/2020, 25/2530	O, N, P, U, M, Q, R	0,8	0,088	4	0,091	**0,090**
5	Сектор поштового та транспортного зв'язку	20/2030	H	0,7	0,077	3	0,068	**0,073**
6	Інформаційно-телекомунікаційний сектор (сектори цифрових технології; інформаційний; захисту інформації; державної реєстрації)	25/2540, 45, 50	J	1	0,109	3	0,068	**0,073**

7	Промислово-екологічний сектор (сектори промисловості; харчової промисловості та агропромислового комплексу; охорони навколишнього природного середовища)	15, 20/2010, 30	A, B, C	0,6	0,066	2	0,045	**0,055**
8	Сектор послуг життєзабезпечення (вода, тепло, світло, дамби, греблі тощо)	55	E, R, S, T, I, G	1	0,109	6	0,136	**0,123**
9	Сектор охорони здоров'я	35	Q	0,7	0,077	3	0,068	**0,073**
10	Сектор служб екстреної допомоги, надзвичайних ситуацій та цивільного захисту (сектори громадської безпеки, цивільного захисту населення і територій; виконання кримінальних покарань, тримання під вартою та утримання військовополонених)	20/2020	O / 84.24, 84.25	0,9	0,099	5	0,114	**0,107**
11	Інфраструктурний сектор (майданчики, будівлі, стадіони)	60, 40/4040	F	0,5	0,055	1	0,023	**0,039**

2) *За наслідком оцінки національного впливу важливості сектору на критичну інфраструктуру держави* (*критерій національного впливу*). Даний критерій є альтернативою для попереднього, за яким передбачається ранжування та оцінювання наслідків втрати ОКІІ у секторах критичної інфраструктури держави, віднесених до «Переліку секторів критичної інфраструктури» за національним законодавством [26], де важливість кожного з них розраховується загальною кількістю наявних основних послуг розподілених за цим сектором (підсектором) до рівнів негативних впливу за видами можливих наслідків (катастрофічні наслідки (4 бали), критичні наслідки (3 бали), значні наслідки (2 бали), незначні наслідки (1 бал)), які можуть настати у разі порушення функціонування ОКІ, визначених у додатку 1 методики категоризації ОКІ [26].

Для отримання коефіцієнта, що характеризує національний вплив важливості сектору (галузі) на критичну інфраструктуру держави, віднесеного до критичного за національним законодавством, cl_2 використаємо такий вираз:

$$cl_2 = \frac{i_i}{\sum_{i=1}^{n} i_i}, \quad (5)$$

де n — кількість секторів; i_i — коефіцієнт, який характеризує важливість i-го сектору критичної інфраструктури держави за кількістю наявних послуг та рівнем можливих наслідків.

Отримані результати розрахунку наслідків за *критерієм національного впливу* наведені у табл. 3.

Таблиця 3

Наслідки впливу важливості сектору (галузі) на критичну інфраструктуру держави (національний вплив)

№ сект.	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	∑
послуг	27	9	1	5	1	10	1	6	24	5	14	2	105
4 бали	108	36	4	20	4	40	4	24	96	20	56	8	420
3 бали	81	27	3	15	3	30	3	18	72	15	42	6	315
2 бали	54	18	2	10	2	20	2	12	48	10	28	4	210
1 бал	27	9	1	5	1	10	1	6	24	5	14	2	105
i_i,%	19,4	6,4	0,7	3,6	0,7	7,1	0,7	4,3	17,2	3,6	10	1,4	75,1
cl_2	**0,194**	**0,064**	**0,007**	**0,036**	**0,007**	**0,071**	**0,007**	**0,043**	**0,171**	**0,036**	**0,1**	**0,014**	0,75
№ сект.	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	∑
послуг	1	9	3	1	1	1	3	5	2	5	2	2	140
4 бали	4	36	12	4	4	4	12	20	8	20	8	8	560
3 бали	3	27	9	3	3	3	12	15	6	15	6	6	423
2 бали	2	18	6	2	2	2	6	10	4	10	4	4	280
1 бал	1	9	3	1	1	1	3	5	2	5	2	2	140
i_i,%	0,7	6,4	2,1	0,7	0,7	0,7	2,1	3,6	1,4	3,6	1,4	1,4	100
cl_2	**0,007**	**0,064**	**0,021**	**0,007**	**0,007**	**0,007**	**0,021**	**0,036**	**0,014**	**0,036**	**0,014**	**0,014**	1

3) *За наслідками порушення надання життєво важливих функцій та/або основних послуг у разі знищення, пошкодження або порушення функціонування ОКІ для національної безпеки України, спричинених втратою ОКІІ* (*критерій функцій та/або послуг*). Даний критерій передбачає ідентифікацію усіх встановлених законодавством життєво важливих функцій та/або основних послуг і оцінку їх наслідків для національної безпеки України від порушення надання ОКІ, спричинених втратою ОКІІ. Так, за законом [24] віднесено 17 життєво важливих функцій та/або послуг, порушення яких призводить до настання негативних наслідків для національної безпеки України, серед яких [24]: «1) урядування та надання найважливіших публічних (адміністративних) послуг;…; 8) інформаційні послуги; …; 12) оборона, державна безпека; …; 17) дослідницька діяльність». Також постановою [26] до основних послуг, порушення яких призводить до негативних наслідків у разі знищення, пошкодження або порушення функціонування ОКІ, за переліком є 33 послуги, серед них: «п.1. Послуги, що надаються підсектором електроенергетики та підсектором ядерної енергетики»;…; п.33. Послуги (сервіси) кіберзахисту». При проведенні процедури віднесення і категоризації ОКІ до категорії критичності, визначаються послуги з виставленням їм балів, які відповідають рівню негативного впливу, опис якого характеризує наслідки, що можуть настати у разі порушення функціонування ОКІ.

