УДК 342.1
DOI https://doi.org/10.24144/2307-3322.2023.77.2.11

ОЦІНЮВАННЯ ГІБРИДНИХ ЗАГРОЗ ТА СПРОМОЖНОСТЕЙ ПРОТИДІЇ ЇМ ПРИ ФОРМУВАННІ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ

Користін О.Є.,
доктор юридичних наук, професор,
Заслужений діяч науки і техніки України,
ЦСК ННІ ІБСК НА СБ України;
https://orcid.org/0000-0001-9056-5475

Свиридюк Н.П.,
доктор юридичних наук, професор;
https://orcid.org/0000-0001-9772-1119

Користін О.Є., Свиридюк Н.П. Оцінювання гібридних загроз та спроможностей протидії їм при формуванні стратегічних комунікацій.

У статті зосереджується увага на питаннях розвитку стратегічних комунікацій. Зроблено наголос на об'єктивності формування системи знань при розробленні відповідної державної політики.

На основі унікальної емпіричної бази, сформованої опитуванням суб'єктів системи громадської безпеки та цивільного захисту України, запропоновано підходи щодо оцінювання ризиків поширення гібридних загроз, пов'язаних з інформаційним середовищем, оцінюванням спроможностей відповідної системи щодо зниження зазначених ризиків та на основі аналізу статистичних закономірностей обґрунтовано пропозиції щодо формування напрямів стратегічних комунікацій у визначеному секторі безпеки України.

На основі оцінювання ризиків поширення гібридних загроз, пов'язаних з інформаційним середовищем, виділено ключові загрози, зокрема стимулювання та заохочення громадян України, які мешкають у прикордонних регіонах, до отримання 2-го громадянства всупереч законам України (53%); контроль агресором контенту у регіонах близьких до бойових дій та прикордонних районів (51%); створення та підтримка (в т.ч. фінансова) різноманітних політичних проектів з метою розхитування соціально-політичної ситуації, дискредитації керівництва держави, підбурювання населення до громадянської непокори (51%), які прямо вказують на аспекти та напрями розвитку стратегічних комунікацій; вплив на свідомість працівників органів системи МВС, шляхом цілеспрямованої дискредитації, спрямованої на зниження довіри до політичної еліти в державі (44%).

Акцентовано на тому, що гібридні загрози у формі дезінформації є інструментом гібридної агресії, якій неможливо запобігти традиційними правоохоронними заходами, а тому є потреба формування відповідної системи стійкості, яка залежить не від характеру чи рівня гібридних загроз, а від уразливості суспільства та спроможності національної правоохоронної системи забезпечувати належний рівень безпеки.

На основі моделі лінійної регресії оптимізовано перелік спроможностей, що мають найбільший вплив на обрану для аналізу гібридну загрозу.

Ключові слова: стратегічні комунікації, ризики, оцінювання ризиків, гібридні загрози, спроможності, стійкість.

Korystin O.E., Svyrydiuk N.P. Assessment of hybrid threats and capabilities to counter them in the formation of strategic communications.

The article focuses on the development of strategic communications. Emphasis is placed on the objectivity of the formation of a knowledge system in the development of appropriate public policy.

Based on a unique empirical base formed by a survey of the subjects of the public security and civil defense system of Ukraine, the author proposes approaches to assessing the risks of the spread of hybrid threats related to the information environment, assessing the capabilities of the relevant system to reduce

these risks, and, based on the analysis of statistical patterns, substantiates proposals for the formation of strategic communications in the defined security sector of Ukraine.

Based on the assessment of the risks of the spread of hybrid threats related to the information environment, the key threats are identified, in particular, stimulation and encouragement of Ukrainian citizens living in the border regions to obtain a second citizenship in violation of the laws of Ukraine (53%); control by the aggressor of content in regions close to hostilities and border areas (51%); creation and support (including financial support) of various political projects aimed at undermining the socio-political situation, discrediting the state leadership, inciting the population to civil disobedience (51%), which directly indicate the aspects and directions of strategic communications development; influence on the minds of employees of the Ministry of Internal Affairs through targeted discrediting aimed at reducing confidence in the political elite in the country (44%).

