УДК 316.774 (477)
JEL Classification: L15, M15
DOI: 10.15587/2312-8372.2019.169592

МОНІТОРИНГ РОЗВИТКУ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

Прав Р. Ю.

1. Вступ

З початку ведення військового конфлікту в умовах гібридної війни в Україні активізувався процес розвитку нормативно-правової бази, що в цілому сприяє законодавчому забезпеченню інформаційної безпеки. У 2015–2018 рр. було прийнято:

– Стратегію національної безпеки України (2015) [1];

– Стратегію кібербезпеки (2016) [2];

– Доктрину інформаційної безпеки України (2016) [3];

– Закон України «Про основні засади забезпечення кібербезпеки України» (2017) [4];

– Закон України «Про національну безпеку України» (2018) [5].

В Указі Президента України «Про Стратегію національної безпеки України» визначено загрози інформаційній безпеці, інформаційним ресурсам [1]:

– ведення інформаційної війни проти України та відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства;

– уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак;

– фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом;

– критична зношеність основних фондів об'єктів інфраструктури України та недостатній рівень їх фізичного захисту;

– недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій;

– неефективне управління безпекою критичної інфраструктури і систем життєзабезпечення.

У Доктрині визначено ряд найбільш суттєвих та актуальних загроз національним інтересам та національній безпеці України в інформаційній сфері [3]:

– інформаційні операції;

– деморалізація;

– провокування;

– міжетнічні та міжконфесійні конфлікти;

– негативний імідж;

– інформаційна експансія;

– недостатній рівень розвитку інформаційної інфраструктури та неефективна інформаційна політика;

– заклики до радикальних дій населення;

– інші загрози.

Зазначені загрози потребують постійного моніторингу та оцінки.

Закон України «Про національну безпеку» [5] передбачає спрямування державної політики на забезпечення інформаційної безпеки та кібербезпеки України. У цьому законі визначено поняття «індикатори кіберзагроз – показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози», проте відсутній перелік індикаторів, що дали б змогу виявити рівень інформаційної безпеки інфраструктури суб'єктів різних форм власності. У Доктрині інформаційної безпеки України та в Указі Президента України [1] одним з пріоритетних напрямків державної політики в інформаційній сфері визначено «створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них». Іншим важливим напрямком є «моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації». Міністерство інформаційної політики України відзначає потребу у створенні інтегрованої системи оцінки й моніторингу загроз в інформаційному просторі України, що дасть змогу приймати ефективні управлінські рішення державним органам в критичних ситуаціях [6].

Згідно Стратегії Сталого розвитку Україна – 2020 [7] стратегічним індикатором реалізації Стратегії в інформаційній сфері є частка проникнення широкосмугового Інтернету. Показник розраховується за даними Світового банку. У 2020 р. показник повинен скласти 25 абонентів на 100 осіб. Крім цього, 20 фільмів українського виробництва повинні вийти у широкий прокат у 2020 р. Крім того, Стратегія передбачає популяризацію України у світі, просування інтересів України у світовому інформаційному просторі, розвиток медіа та інформаційного суспільства.

Відповідно, розробка системи моніторингу та оцінки розвитку інформаційної інфраструктури в Україні є актуальним завданням, що потребує вирішення у зв'язку з потребою своєчасного виявлення інформаційних загроз та заходів реагування на них.

2. Об'єкт дослідження та його технологічний аудит

Об'єктом дослідження є система моніторингу розвитку інформаційної інфраструктури з метою забезпечення інформаційної безпеки країни та її складові. Компонентами системи моніторингу є індикатори інформаційних загроз та індикатори рівня інформаційної безпеки. Одним з найбільш проблемних місць є відсутність інтегрованої системи оцінки розвитку інформаційної інфраструктури, що унеможливлює своєчасне виявлення інформаційних загроз та своєчасне реагування на них. Відсутній також підхід до оцінювання рівня розвитку інформаційної інфраструктури в Україні.

3. Мета та задачі дослідження

Мета дослідження полягає в оцінюванні розвитку інформаційної інфраструктури в Україні.

Основними завданнями дослідження виступають:

1. Формування системи показників оцінювання рівня розвитку інформаційної інфраструктури в розрізі суб'єктів господарювання.

2. Виокремлення основних тенденцій розвитку інформаційної інфраструктури в Україні.