Коефіцієнт, що характеризує наслідки порушення надання життєво важливих функцій та/або основних послуг у разі знищення, пошкодження або порушення функціонування ОКІ для національної безпеки України, спричинених втратою ОКІІ, cl_3 складається з двох рівнозначних коефіцієнтів $cl_{3.1}$ і $cl_{3.2}$, а його значення є середнім арифметичним значень цих коефіцієнтів, аналогічно до формули (2) як:

$$cl_3 = \frac{cl_{3.1} + cl_{3.2}}{n}, \qquad (6)$$

де n — кількість коефіцієнтів; $cl_{3.1}$ — коефіцієнт, що характеризує наслідки для національної безпеки України від порушення надання життєво важливих функцій та/або

послуг; $cl_{3.2}$ — коефіцієнт, що характеризує наслідки порушення надання основних послуг у разі знищення, пошкодження або порушення функціонування ОКІ.

Для отримання коефіцієнта $cl_{3.1}$ використаємо формулу аналогічну до (3) – (5) як:

$$cl_{3.1} = \frac{v_i}{\sum_{i=1}^{n} v_i}, \quad (7)$$

де n — кількість рівнів; v_i — коефіцієнт, який характеризує наслідок за i-м рівнем негативного впливу від порушення надання життєво важливих функцій та/або послуг.

Для отримання коефіцієнта, $cl_{3.2}$ використаємо формулу аналогічну до (7), а саме:

$$cl_{3.2} = \frac{s_i}{\sum_{i=1}^{n} s_i}, \quad (8)$$

де n — кількість рівнів; s_i — коефіцієнт, який характеризує наслідок за i-м рівнем негативного впливу від порушення надання основних послуг, встановленого при віднесенні і категоризації ОКІ за затвердженою у [26] методикою.

Розрахунки наслідків за *критерієм функцій та/або послуг* приведені у табл. 4.

Таблиця 4

Наслідки порушення надання життєво важливих функцій та/або основних послуг у разі знищення, пошкодження або порушення функціонування ОКІ для національної безпеки України, спричинених втратою ОКІ

За видом наслідків	За рівнем впливу (бали)	Життєво важливих функцій/послуг	Оцінка $\sum PK_i$	v_i	$cl_{3.1}$	Основних послуг	Оцінка $\sum PK_i$	s_i	$cl_{3.2}$	cl_3
катастрофічні	4	17	68	0,058	0,397	33	132	0,030	**0,4**	
критичні	3		51	0,044	0,301		99	0,023	**0,3**	
значні	2		34	0,029	0,198		66	0,015	**0,2**	
незначні	1		17	0,015	0,103		33	0,008	**0,1**	

Міжсекторальні критерії

4) За наслідками оцінки рівня негативного впливу соціальної, суспільної, економічної значущості *ОКІ, взаємозв'язку між ОКІ,* значущості *ОКІ для забезпечення національної безпеки та обороноздатності країни, встановленого категорією критичності* (*критерій значущості*). Відповідно до затвердженої методики категоризації ОКІ [26], віднесення об'єктів до критичної інфраструктури здійснюється секторальним органом у сфері захисту критичної інфраструктури разом із оператором критичної інфраструктури, які проводять оцінку їх критичності, використовуючи сукупність секторальних та міжсекторальних критеріїв визначення рівня негативного впливу. Законодавством [24] встановлено, що ця сукупність критеріїв повинна визначати: «…їх соціальну, політичну, економічну, екологічну значущість для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку, зокрема для реалізації життєво важливих функцій та надання життєво важливих послуг, свідчать про існування загроз для них, можливість виникнення кризових ситуацій через несанкціоноване втручання в їх функціонування, припинення функціонування, людський фактор чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму» [24]. До даної сукупності за законом [24] увійшло 7 критеріїв, які за методикою [26] є секторальними і міжсекторальними

критеріями визначення рівня негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування ОКІ.

Для отримання коефіцієнта, що характеризує негативний вплив, який враховує значущість ОКІ для забезпечення національної безпеки та обороноздатності країни, соціальну, суспільну, економічну, наявність взаємозв'язків між ними, встановлених за оцінкою їх критичності, cl_4 використаємо наступною формулу:

$$cl_2 = \frac{e_i}{\sum_{i=1}^{n} e_i}, \tag{9}$$

де n — кількість впливів; e_i — коефіцієнт, який характеризує рівень негативний впливу i-го ОКІ, визначеного за його оцінкою категоризації.

Результати розрахунку коефіцієнта cl_4, який характеризує наслідки за *критерієм значущості* наведено у табл. 5.