It is emphasized that hybrid threats in the form of disinformation are an instrument of hybrid aggression that cannot be prevented by traditional law enforcement measures, and therefore there is a need to form an appropriate system of resilience that depends not on the nature or level of hybrid threats, but on the vulnerability of society and the ability of the national law enforcement system to ensure an adequate level of security.

Based on a linear regression model, the author optimizes the list of capabilities that have the greatest impact on the hybrid threat selected for analysis.

Key words: strategic communications, risks, risk assessment, hybrid threats, capabilities, resilience.

Постановка проблеми. Розвиток можливостей стратегічних комунікацій щодо протидії гібридним загрозам займає відповідну нішу в системі інформаційної безпеки. Проте важливим щодо адекватності такої діяльності є достатньо об'єктивне розуміння, при формуванні відповідної державної політики, необхідності оцінювання інформаційного середовища на предмет виявлення гібридних загроз, оцінювання спроможностей і вразливостей певної системи протидії їм та оптимізація процесів реалізації конкретних заходів в системі стратегічних комунікацій.

Метою цієї статті є дослідження проблематики щодо обґрунтування формування напрямів стратегічних комунікацій, протидії гібридним загрозам, пов'язаним з інформаційним середовищем, із врахуванням рівня та специфіки відповідних спроможностей.

На основі унікальної емпіричної бази, сформованої опитуванням суб'єктів системи громадської безпеки та цивільного захисту України, запропонувати підходи щодо оцінювання ризиків поширення гібридних загроз, пов'язаних з інформаційним середовищем, оцінюванням спроможностей відповідної системи щодо зниження ризиків поширення загроз та на основі аналізу статистичних закономірностей обґрунтувати пропозиції щодо формування напрямів стратегічних комунікацій у визначеному секторі безпеки України.

Виклад основного матеріалу. Сьогодні в Україні питання, пов'язані з протидією гібридним загрозам набули великої актуальності та перебувають у центрі суспільної уваги. В останні роки у багатьох наукових роботах значна увага приділяється саме окремим проблемам протидії гібридним загрозам в Україні. Зокрема питання, пов'язані з розробкою напрямів щодо протидії гібридним загрозам ставали предметом досліджень багатьох відомих учених: О. Акульшина [1], Р. Арзуманяна [2], З. Гбур [3], О. Заруби [2], Л. Компанцевої, С. Кудінова [1], Є. Магди [4], М. Мальського [8], В. Мартинюка [5], В. Предборського [6], І. Руснака [7] та інших [9, 10]. Разом з тим, усвідомлення феномену гібридної війни, а також її масштабів, вимагає напрацювання відповідної методології аналізу гібридних загроз, що формує у свою чергу достатній масив знань для формування обґрунтованої та ефективної державної політики щодо протидії гібридним загрозам.

Зростання сучасного суспільства нерозривно пов'язане із запобіганням різноманітним загрозам, які посилюються у період реформування будь-якої сфери життєдіяльності суспільства. Питання протидії гібридним загрозам достатньо широко та комплексно охоплює проблеми національної безпеки. Зазначене, перш за все, потребує суттєвого аналізу ситуації, дослідження тих факторів, що спричинюють неспроможність ефективного реагування на протидію гібридним загрозам. Водночас, об'єктивність та обґрунтованість результатів дослідження потребує відповідної методологічної бази. Наразі, вкрай важливо забезпечити формування відповідної політики розвитку стратегічних комунікацій із врахуванням оцінки гібридних загроз в інформаційному середовищі та їх кореляцій зі спроможностями протидії, що реально та найбільше впливають на стан безпеки в нашому суспільстві.