3. Формування напрямків покращення державної політики органів влади щодо розвитку інформаційної інфраструктури.

4. Дослідження існуючих рішень проблеми

Упродовж 2014–2019 рр. посилилася увага науковців щодо проблематики інформаційних загроз та інформаційної безпеки в Україні. У ряді праць [8, 9] виділено та систематизовано стан інформаційної інфраструктури та рівень захисту інформації в розрізі суб'єктів господарювання України, запропоновано напрямки забезпечення інформаційної безпеки та шляхи протидії інформаційним загрозам.

У роботі [10] систематизовано основні інформаційні загрози зовнішніх джерел:

– несанкціонований доступ до інформації, інформаційної інфраструктури;

– недостатній рівень поінформованості населення про внутрішньополітичну та зовнішньополітичну діяльність України;

– поширення дезінформації;

– інформаційний вплив структур в різних сферах;

– порушення прав українських суб'єктів господарювання в галузі інформаційної безпеки.

Автор роботи [9] обґрунтував потребу моніторингу загроз національній безпеці та визначив технологію моніторингу як процес «збирання, збереження й аналіз необхідної для ефективного управління інформації».

В Україні відсутні напрацювання щодо інтегрального показника розвитку інформаційної інфраструктури та основних його складових. Запропонована система показників дасть змогу комплексно оцінити розвиток інформаційної інфраструктури країни в розрізі основних суб'єктів. Інформаційну безпеку можна трактувати з точки зору взаємодії суб'єктів та об'єктів. Відповідно такому підходу інформаційна безпека – це захист інформації, що підтримує інфраструктуру від випадкового або навмисного впливу природного або штучного характеру, що може завдати шкоди суб'єктам інформаційних відносин. Таким чином, з поданого визначення випливає, що інформаційні загрози виникають у разі недостатнього рівня захисту інформації суб'єктів інформаційних відносин в результаті впливу різного характеру через недостатній рівень розвитку інфраструктури. Рівень захисту інформації суб'єктів можна оцінити на основі моніторингу стану розвитку інформаційно-комунікаційних технологій. Це вказуватиме на достатній або низький рівень захисту інформації, на ступінь впливу на об'єкти інформаційних загроз. Такий підхід забезпечить встановлення потреби у вдосконаленні конкретних напрямків державної політики їх протидії [3].

Науковцями запропоновано ряд методик моніторингу інформаційного простору задля виявлення інформаційних загроз в інформаційному просторі України. Так, автори досліджень [11, 12] пропонують здійснювати контент-моніторинг інформаційного простору на основі аналізу інформації в засобах масової інформації, публікацій в мережі Інтернет, джерел публікацій та їх

наслідків. У працях [13, 14] відзначено необхідність розробки моделей оцінки впливу інформаційних загроз на окремі сфери суспільної діяльності України для їх своєчасного виявлення та нейтралізації засобами системи забезпечення інформаційної безпеки держави. Це також відзначено у роботі [15]: «своєчасний моніторинг характеру, особливостей, масштабів загроз та їх прогнозування мають важливе значення для забезпечення національної безпеки».

Серед основних напрямків вирішення цієї проблеми, виявлених в ресурсах світової наукової періодики, можуть бути виділені дослідження [16], але в них не розглянуто показники моніторингу інформаційних загроз. Автор цих досліджень лише зазначає типи інформації про кіберзагрози, тобто у праці визначено джерела загроз без зазначення рівня їх небезпеки.

У роботі [17] визначено ключові інформаційні загрози та проблеми в інформаційні сфері, проте є невирішеним питання щодо їх оцінки та критичності.

А про вплив нових технологій на рівень інформаційної безпеки та загроз об'єктам інформаційної інфраструктури зазначено в роботі [18]. Однак, у цій роботі не до кінця розкрито ступінь інформаційної безпеки в умовах діджиталізації. Авторами же роботи [19] показано, що хмарні обчислення та технології становлять загрозу інформаційній безпеці та створюють ряд ризиків. Автори цієї роботи також розглядають схеми оцінки ризиків на основі реверсивного підходу, що мінімізує такі ризики за мінімальних витрат, але залишається питання оцінки ризиків інших технологій: технологій аналізу «великих» даних, соціальних медіа, веб-сайтів.