Таблиця 5

Наслідки негативного впливу, який враховує значущість ОКІ для забезпечення національної безпеки та обороноздатності країни, соціальну, суспільну, економічну, наявність взаємозв'язків між ними

Значущість	**Соціальна**					∑	**Всього**
	Суспільна/Економічна/Для забезпечення національної безпеки та обороноздатності країни						
	Взаємозв'язок між ОКІ						
К-сть впливів	1	2	3	4	5	15	16
4 бали	4	8	12	16	20	60	64
3 бали	3	6	9	12	15	45	48
2 бали	2	4	6	8	10	30	32
1 бал	1	2	3	4	5	15	16
e_i, %	6,25	12,5	18,75	25	31,25	93,75	100
cl_4	**0,0625**	**0,125**	**0,1875**	**0,25**	**0,3125**	0,9375	1

5) *За оцінкою характеристик наслідків відмови або припиненням функціонування ОКІ, визначених категорією складності об'єкта, рівнем потенційних надзвичайних ситуацій та класом наслідків (відповідальності) будівель і споруд, спричинених втратою ОКІІ* (*критерій відповідальності*). Згідно до постанови [29], для забезпечення організації взаємодії центральних і місцевих органів виконавчої влади, підприємств, установ та організацій у процесі вирішення питань, пов'язаних з надзвичайними ситуаціями (НС) та ліквідацією їх наслідків, здійснюється класифікація НС за їх рівнями як [29]: державного (Д), регіонального (Р), місцевого (М) або об'єктового (О) рівня. Критеріями визначення конкретного рівня НС є [29]: територіальне поширення та обсяги технічних і матеріальних ресурсів, що необхідні для ліквідації наслідків НС; кількість людей, які внаслідок дії уражальних чинників джерела НС загинули або постраждали, або нормальні умови життєдіяльності яких порушено; розмір збитків, завданих уражальними чинниками джерела НС, розраховується відповідно до Методики оцінки збитків від наслідків НС техногенного і природного характеру. Клас наслідків (відповідальності) будівель і споруд визначається відповідно до вимог будівельних норм і правил для кожного об'єкта — будинку, будівлі, споруди будь-якого призначення, їхніх

частин, лінійних об'єктів інженерно-транспортної інфраструктури, у тому числі тих, що належать до складу комплексу (будови). Усі об'єкти поділяються за класами наслідків (відповідальності) на [17]: незначні — СС1; середні — СС2; значні — СС3.

Для отримання коефіцієнта, що характеризує наслідки відмови та/або припинення функціонування ОКІ, визначених категорією складності об'єкта, рівнем потенційних НС та класом наслідків (відповідальності) будівель і споруд, спричинених втратою ОКІІ, cl_5 використаємо формулу:

$$cl_5 = \frac{k_i}{\sum_{i=1}^{n} k_i}, \qquad (10)$$

де n — кількість категорій складності; k_i — коефіцієнт, який характеризує рівень негативний впливу за категорією складності ОКІ, визначеного за рівнем можливої НС і класом наслідків (відповідальності).

Взаємозв'язок характеристик наслідків за *критерієм відповідальності* наведено у табл. 6.

Таблиця 6

Наслідки відмови та/або припинення функціонування ОКІ, визначені категорією складності об'єкта, рівнем потенційних НС та класом наслідків (відповідальності) будівель і споруд, спричинених втратою ОКІІ

Категорія складності об'єкта	Клас/тяжкість наслідків	Умовне позначення	Рівень НС	Колір за рівнем наслідків	Ризик критичності	k_i	cl_5
I категорія	СС-1/незначні наслідки (НН)	СС-I(НН)_I	О	голубий	несуттєвий	1	**0,07**
II категорія		СС-I(НН)_II	О→М	зелений	незначний	2	**0,13**
III категорія	СС-2/середні наслідки (СН)	СС-2(СН)_III	М→Р	жовтий	значимий	3	**0,20**
IV категорія		СС-2(СН)_IV	Р→Д	помаранчевий	значний	4	**0,27**
V категорія	СС-3/значні наслідки (ЗН)	СС-3(ЗН)_V	Д	червоний	критичний	5	**0,33**

6) *За оцінкою наслідків витоку критичної інформації (певного виду інформації за порядком доступу), яка обробляється на ОКІІ, визначених категорією ОІД та/або категорією критичності ОКІ і рівнем можливої кризової ситуації* (*критерій інформації*). Відповідно до п.6 «Порядку внесення ОКІІ до державного реєстру ОКІІ, його формування та забезпечення функціонування», затвердженого постановою [27] і за «Відомості про ОКІІ», передбачено внесення операторами основних послуг відомостей про [6], [27]: повну назву ОКІІ, його призначення, перелік основних послуг, надання яких він забезпечує, категорія критичності; вид інформації за порядком доступу, яка обробляється або планується для оброблення на ОКІІ [13], перелік яких визначено у словнику. Як відомо з [27], категорія критичності ОКІІ встановлюється за категорією критичності ОКІ. За законом [24], встановлено чотири категорії критичності I (перша), II (друга), III (третя) і IV (четверта). Такі ж самі категорії встановлено за [21] і до ОІД залежно від виду інформації з обмеженим доступом (ІзОД), що там циркулює. Також за кожною категорією критичності ОКІ визначено рівень кризової ситуації до якої може призвести порушення функціонування ОКІ, а саме [24]: Д, Р, М, локального (Л) значення.

Для отримання коефіцієнта, що характеризує наслідки витоку критичної інформації (певного виду інформації за порядком доступу), яка обробляється на ОКІІ

визначених категорією ОІД та/або категорією критичності ОКІ і за рівнем можливої кризової ситуації, cl_6 використаємо формулу:

$$cl_6 = \frac{z_i}{\sum_{i=1}^{n} z_i}, \quad (11)$$

де n — кількість категорій ОІД та/або критичності ОКІ/ОКІІ; z_i — коефіцієнт, який характеризує рівень негативний впливу за категорією ОІД та/або критичності ОКІ / ОКІІ і рівнем можливої кризової ситуації.