Фахівці та науковці у сфері державної безпеки вказують на дієвість у протидії гібридним загрозам саме стратегічних комунікацій, ефективність яких зумовлюється відповідним алгоритмом дій: оцінювання інформаційного середовища та гібридних загроз; вироблення стратегічної концепції; розроблення загальнодержавного стратегічного наративу; визначення ефективності стратегічнокомунікативної діяльності [1].

У контексті предмету нашого дослідження варто зосередитись на першому етапі зазначеного алгоритму: оцінюванні інформаційного середовища та гібридних загроз. Емпіричною базою цього аналізу є попереднє дослідження гібридних загроз у сфері громадської безпеки та цивільного захисту. І не зважаючи на певну обмеженість предмету обраної емпіричної бази, з методологічної точки зору актуальність цього аналізу ніяким чином не втрачається.

На основі попереднього аналізу, проведеного робочою групою [10, 11], ідентифіковано 131 гібридну загрозу у сферах громадської безпеки та цивільного захисту (рис. 1).

У зв'язку з тим, що гібридні загрози оцінювалися за двома характеристиками «ймовірність» і «наслідки», подальший аналіз щодо визначення їх рейтингу здійснювався на основі визначення середнього значення.

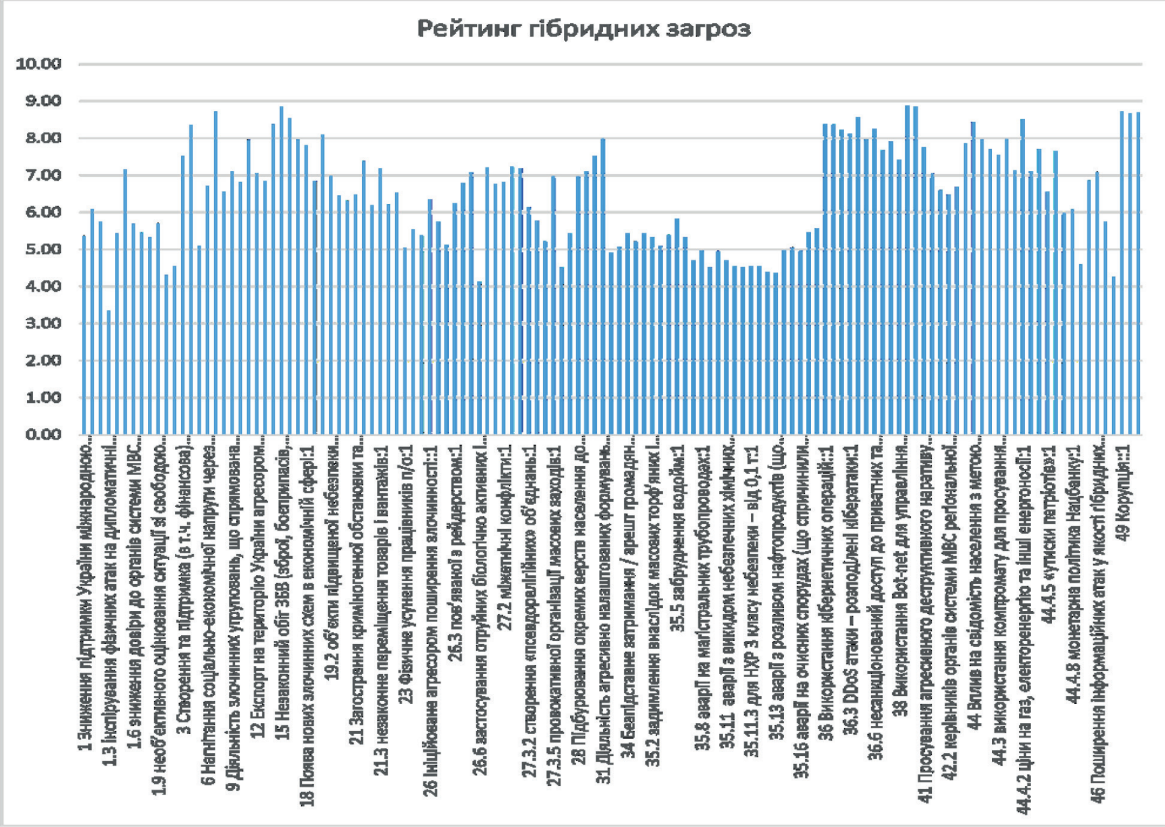


Рис 1. Рейтинг гібридних загроз у сферах громадської безпеки та цивільного захисту