Альтернативний варіант вирішення проблеми, викладений в [20], передбачає створення інформаційної моделі моніторингу загроз національній безпеці. Автор пропонує методи дискретної математики та статистичного аналізу оцінки загроз. Проте отримані результати не містять вимоги до систем моніторингу та оцінки загроз інформаційній безпеці.

Способи впливу різних інформаційно-комунікаційних технологій на безпеку економічних агентів показано в [21]. Однак, у цій роботі відсутні параметри ступеня такого впливу на інформаційну безпеку суб'єктів інформаційної інфраструктури. Автори же роботи [22] підкреслюють важливість використання інтегрованого стратегічного підходу для розробки методології виявлення потенційних гібридних загроз. Хоча це твердження може бути розглянуто в контексті інформаційних загроз.

Таким чином, результати літературного аналізу дозволяють зробити висновок про те, що науковці пропонують ряд підходів, методологій та методів оцінювання і виявлення загроз, а також деталізують інформаційні загрози та вплив нових технологій на інформаційну безпеку. Та пропонують схеми оцінки ризиків та інформаційні моделі оцінки загроз. З чого можна заключити, що розробка системи оцінки та моніторингу стану інформаційної інфраструктури в Україні є перспективним завданням.

5. Методи дослідження

У дослідженні використано статистичний аналіз показників розвитку інформаційної інфраструктури та рівня інформаційних загроз. На основі методів

аналізу та синтезу праць науковців узагальнено основні тенденції розвитку інформаційної інфраструктури в Україні, напрямки вдосконалення державної політики протидії інформаційним загрозам в Україні. А також виділено потребу у розробці системи показників моніторингу якості державної політики.

6. Результати дослідження

На Міністерство інформаційної політики України покладено в установленому порядку організація та забезпечення моніторингу загроз національним інтересам і національній безпеці в інформаційній сфері [1]. Крім того, на підрозділ Державного центру кіберзахисту Держспецзв'язку CERT-UA [23] покладено функції моніторингу і виявлення, накопичення та проведення аналізу даних про кіберзагрози.

Оцінювання стану захищеності державних інформаційних ресурсів в державних органах, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності проводиться згідно з річним планом, який затверджується наказом Адміністрації Держспецзв'язку.

Для моніторингу (оцінювання) розвитку інформаційної інфраструктури в Україні було сформовано систему показників оцінки рівня інформаційної безпеки в розрізі суб'єктів господарювання. До основних показників в Україні відносимо:

1) $К_а$ – кількість абонентів зв'язку, зокрема мережі Інтернет, в тому числі кількість абонентів Інтернет за регіонами, що характеризує кількість пунктів потенційних загроз інформаційній безпеці (ІБ) за територіальною ознакою;

2) $З_{шд}$ – забезпеченість населення широкосмуговим доступом до мережі Інтернет. Показник відображає наявність і здатність використання і запобігання труднощів у сфері інформаційно-комунікаційних технологій (ІКТ) та в цілому відображає рівень потенційних загроз в інформаційній сфері. Зростання показника вказує на підвищення рівня загроз дезінформації населення в Україні;

3) $К_к$ – кількість підприємств, які використовували комп'ютери, одиниць; частка підприємств, які використовували комп'ютери, у % до загальної кількості підприємств, які взяли участь в обстеженні. Показник відображає здатність застосування надійних засобів захисту і боротьби в сфері комп'ютерної безпеки як однієї зі складових ІБ;

4) $К_д$ – кількість підприємств, які мали доступ до мережі Інтернет, одиниць, та частка підприємств, які мали доступ до мережі Інтернет, у % до кількості підприємств, які використовували комп'ютери. Показники характеризують рівень потенційних загроз ІБ підприємств, установ та організацій;

5) $К_ф$ – кількість підприємств, які мали фахівців у сфері інформаційно-комунікаційних технологій: характеризує спроможність підприємств до захисту інформації та інформаційної інфраструктури за рахунок самофінансування;

6) $К_{веб}$ – кількість підприємств, що мали веб-сайт, який функціонував у мережі Інтернет, що відображає рівень сучасного розвитку компанії, можливості підприємств у різних напрямках діяльності, одиниць (рис. 1). Розвиток електронної торгівлі сприяє розвитку українських підприємств, проте водночас вказує на ураження потенційними інформаційними загрозами;