Взаємозв'язок характеристик наслідків та отримані результати за *критерієм інформації* наведені у таблиці 7.

Таблиця 7

Наслідки витоку критичної інформації (певного виду інформації за порядком доступу), яка обробляється на ОКІІ, визначених категорією ОІД та/або категорією критичності ОКІ і рівнем можливої кризової ситуації

Вид інформації за порядком доступу, яка обробляється або планується для оброблення на ОКІІ / циркулює на ОІД	Категорія (критичності) ОКІ/ОКІІ/ОІД	Рівень кризової ситуації	Рівень критичності ОКІ	z_i	cl_6
(відкрита; службова; державна таємниця, що має ступінь секретності «таємно»; державна таємниця, що має ступінь секретності «цілком таємно»; державна таємниця, що має ступінь секретності «особливої важливості»; конфіденційна інформація про фізичну або юридичну особу (персональні дані); інша таємниця, яка не належить до державної таємниці (лікарська, банківська, тощо); технологічна інформація ОКІІ; інша інформація, вимога щодо захисту якої визначена законом	перша (I)	Д	0,8 ÷ 1	0,9	**0,36**
	друга (II)	Р	0,63 ÷ 0,8	0,715	**0,29**
	третя (III)	М	0,37 ÷ 0,63	0,5	**0,20**
	четверта (IV)	Л	0,2 ÷ 0,37	0,285	**0,11**
		-	< 0,2	0,1	**0,04**

Об'єктові критерії

7) *За наслідком втрати ефективності способів виконання кіберзахисту ОКІІ, визначених переліком базових і загальними вимогами до організаційно-методологічних, технічних та технологічних умов кіберзахисту ОКІ (критерій кіберзахисту).* Законом [22] встановлено, що кіберзахист ОКІ забезпечується згідно до Загальних вимог [28]. Так у випадку, якщо на ОКІІ ОКІ не обробляються державні інформаційні ресурси або ІзОД, вимога щодо захисту якої встановлена законом, Загальні вимоги [28] враховуються під час створення (модернізації) системи інформаційної безпеки (СІБ) ОКІ, а якщо у інакшому випадку — комплексної системи захисту інформації (КСЗІ). Створення КСЗІ здійснюється шляхом впровадження підсистем КСЗІ та комплексів засобів захисту (КЗЗ) технічного (ТЗІ) та/або криптографічного захисту інформації (КЗІ). Також Загальні вимоги [28] визначають перелік базових вимог із забезпечення кіберзахисту ОКІ, які повинні бути впроваджені під час створення КСЗІ (СІБ) ОКІІ ОКІ. Відомо, що кіберзахист ОКІ забезпечується власником та/або керівником ОКІ відповідно до цих Загальних вимог та законодавства в сфері захисту інформації (у т.ч. правила [25]) та кібербезпеки. Тому іншим законом [23] передбачена можливість обробки в системі державних інформаційних ресурсів та ІзОД, вимога щодо захисту якої встановлена законом, крім державної таємниці, службової інформації та інформації з державних і єдиних реєстрів, створення та забезпечення функціонування яких визначені законом, без застосування КСЗІ у разі виконання всіх таких умов, серед яких є: підтвердження відповідності системи управління інформаційною безпекою (СУІБ) тощо; використання

для захисту інформації в системі засобів КЗІ, які мають позитивний експертний висновок за результатами державної експертизи у сфері КЗІ; та інші. Відповідно до НД ТЗІ [20] для захисту інформації на ОІД, де циркулює державна таємниця також впроваджується комплекс технічного (та/або криптографічного) захисту інформації (КТЗІ/ККЗІ).

Для отримання коефіцієнта, що характеризує наслідки втрати ефективності способів виконання кіберзахисту ОКІ та захисту інформації в системі або на ОІД, встановлених законодавством, cl_7 використаємо формулу:

$$cl_7 = \frac{m_i}{\sum_{i=1}^{n} m_i}, \qquad (12)$$

де n — кількість способів кіберзахисту ОКІІ; m_i — коефіцієнт, який характеризує вид i-го способу кіберзахисту ОКІІ залежно від виду інформації за порядком доступу, яка оброблялася на ОКІ та/або циркулювала на його ОІД.

Результати розрахунку наслідків за *критерієм кіберзахисту* наведено у таблиці 8.

Таблиця 8

Наслідки втрати ефективності способів виконання кіберзахисту ОКІІ, визначених переліком базових і загальними вимогами до організаційно-методологічних, технічних та технологічних умов кіберзахисту ОКІ

Вид інформації за порядком доступу, яка оброблялася на ОКІ/циркулювала на ОІД	Способи виконання кіберзахисту ОКІ	m_i	cl_7
(відкрита інформація (у т.ч. державні інформаційні ресурси); службова інформація; державна таємниця, що має ступінь секретності «таємно»; державна таємниця, що має ступінь секретності «цілком таємно»; державна таємниця, що має ступінь секретності «особливої важливості»; конфіденційна інформація про фізичну або юридичну особу (персональні дані); інша таємниця, яка не належить до державної таємниці (лікарська, банківська, слідства, тощо); технологічна інформація ОКІІ; інша інформація, вимога щодо захисту якої визначена законом	Правила та загальні вимоги до кіберзахисту ОКІ за переліком	1	**0,07**
	СІБ	2	**0,13**
	СУІБ; засоби КЗІ; та ін.	3	**0,20**
	КСЗІ та КЗЗ (ТЗІ/КЗІ)	4	**0,27**
	КТЗІ / ККЗІ	5	**0,33**