На основі факторного аналізу та експертного оцінювання щодо змісту гібридних загроз і середовища поширення перші дві групи найзначніших та значних гібридних загроз розподілено у 6 підгруп, що характеризуються наступним чином [12, 13]:

- гібридні загрози, пов'язані з інформаційним середовищем;
- гібридні загрози, пов'язані з використанням кібероперацій;
- гібридні загрози, пов'язані з поширенням злочинності;
- гібридні загрози, пов'язані з діяльністю ОКІ (об'єкти критичної інфраструктури);
- гібридні загрози, пов'язані з провокуванням громадянської непокори, порушення громадського порядку;
- гібридні загрози, пов'язані з корупцією.

До групи гібридних загроз, пов'язаних з інформаційним середовищем віднесено 40 гібридних загроз (рис. 2).

Гібридні загрози, що пов'язані з інформаційним середовищем, %	Середнє	МВС апарат	НПУ	НГУ	ДСНС	ДПСУ	ДМСУ	ГСЦ
1 Зниження підтримки України міжнародною спільнотою шляхом:	28,62	42,83	28,82	37,76	18,51	20,35	29,61	22,59
1.1 необ'єктивного оцінювання ситуації щодо України	30,70	40,70	31,21	27,87	21,26	23,80	33,46	27,00
1.2 підтримки популістських політсил в Європі	26,84	40,44	27,97	19,74	22,70	16,13	24,98	23,57
1.3 інспірування фізичних атак на дипломатичні представництва в Україні	15,12	31,24	15,02	9,71	9,25	9,18	15,21	11,57
1.4 учинення актів наруги над чутливими пам'ятками історії/плюндрування релігійних об'єктів	22,62	34,49	23,25	21,19	14,07	18,05	21,46	21,96
1.5 просування кандидатів (лояльних до країни-агресора) на керівні посади у міжнародних організаціях (у т.ч. недержавних)	41,97	**54,08**	44,09	45,23	32,63	33,55	37,96	33,71
1.6 з метою зниження довіри до органів системи МВС України	31,22	39,81	34,71	24,26	18,05	17,95	29,73	24,04
1.7 з метою зменшення міжнародної технічної допомоги для реформування органів системи МВС України	27,67	40,95	29,43	20,00	21,51	19,09	23,74	24,18
1.8 з метою зниження ефективності моніторингу безпекової / інформаційної сфери	26,75	40,16	28,92	20,09	19,88	15,76	24,06	16,36
1.9 з метою необ'єктивного оцінювання ситуації зі свободою ЗМІ	27,02	34,35	28,76	21,23	17,38	23,13	26,74	17,96
1.10 з метою використання інструментів міжнародних організацій для безпідставної затримки / арешту громадян України за кордоном	21,74	31,33	21,77	25,41	16,79	15,71	22,84	16,57
2 Отримання патронату над державою через вплив агресором на органи системи МВС.	30,10	43,79	30,18	28,09	25,58	22,64	30,79	23,36
3 Створення та підтримка (в т.ч. фінансова) різноманітних політичних проектів з метою розхитування соціально-політичного стану, дискредитації керівництва держави, збудження населення до громадянської непокори тощо	**51,36**	**54,87**	**54,24**	**61,01**	33,00	43,93	**51,77**	44,46
4 Стимулювання та заохочення громадян України, що мешкають в прикордонних регіонах, до отримання 2-го громадянства всупереч закон Укр	**53,33**	**64,22**	**53,13**	**66,15**	47,88	41,80	**53,20**	**60,18**