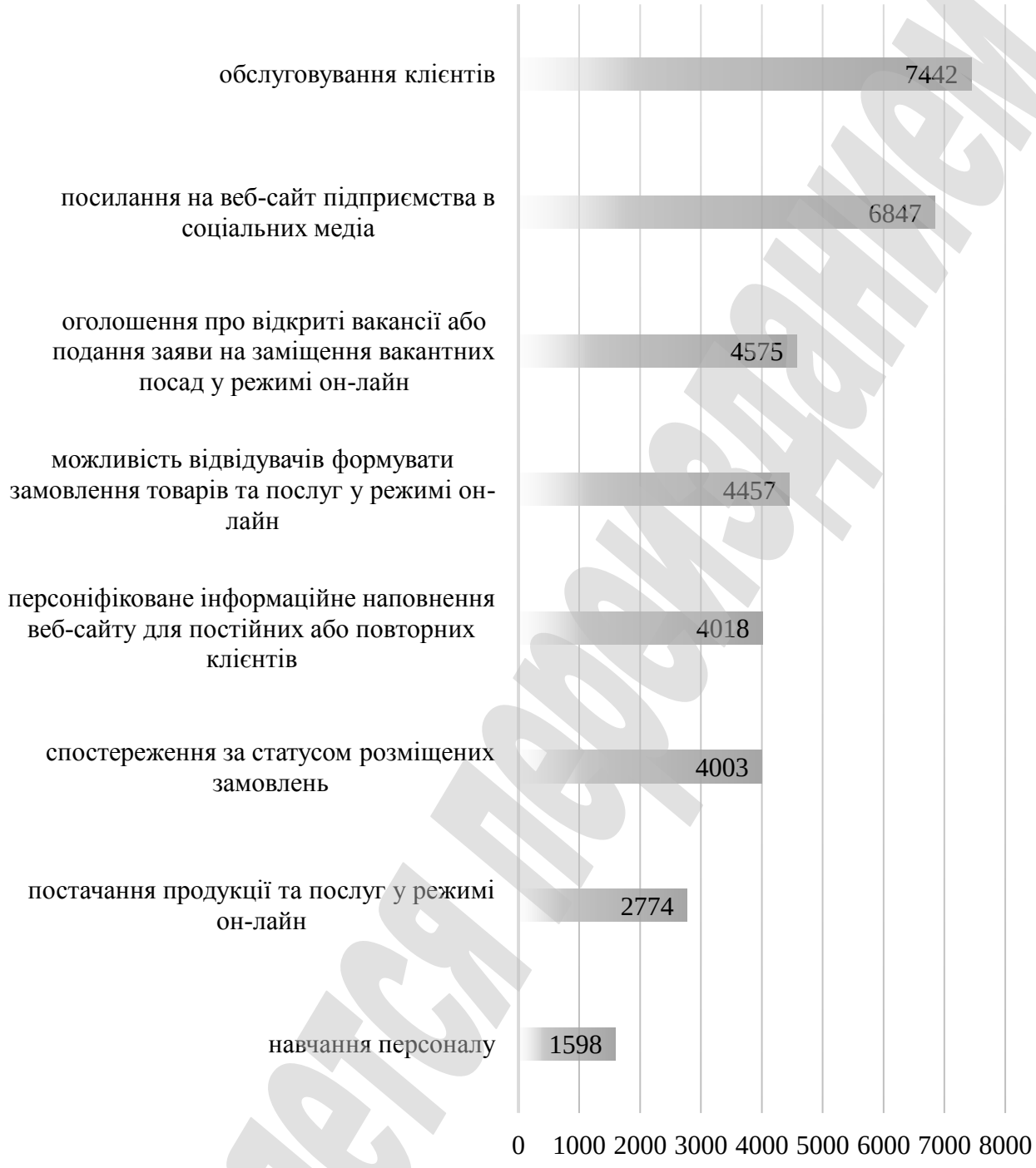

Рис. 1. Кількість підприємств України, що мали веб-сайт, який функціонував у мережі Інтернет в розрізі можливостей веб-сайту у 2017 р. [24]

7) $B_{см}$ – використання соціальних медіа на підприємствах, що характеризує ступінь інтеграції підприємств до медіапростору та можливості підприємств у різних напрямках діяльності, одиниць (рис. 2). Досить вагома частка підприємств використовує соціальні медіа, які водночас мають можливість здійснювати негативний вплив на внутрішнє середовище та інформаційну інфраструктуру компаній;