8) *За наслідками порушення конфіденційності, цілісності та доступності інформації, недоступності служб та функцій захисту (функціональних послуг безпеки (ФПБ)), визначених функціональним профілем захищеності КСЗІ і рівнем гарантій* (*критерій захисту і гарантій*). Законодавством [23] передбачено, що державні інформаційні ресурси або ІзОД, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням КСЗІ з підтвердженою відповідністю. Підтвердження відповідності КСЗІ здійснюється за результатами державної експертизи у встановленому законодавством порядку. За порядком [20], на титульному аркуші експертного висновку повинен бути наведений узагальнений перелік ФПБ (функціональний профіль захищеності) згідно з НД ТЗІ [18], а також рівень гарантій коректності реалізації ФПБ, підтверджені за результатами експертизи. В [19] приведено перелік стандартних функціональних профілів захищеності (СФПЗ) для автоматизованих систем (АС) 1, 2 та 3 класу. Проведеним аналізом експерт повинен встановити інформацію про: клас та підклас ІТС як АС згідно з вимогами НД ТЗІ [19]; вимоги чинних нормативних документів щодо захисту певних властивостей (конфіденційності (К), цілісності (Ц), доступності (Д)) інформації, оброблюваної в ІТС, задоволення яких має забезпечуватися КСЗІ; функціональний склад об’єкта експертизи та його основні характеристики, які мають бути підтверджені в ході проведення експертизи (реалізований функціональний

профіль захищеності, наприклад як у [10]; рівень гарантій коректності реалізації ФПБ; певний перелік організаційних, фізичних та інших заходів захисту тощо); та інше. В критеріях [18] вводиться сім рівнів гарантій (Г-1, ..., Г-7), які є ієрархічними і поступово відбивають наростаючу міру певності в тому, що реалізовані в АС послуги дозволяють протистояти певним загрозам, що механізми, які їх реалізують, в свою чергу коректно реалізовані і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації АС.

Коефіцієнт, який характеризує наслідки за цим критерієм, cl_8 складається з двох рівнозначних коефіцієнтів $cl_{8.1}$ і $cl_{8.2}$, а його значення є сумою значень цих коефіцієнтів як (2):

$$cl_8 = cl_{8.1} + cl_{8.2}, \tag{13}$$

де n — кількість коефіцієнтів; $cl_{8.1}$ — коефіцієнт, що характеризує СФПЗ з вимогами до (К, Ц, Д) КЗЗ для АС; $cl_{8.2}$ — коефіцієнт, що характеризує рівень гарантій (Г-1, ..., Г-7).

Вираз для отримання коефіцієнта $cl_{8.1}$, що характеризує СФПЗ, визначений у [18] як:

$$cl_{8.1} = \frac{p_i}{\sum_{i=1}^{n} p_i}, \tag{14}$$

де n — кількість СФПЗ; p_i — коефіцієнт, що характеризує i-й СФПЗ з вимогами до КЗЗ.

Методом ранжування отримано коефіцієнт $cl_{8.2}$, що характеризує рівень гарантій як:

$$cl_{8.2} = \frac{l_i}{\sum_{i=1}^{n} l_i}, \tag{15}$$

де n — кількість рівнів гарантій; l_i — коефіцієнт ієрархічного рейтингу i-го рівня гарантій.

Отримані результати за *критерієм захисту і гарантій* приведені у табл. 9.

Таблиця 9

Наслідки порушення К, Ц і Д інформації, недоступності служб та функцій захисту (ФПБ), визначених функціональним профілем захищеності КСЗІ і рівнем гарантій

Вимоги до КЗЗ для АС	**класу «1»**	p_i	$cl_{7.1}$	**класу «2»**	p_i	$cl_{7.1}$	**класу «3»**	p_i	$cl_{7.1}$	**Рівень гарантій**	l_i	$cl_{7.2}$
К	1.К.х	1	0,022	2.К.х	4	0,088	3.К.х	7	0,155	*Г-1*	1	0,036
Ц	1.Ц.х		0,022	2.Ц.х		0,088	3.Ц.х		0,155	*Г-2*	2	0,071
Д	1.Д.х		0,022	2.Д.х		0,088	3.Д.х		0,155	*Г-3*	3	0,107
КЦ	1.КЦ.х	2	0,044	2.КД.х	5	0,111	3.КД.х	8	0,177	*Г-4*	4	0,143
КД	1.КД.х		0,044	2.КД.х		0,111	3.КД.х		0,177	*Г-5*	5	0,179
ЦД	1.ЦД.х		0,044	2.ЦД.х		0,111	3.ЦД.х		0,177	*Г-6*	6	0,214
КЦД	1.КЦД.х	3	0,066	2.КЦД.х	6	0,133	3.КЦД.х	9	0,2	*Г-7*	7	0,25

9) *За наслідком втрати кіберстійкості ОКІІ до здатності виконання цільового призначення підтримки безперервності і стійкості надання основних послуг та/або життєво важливих функцій ОКІ, забезпечення режимів роботи та стану захищеності ОКІ в умовах здійснення деструктивних інформаційних впливів* (*критерій кіберстійкості*). Відповідно до закону [24], забезпечення захисту та стійкості критичної

інфраструктури здійснюється в таких режимах її функціонування як: штатний режим, де функціонування інфраструктури здійснюється відповідно до проектного цільового призначення (ЦП); режим готовності та запобігання реалізації загроз, де проводиться перевірка та переведення системи захисту до готовності забезпечити захист та реагування на випадок реалізації загрози, а функціонування інфраструктури здійснюється відповідно до проектного ЦП; режим реагування на виникнення кризової ситуації, де функціонування інфраструктури відбувається в режимі кризової ситуації, вводяться обмеження на режими роботи об'єктів інфраструктури, економічні умови господарювання, доступ до об'єктів; режим відновлення штатного функціонування, де застосовуються заходи щодо повернення параметрів функціонування критичної інфраструктури до штатного режиму, а функціонування інфраструктури здійснюється з обмеженнями відповідно до визначених термінів ліквідації наслідків кризи. За Порядком [30], дані про стан захищеності ОКІ, який визначається відповідно до критеріїв оцінки як «забезпечує», «обмежено забезпечує», «не забезпечує».

Нажаль, для критичної інформаційної інфраструктури законодавством не встановленні режими їх функціонування, але у праці [11] автор наводить наступні критерії здатності ОКІІ виконувати цільову функцію (як ЦП) в умовах здійснення деструктивних інформаційних впливів, де ОКІІ: повністю дієздатний — система повністю справна та функціонує у відповідності до проектної і експлуатаційної документації; загалом дієздатний — система в цілому справна та функціонує у відповідності до експлуатаційної документації, при цьому можливі відхилення від проектних рішень; обмежений — система вийшла з ладу, функціональні характеристики не відповідають проектній документації; недієздатний (підлягає відновленню) — система недієздатна, функціональні характеристики не відповідають проектній і експлуатаційній документації; недієздатний (не підлягає відновленню).

На основі аналізу вище наведених класифікацій для даного критерію оцінки втрати кіберстійкості ОКІІ до здатності виконання ЦП підтримки безперервності і стійкості надання основних послуг та/або життєво важливих функцій ОКІ, забезпечення режимів роботи та стану захищеності ОКІ в умовах здійснення деструктивних інформаційних впливів, запропоновано такі режими функціонування ОКІІ, які більшою мірою відповідають режимам роботи ОКІ як: штатний режим; режим готовності; режим реагування; режим відновлення; режим заміни. Відповідно до цих запропонованих режимів, ОКІІ може мати наступну здатність виконання ЦП (наприклад, за рівнями живучості ОКІІ у [11]) як: повне виконання ЦП (0,9 ÷ 1); дієздатне виконання ЦП (0,7 ÷ 0,9); часткове/обмежене виконання ЦП (0,5 ÷ 0,7); недієздатне виконання ЦП (0,3 ÷ 0,5); повне не виконання ЦП (0 ÷ 0,3). Детальна класифікація режимів функціонування, станів та зон кіберзахисту, рівнів живучості для ОКІІ та станів захищеності ОКІ приведено у табл. 10.

Для отримання коефіцієнта, що характеризує наслідки за цим критерієм, cl_9 використаємо формулу аналогічну до (7) – (12):

$$cl_9 = \frac{c_i}{\sum_{i=1}^{n} c_i}, \tag{16}$$

де n — кількість станів; c_i — коефіцієнт, який характеризує i-й стану кіберстійкості, режим функціонування та рівень живучості ОКІІ, стан захищеності ОКІ.

Отримані результати розрахунку наслідків за *критерієм кіберстійкості* приведені у табл. 10.

Таблиця 10

Наслідки втрати ефективності способів виконання кіберзахисту ОКІІ, визначених переліком базових і загальними вимогами до організаційно-методологічних, технічних та технологічних умов кіберзахисту ОКІ

Визначення стану кіберстійкості ОКІІ	Зони станів	Рівні живучості ОКІІ	Режими функціонування ОКІІ	Стан захищеності ОКІ	c_i	cl_9
повне виконання ЦП	оптимальні	0,9 ÷ 1	штатний	забезпечує	1	**0,067**
дієздатне виконання ЦП	допустимі	0,7 ÷ 0,9	готовності	обмежено забезпечує	2	**0,133**
часткове/обмежене виконання ЦП	граничні	0,5 ÷ 0,7	реагування		3	**0,200**
недієздатне виконання ЦП	критичні	0,3 ÷ 0,5	відновлення	не забезпечує	4	**0,267**
повне не виконання ЦП	незворотні	0 ÷ 0,3	заміни		5	**0,333**

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У цій роботі розроблено метод оцінювання наслідків втрати ОКІІ узагальненими критеріями 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 за такими критеріями як: критерій міжнародного впливу, критерій національного впливу, критерій функцій та/або послуг, критерій значущості, критерій відповідальності, критерій інформації, критерій кіберзахисту, критерій захисту і гарантій, критерій кіберстійкості.