8) $К_{хт}$ – використання послуг хмарних обчислень в цілому характеризує фінансові можливості підприємств та їх технологічний рівень розвитку, впливає на стан приватної інформаційної інфраструктури в Україні (рис. 3). Хмарні сервіси, технології та обчислення суттєво спрощують роботу підприємств та оптимізують бізнес-процеси. Технологічний рівень розвитку українських підприємств зростає, забезпечуючи розвиток інформаційної інфраструктури в Україні приватного сектору, а тому вказує на можливість фінансування заходів інформаційної безпеки;

9) $К_{вд}$ – статистика аналізу «великих даних» підприємствами, що характеризує стан інформаційної безпеки суб'єктів господарювання, зокрема фізичних та юридичних осіб (рис. 4). Використання підприємствами даних для потреб розвитку діяльності водночас може порушувати інформаційну безпеку інших суб'єктів, а тому державні органи повинні вдосконалювати політику захисту персональних даних. Це має передбачати використання даних в необхідних обсягах та не шкодити громадянам.

Рис. 2. Використання соціальних медіа на підприємствах України за цілями використання у 2017 р., одиниць [24]

Рис. 3. Кількість підприємств, що купували послуги хмарних обчислень упродовж року в розрізі послуг в Україні у 2017 р., одиниць [24]

Рис. 4. Кількість підприємств, що проводили аналіз «великих даних» за даними джерел для аналізу в Україні у 2017 р., одиниць [24]

Визначена система показників оцінки та моніторингу стану ефективності реалізації державної політики органами влади щодо протидії інформаційним загрозам дає змогу проаналізувати основні тенденції рівня інформаційної безпеки в розрізі основних суб'єктів інформаційного простору України (табл. 1).

Таблиця 1

Система показників моніторингу розвитку інформаційної інфраструктури в Україні у 2017 р.

№ п/п	Показник	Одиниці вимірювання	2017
1	$К_а$	тисяч осіб	23632,3
2	$З_{шд}$	тисяч осіб	22625,8
3	$К_к$	–	–
3.1	кількість підприємств, які використовували комп'ютери	одиниць	40327
3.2	частка підприємств, які використовували комп'ютери	у % до загальної кількості підприємств	95,4
4	$К_д$	–	–
4.1	кількість підприємств, які мали доступ до мережі Інтернет	одиниць	39582
4.2	частка підприємств, які мали доступ до мережі Інтернет	у % до загальної кількості підприємств	98,2
5	$К_ф$	одиниць	10660
6	$К_{веб}$	одиниць	16240
7	$В_{см}$	одиниць	23849
8	$К_{хт}$ кількість підприємств, що купували послуги хмарних обчислень упродовж року	одиниць	4135
9	$К_{вд}$	одиниць	–
9.1	кількість підприємств, що проводили аналіз «великих даних»	одиниць	10252
9.2	кількість підприємств, на яких аналіз «великих даних» проводили	одиниць	8526

Примітка: розроблено на основі даних [24–26]

Дані в табл. 1 вказують на слабкий рівень розвитку інформаційно-комунікаційних технологій в Україні. Лише більше половини населення України мають доступ до мережі Інтернет. Високим рівнем забезпеченості інформаційно-комунікаційними технологіями характеризуються підприємства, що активно використовують мережу Інтернет в різних цілях. Це вказує на розвиток приватної інформаційної інфраструктури, що потребує ефективного захисту від інформаційних загроз з боку держави. Українські підприємства активно використовують веб-сайти, соціальні медіа для просування власної продукції в мережі Інтернет, а це свідчить про потенційні ризики загроз в інформаційному просторі.

На рис. 5 відображено динаміку фіксованого широкосмугового доступу до Інтернету в Україні у 2005–2017 рр.

Рис. 5. Динаміка фіксованого широкосмугового доступу до Інтернету в Україні у 2005–2017 рр. (на 100 осіб) [26]

Спостерігається позитивна динаміка зростання фіксованого широкосмугового доступу до Інтернету в Україні у 2005–2017 рр. Проте частка проникнення мережі Інтернет за даними Інтернет Асоціації України становила 65 % станом на серпень 2017 р. (в містах з населенням більше 100 тисяч осіб – 75 %, в селах – 54 % [27]). Кількість абонентів Інтернет станом на 1 жовтня 2018 р. – 26014,9 тисяч осіб [24].