У подальшому, для проведення експериментального дослідження та практичної реалізації, необхідно розробити і метод оцінки ризику втрати ОКІІ, який за рахунок розробленого методу оцінювання наслідків втрати ОКІІ за узагальненими критеріями, дозволить розрахувати ризик можливості виникнення такої негативної події як втрата ОКІІ і величини можливих її наслідків з метою ефективного забезпечення безперервності функціонування та стійкості надання ОКІ основних послуг та/або життєво важливих функцій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kondratovб S., et al. (2017). Developing The Critical Infrastructure Protection System in Ukraine. *Monografia.*
2. Єрменчукб О. (2018). Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України. *Монографія.*
3. Бобро, Д., та ін. (2019). Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України. *Аналіт. доп*.
4. Korchenko, A., et al. (2017). Analysis problems in the field of state's critical infrastructure. *Projekt interdyscyplinarny projektem XXI wieku: Monografia, 1*, 397–402.
5. Korchenko, A., et al. (2019). Criteria for assigning objects to critical infrastructure of Ukraine. *Przetwarzanie, transmisja i bezpieczenstwo informacij*: *Monografia, 2,* 189–196.
6. Корченко, О., та ін. (2018). Модель класифікатора об'єктів критичної інформаційної інфраструктури держави. *Захист інформації*, *20(1)*, 5–11.

7. Korchenko A., et al. (2017). Ukrainian critical information infrastructure: terms, sectors and consequences. *Захист інформації*, *19(4),* 303–309.
8. Корченко, О. (2017). Прикладні системи оцінювання ризиків інформаційної безпеки. *Монографія*.
9. Мохор, В., & Гончар, С. (2019). Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури. *Електронне моделювання, 41(6),* 65–76.
10. Гнатюк, С., Юдін, О., Сидоренко, В., & Євченко, Я. (2021). Метод формування функціонального профілю захищеності галузевих інформаційно-телекомунікаційних систем. *Кібербезпека: освіта, наука, техніка*, *3(11)*, 166–182.
11. Комаров, М.. (2021) Метод та засоби захисту інформації від кібервпливів в комп'ютерних системах та мережах об'єктів критичної інфраструктури. *Дис. канд. техн. наук*.
12. Дрейс, Ю. (2017). Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури держави. *Захист інформації*, *19(3)*, 214–222.
13. Dreis, Yu., et al. (2022). Restricted Information Identification Model. In: *CEUR Workshop Proceedings, vol. 3288*, 89–95.
14. *The Global Industry Classification Standard (GICS)–S&P Global.* (2018). https://www.spglobal.com/marketintelligence/en/documents/112727-gics-mapbook_2018_v3_letter_digitalspreads.pdf
15. International Standard Industrial Classification of All Economic Activities. (2008). *Revision 4. United Nations. New York*. https://unstats.un.org/unsd/publication/seriesM/seriesm_4rev4e.pdf
16. *ДК 009:2010. Класифікація видів економічної діяльності. Національний класифікатор України.* (б. д.). https://zakon.rada.gov.ua/rada/show/vb457609-10
17. *ДСТУ 8855:2019. Будівлі та споруди. Визначення класу наслідків (відповідальності). Київ. ДП «УкрНДНЦ».* (2019). http://www.utsks.com/images/My_pdf/8855_2019.pdf
18. *НД ТЗІ 2.5-004-99. Критерії захищеності інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБ України.* Наказ №22 від 28.04.1999.
19. *НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.* Наказ №22 від 28.04.1999.
20. *НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.* Наказ №65 від 25.03.2011 (зі змінами від 28.12.2012).
21. *ТПКО-95. Тимчасове положення про категоріювання об'єктів.* Наказ №35 від 10.07.1995. https://zakon.rada.gov.ua/rada/show/v0035267-95#Text
22. *Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017* (редакція від 21.06.2024). http://zakon2.rada.gov.ua/laws/show/2163-19.
23. *Про захист інформації в інформаційно-комунікаційних системах.* Закон України від 05.07.1994 (редакція від 28.06.2024). https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
24. *Про критичну інфраструктуру.* Закон України від 16.11.2021 (редакція від 21.06.2024). https://zakon.rada.gov.ua/laws/show/1882-20#Text
25. *Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.* Кабінет Міністрів України. Постанова, правила № 373 від 29.03.2006 (редакція від 31.12.2021). https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text
26. *Деякі питання об'єктів критичної інфраструктури.* Кабінет Міністрів України. Постанова №1109 від 09.10.2020 (редакція від 20.01.2024). https://zakon.rada.gov.ua/rada/show/1109-2020-%D0%BF#n94
27. *Деякі питання об'єктів критичної інформаційної інфраструктури.* Кабінет Міністрів України. Постанова №943 від 09.10.2020 (редакція від 07.09.2022). https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text
28. *Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури.* Кабінет Міністрів України. Постанова №518 від 19.06.2019 (редакція від 07.09.2022). https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
29. *Про затвердження Порядку класифікації надзвичайних ситуацій за їх рівнями*. Кабінет Міністрів України. Постанова, порядок № 368 від 24.03.2004 (редакція від 31.12.2021). https://zakon.rada.gov.ua/laws/show/368-2004-%D0%BF.
30. *Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури.* Кабінет Міністрів України. Постанова, порядок №821 від 22.07.2022. https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF#n8

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 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

METHOD FOR ASSESSING CONSEQUENCES OF LOS A CRITICAL INFORMATION INFRASTRUCTURE OBJECT BY GENERALIZED CRITERIA

Abstract. On the basis of the conducted analysis and research of the criteria for the definition and assessment of critical infrastructure sectors, the criticality of critical infrastructure objects and critical information infrastructure objects, objects of information activity, the social, public, and economic significance of these critical infrastructure objects, the relationship between them, including to ensure the national security and defense capability of the country, taking into account the complexity categories of the object by classes of consequences (responsibility) of buildings and structures, provision of vital functions and/or basic services, levels of possible emergency or crisis situations in case of loss, etc., developed a method for assessing consequences of loss a critical information infrastructure object by generalized criteria (international and national impact, functions and/or services, significance, responsibility, information, cyber security, protection and guarantees, cyber resilience). This method is one of the ways to prevent, detect, prevent and neutralize threats to the security of a critical infrastructure object and to maintain the state of cyber security of a critical information infrastructure object at a level that ensures the continuity of operation and the stability of the provision of basic services and/or vital functions for the timely minimization and elimination of the estimated consequences. In the future, for experimental and practical implementation, it is necessary to develop method for assessing the risk of loss a critical information infrastructure object.