Автор роботи [10] зазначає, що в Україні розвиток Інтернету гальмується у зв’язку з негативними факторами, а саме: застарілі телекомунікаційні мережі, низький рівень комп’ютеризації, низькі доходи населення. Тому громадяни можуть піддаватися дезінформації та пропаганді з інших інформаційних джерел. Якщо розглянути статистику кількості абонентів Інтернет за регіонами в Україні (табл. 2), то найбільша кількість у більш розвинених областях: м. Київ (13 %), Одеська область (11 %), Донецька (8 %), Дніпропетровська (7 %), Львівська (6 %), Харківська (6 %), Київська (4 %).

Таблиця 2

Кількість абонентів Інтернет за регіонами в Україні станом на 1 січня 2019 р.

Території	Усього	З них				
		домашні	у сільській місцевості		з наданням широкосмугового доступу	
			усього	у тому числі домашні	усього	у тому числі домашні
Україна	26066,8	23354,2	652,9	629,5	25312,7	22861,1
Вінницька	968,2	862,1	31,0	29,6	929,4	836,9
Волинська	576,3	513,2	11,5	10,9	558,7	501,8
Дніпропетровська	1796,5	1608,1	16,2	15,7	1746,2	1575,9
Донецька	1800,4	1608,6	16,6	16,3	1788,4	1600,6
Житомирська	689,7	616,2	28,4	28,0	669,1	603,0
Закарпатська	583,7	520,2	21,6	20,9	575,6	514,9
Запорізька	865,1	771,4	23,2	22,2	855,5	765,2
Івано-Франківська	659,8	589,4	33,8	32,8	651,7	584,2
Київська	1215,3	1088,9	19,2	18,9	1146,4	1044,3
Кіровоградська	465,7	415,3	6,5	6,0	459,1	411,0
Луганська	913,4	814,3	3,8	3,5	907,5	810,5
Львівська	1664,8	1475,6	82,0	78,9	1588,4	1425,6
Миколаївська	800,7	723,1	8,6	8,2	768,4	702,3
Одеська	2688,6	2438,6	56,5	54,9	2610,0	2388,3
Полтавська	749,8	667,3	40,2	38,6	735,1	656,4
Рівненська	593,3	529,0	25,5	24,5	579,1	519,7
Сумська	548,4	489,0	9,7	9,2	539,4	483,1
Тернопільська	511,7	454,8	38,0	35,1	505,8	451,0
Харківська	1582,4	1402,2	21,7	21,2	1522,9	1363,7
Херсонська	534,5	476,4	21,7	20,4	524,6	469,1
Хмельницька	653,1	581,3	13,9	13,3	641,4	573,7
Черкаська	692,1	614,4	15,8	15,0	667,9	598,8
Чернівецька	421,0	377,4	17,9	17,4	416,2	373,7
Чернігівська	673,7	599,9	13,7	13,2	642,8	579,9
м. Київ	3418,6	3117,5	75,9	74,8	3283,1	3027,5

Примітка: розроблено на основі даних [26]

Саме ці регіони за даними Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, мають найбільшу щільність постачальників телекомунікаційних послуг [28, 29] (у 2017 р.). Тому суб'єкти цих регіонів можуть піддаватися інформаційним загрозам більшою мірою. Це потребує встановлення пріоритетів регіональної інформаційної безпеки та фінансування заходів в першу чергу у цих регіонах.

7. SWOT-аналіз результатів дослідження

Strengths. Сильні сторони проведеного дослідження щодо оцінки розвитку інформаційної інфраструктури:

– виявлено ключові загрози інформаційній безпеці;

– оцінено стан інформаційної безпеки суб'єктів інформаційної інфраструктури;

– виявлено пріоритетні об'єкти інформаційної інфраструктури, що потребують фінансування та підвищення рівня інформаційної безпеки; забезпечує виявлення ключових загроз інформаційній інфраструктурі;

– виявлено рівень технологічного зносу об'єктів інформаційної інфраструктури;

– виявлено рівень комп'ютеризації приватного сектору інформаційної безпеки;

– встановлено рівень технологічного оснащення та розвитку підприємств;

– визначено ступінь інтеграції підприємств до медіапростору.

Weaknesses. Слабкі сторони проведеного дослідження щодо оцінки розвитку інформаційної інфраструктури:

– відсутній аналіз інформації для оцінки індикаторів, що дають змогу оцінити інформаційні загрози об'єктам, які існують в медіапросторі;

– відсутність показників розвитку інформаційної інфраструктури в регіональному розрізі;

– відсутні дані за останні часові періоди.

Opportunities. Можливості подальших досліджень системи моніторингу розвитку інформаційної інфраструктури:

– розробка інтегрального показника оцінки розвитку інформаційної інфраструктури на основі індикаторів системи моніторингу;

– розробка моделі прогнозування розвитку інформаційної інфраструктури;

– розробка моделі автоматизації процесів обчислень індикаторів системи моніторингу розвитку інформаційної інфраструктури;

– скорочення витрат на протидію інформаційним загрозам за умов своєчасного моніторингу критичних загроз на основі розробленої системи показників;

– можливість вчасного реагування на існуючі інформаційні загрози об'єктам інформаційної інфраструктури.

Threats. Загрози системі моніторингу розвитку інформаційної інфраструктури:

– швидкі темпи розвитку ІКТ призводять до трансформації загроз об'єктам інформаційної інфраструктури, а це потребує включення в систему моніторингу нових індикаторів;

– включення нових індикаторів потребує часових затрат для їх оцінки, пошуку джерел збору інформації для оцінки показників;

– суттєві обсяги фінансування для оцінки показників системи моніторингу розвитку інформаційної інфраструктури в інформаційному просторі;

– суттєві витрати на проведення досліджень та збору інформації щодо існуючих інформаційних загроз об'єктам інформаційної інфраструктури.

8. Висновки

1. Сформовано систему показників оцінювання рівня розвитку інформаційної інфраструктури в розрізі суб'єктів господарювання. Ця система включає показники моніторингу рівня інформаційної безпеки та рівня інформаційних загроз в розрізі основних суб'єктів господарювання.

2. Виокремлено основні тенденції розвитку інформаційної інфраструктури в Україні. Оцінені значення показників системи моніторингу дають змогу стверджувати про потребу в фінансуванні інформаційної інфраструктури приватного сектору. Це дасть змогу підвищити рівень доступу населення до мережі Інтернет та забезпечити захист персональної інформації, унеможливити вплив дії пропаганди та дезінформації населення. Розвиток інформаційної інфраструктури підприємств та технологій в інформаційній сфері відбувається швидкими темпами. Це зумовлено такими факторами: зростаючий рівень комп'ютеризації, технологічне переоснащення, використання підприємствами соціальних медіа та аналізу «великих даних», хмарних технологій та обчислень. Нові технології водночас дають змогу автоматизувати бізнес-процеси обробки й аналізу інформації та слугують джерелом загроз внутрішній інформацій та інформаційній інфраструктурі.

3. Сформовано основні напрямки покращення державної політики органів влади щодо розвитку інформаційної інфраструктури, до яких відносяться:

– захист персональних даних приватного та державного секторів;

– стимулювання розвитку об'єктів інформаційної інфраструктури приватного сектору;

– розвиток державно-приватного партнерства з метою розвитку інформаційної інфраструктури.

Література

1. Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України»: Указ Президента України від 06.05.2015 р. № 287/2015 / ВР України // База даних «Законодавство України». Дата оновлення: 26.05.2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015#n14

2. Стратегія кібербезпеки України: Указ Президента України від 27.01.2016 р. № 96/2016 / ВР України // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/96/2016#n11

3. Про рішення Ради національної безпеки і оборони України «Про Доктрину інформаційної безпеки України»: Указ Президента України від 29.12.2016 р. № 47/2017 / ВР України // База даних «Законодавство України». Дата оновлення: 25.02.2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017

4. Про основні засади забезпечення кібербезпеки України: Закон України від 08.07.2018 р. № 2163-VIII / ВР України // База даних «Законодавство України». Дата оновлення: 08.07.2018. URL: https://zakon.rada.gov.ua/laws/show/2163-19/conv

5. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII / ВР України // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/2469-19?lang=en

6. Моніторинг загроз у інформаційному просторі допоможе ефективніше справлятися з критичними ситуаціями. URL: https://mip.gov.ua/news/2431.html

7. Про Стратегію сталого розвитку «Україна – 2020»: Указ Президента України від 12.01.2015 р. № 5/2015. / ВР України // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/5/2015

8. Довгань О. Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки // Інформаційна безпека людини, суспільства, держави. 2015. Вип. 3 (19). С. 6–17.