Keywords: critical information infrastructure object; consequences of loss; method of assessment; criteria of consequences.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Kondratov, S., et al. (2017). Developing The Critical Infrastructure Protection System in Ukraine. *Monografia*.
2. Ermenchuk, O. (2018). Basic approaches to the organization of critical infrastructure protection in European countries: experience for Ukraine. *Monograph*.
3. Bobro, D., et al. (2019). Organizational and legal aspects of ensuring the safety and stability of critical infrastructure of Ukraine. *Analyst add.*
4. Korchenko, O., et al. (2017). Analysis problems in the field of state's critical infrastructure. *Projekt interdyscyplinarny projektem XXI wieku: Monografia, 1*, 397–402.
5. Korchenko, O., et al. (2019). Criteria for assigning objects to critical infrastructure of Ukraine. *Przetwarzanie, transmisja i bezpieczenstwo informacij*: *Monografia, 2,* 189–196.
6. Korchenko, O., et al. (2018). Model of the classifier of objects of critical information infrastructure of the state. *Ukrainian Information Security Research Journal, 20(1),* 5–11.
7. Korchenko, O., et al. (2017). Ukrainian critical information infrastructure: terms, sectors and consequences. *Ukrainian Information Security Research Journal, 19(4),* 303–309.
8. Korchenko, O. (2017). Applied information security risk assessment systems. *Monograph*.
9. Mohor, V., & Honchar, S. (2019). Assessment of cyber security risks of information systems of critical infrastructure objects. *Electronic Modeling, 41(6),* 65–76.
10. Gnatyuk, S., et al. (2021). The method of forming a functional security profile of branch information and telecommunication systems. *Cyber security: education, science, technology, 3(11),* 166–182.
11. Komarov, M. (2021). Method and means of protecting information from cyber influences in computer systems and networks of critical infrastructure objects. *Diss. Ph.D. in Eng*.

12. Dreis, Yu. (2017). Analysis of basic terminology and negative consequences of cyberattacks on information and telecommunication systems of critical state infrastructure objects. *Ukrainian Information Security Research Journal, 19(3),* 214–222.
13. Dreis, Yu., et al. (2022). Restricted Information Identification Model. In: *CEUR Workshop Proceedings, vol. 3288*, 89–95.
14. *The Global Industry Classification Standard (GICS)–S&P Global*. (2018). https://www.spglobal.com/marketintelligence/en/documents/112727-gics-mapbook_2018_v3_letter_digitalspreads.pdf
15. *International Standard Industrial Classification of All Economic Activities*. (2008). *Revision 4. United Nations. New York*, https://unstats.un.org/unsd/publication/seriesM/seriesm_4rev4e.pdf
16. *Classification of types of economic activity*. National Classifier of Ukraine SK 009:2010. (n. d.). https://zakon.rada.gov.ua/rada/show/vb457609-10
17. *Buildings and structures. Determination of the class of consequences (responsibility).* SSTU 8855:2019. (2019). http://www.utsks.com/images/My_pdf/8855_2019.pdf
18. *Information security criteria in computer systems against unauthorized access*. (n. d.). ND TPI 2.5-004-99.
19. *Classification of automated systems and standard functional profiles of protection of processed information against unauthorized access*. (n. d.). ND TPI 2.5-005-99.
20. *The procedure for carrying out work on state examination of means of technical protection of information from unauthorized access and complex systems of information protection in information and telecommunication systems*. (n. d.). ND TPI 2.6-001-11.
21. *Provisional provision on the categorization of objects*. PPCO-95. (n. d.). https://zakon.rada.gov.ua/rada/show/v0035267-95#Text
22. *On the main principles of ensuring cyber security of Ukraine*. (2017). Law of Ukraine, http://zakon2.rada.gov.ua/laws/show/2163-19
23. *On the protection of information in information and communication systems*. (1994). Law of Ukraine, https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
24. *On the critical infrastructure*. (2021). Law of Ukraine. https://zakon.rada.gov.ua/laws/show/1882-20#Text
25. *On the approval of the Rules for ensuring the protection of information in information, electronic communication and information and communication systems*. (2020). Resolution https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text
26. *Some issues of critical infrastructure objects.* (2020). Resolution, https://zakon.rada.gov.ua/rada/show/1109-2020-%D0%BF#n94
27. *Some issues of objects of critical information infrastructure.* (2020). Resolution, https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text
28. *On the approval of General requirements for cyber protection of critical infrastructure objects*. (2019) Resolution. https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
29. *On the approval of the Procedure for the classification of emergency situations by their levels.* (2004). Resolution. https://zakon.rada.gov.ua/laws/show/368-2004-%D0%BF
30. *On approval of the Procedure for Monitoring the Security Level of Critical Infrastructure Objects.* (2022). Resolution. https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF#n8