9. Кобко Є. В. Моніторинг загроз національній безпеці держави: зарубіжний досвід та українські реалії публічно-правового забезпечення // Науковий вісник Національної академії внутрішніх справ. 2018. Вип. 1 (106). С. 122–134.

10. Ковальова К. В., Першко О. Л. Проектний менеджмент: соціальне проектування інновацій в організаціях // Матеріали науково-практичної конференції «Фінансові механізми інноваційного економічного розвитку в умовах євроінтеграції». Київ, 2018. 281 с.

11. Молодецька-Гринчук К. В. Аналіз впливу загроз інформаційній безпеці держави у соціальних-інтернет сервісах на сфери суспільної діяльності // Управління розвитком складних систем. 2017. Вип. 30. С. 121–127.

12. Федоренко Р. М. Контент-моніторинг інформаційного простору як чинник забезпечення інформаційної безпеки держави у воєнній сфері // Сучасний захист інформації. 2015. Вип. 2. С. 21–25.

13. Пахнін М. Л. Принципи, завдання та інструменти державної інформаційної політики України в сучасних умовах // Теорія та практика державного управління. 2014. Вип. 3. С. 87–95.

14. Ткачук Т. Ю. Механізми протидії інформаційним загрозам зовнішніх джерел // Вісник НТУУ «КПІ». 2017. Вип. 1/2 (33/34). С. 242–246.

15. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз // Інформаційне право. 2017. Вип. 10. С. 182–186.

16. Rizov V. Information Sharing for Cyber Threats // Information & Security: An International Journal. 2018. Vol. 39, Issue 1. P. 43–50. doi: http://doi.org/10.11610/isij.3904

17. Parker D. B. A Comprehensive List of Threats To Information // Information Systems Security. 1993. Vol. 2, Issue 2. P. 10–14. doi: http://doi.org/10.1080/19393559308551348

18. Fried L. Information security and new technology Potential Threats and Solutions // Information Systems Management. 1994. Vol. 11, Issue 3. P. 57–63. doi: http://doi.org/10.1080/07399019408964654

19. Kar J., Mishra M. R. Mitigating Threats and Security Metrics in Cloud Computing // Journal of Information Processing Systems. 2016. Vol. 12, Issue 2. P. 226–233. doi: http://doi.org/10.3745/jips.03.0049

20. Suchkov A. P. The information structure of threats to national security // Systems and Means of Informatics. 2017. Vol. 27, Issue 2. P. 113–124. doi: http://doi.org/10.14357/08696527170210

21. Dainow B. Threats to Autonomy from Emerging ICTs // Australasian Journal of Information Systems. 2017. Vol. 21. P. 1–16. doi: http://doi.org/10.3127/ajis.v21i0.1438

22. Monov L., Karev M. How to Counter Hybrid Threats? // Information & Security: An International Journal. 2018. Vol. 39, Issue 2. P. 113–126. doi: http://doi.org/10.11610/isij.3909

23. Підрозділ Державного центру кіберзахисту Держспецзв'язку CERT-UA. URL: https://cert.gov.ua/#recommendations

24. Використання інформаційно-комунікаційних технологій на підприємствах за 2017 рік. URL: http://www.ukrstat.gov.ua

25. Кількість абонентів зв'язку на 1 жовтня 2018 року. URL: http://www.ukrstat.gov.ua

26. Стан і розвиток зв'язку за 2017 рік. URL: http://www.ukrstat.gov.ua

27. Офіційний сайт Інтернет Асоціації України. URL: https://inau.ua/pro-asociaciyu

28. Проведено опрацювання звітів операторів про якість телекомунікаційних послуг за 2017 рік. URL: http://spz.nkrzi.gov.ua/golovna/yakist-poslug/dani-pro-yakist/

29. Обсяг реалізованих послуг у сфері телекомунікацій та поштового зв'язку за 9 місяців 2018 року. URL: http://www.ukrstat.gov.ua