5 Дискредитація (фізичне насилля) відомих діячів у державі, активістів Майдану	27,09	41,57	26,01	20,62	22,49	24,67	30,62	19,11
6 Нагнітання соціально-економічної напруги через економічні інструменти: формування негативного ставлення у населення	38,83	45,90	40,21	42,15	29,54	27,61	42,06	28,39
25 Підбурювання до саботажу або бездіяльності посадових осіб СГБіЦЗ в умовах агресії	32,65	47,52	33,24	35,38	20,29	25,29	33,33	29,50
39 Контроль агресором контенту у регіонах близьких до бойових дій та прикордонних районів	**51,04**	**61,16**	**51,62**	36,40	42,48	45,13	**52,18**	**58,57**
40 Провокаційна діяльність контрольованого агресором медіа ресурсу через приховування кінечного бенефіціара	48,14	**58,46**	47,80	37,23	45,26	35,34	**52,73**	**53,61**
41 Просування агресивного деструктивного наративу щодо органів і працівників системи МВС через інформаційні засоби	41,37	48,57	42,38	43,12	40,73	29,13	41,47	33,50
42 Вплив на свідомість прац органів системи МВС, шляхом цілеспрямованої дискредитації, спрямованої на зниження довіри до:	38,60	48,38	40,81	39,03	29,60	25,31	40,13	17,89
42.1 керівників органів системи МВС нижньої (територіальної, операційної) ланки управління	34,42	39,94	36,91	33,32	25,35	26,69	34,47	18,04
42.2 керівників органів системи МВС регіональної ланки управління	34,03	39,83	36,48	35,74	23,33	25,11	34,86	18,64
42.3 керівників ЦОВВ та підрозділів системи МВС	34,56	40,62	36,15	35,56	25,86	27,04	37,32	17,61
42.4 політичної еліти в державі	43,59	49,10	45,88	**51,47**	32,92	32,47	44,43	31,07
44 Вплив на свідомість населення з метою дискредитації влади, органів і працівників системи МВС шляхом:	49,15	**55,59**	**50,89**	47,69	36,44	47,66	**50,65**	29,93
44.1 використання цільових інформаційно-психологічних операцій	43,38	**50,40**	45,02	41,19	30,10	39,29	47,52	23,57
44.2 використання компромату для усунення з посади працівників органів системи МВС	37,82	45,38	40,09	40,35	28,84	29,09	36,64	25,25
44.3 використання компромату для просування окремих рішень (негативних для держави, органів системи МВС)	40,49	49,67	41,64	49,49	33,70	34,10	38,04	33,57
44.4 проведення компл інформкампаній із штучної поляризації та радикалізації сусп, використовуючи збудженість громадян до проблеми:	44,62	49,90	46,84	45,19	32,89	39,70	44,71	30,07
44.4.1 «євробляхи»	31,92	40,48	33,21	31,25	23,37	21,28	34,78	21,57
44.4.2 ціни на газ, електроенергію та інші енергоносії	47,83	**58,59**	47,86	37,19	37,79	42,96	**52,88**	44,04
44.4.3 слідство по справах Майдану	34,78	46,05	35,33	25,54	25,66	30,49	39,52	17,82
44.4.4 державна політика по ОРДЛО	43,86	**51,48**	44,79	34,73	35,21	32,31	**50,29**	34,36
44.4.5 «утиски патріотів»	32,20	39,21	32,83	30,02	22,78	26,03	36,89	22,39
44.4.6 «провалені реформи»	40,85	**52,94**	41,49	29,05	28,13	32,72	46,11	37,00
44.4.7 вкладники збанкрутілих банків	27,04	38,65	26,88	21,27	18,46	18,39	33,68	18,00
44.4.8 монетарна політика Нацбанку	30,79	36,54	32,29	22,95	17,71	21,16	36,10	27,18
44.4.9 релігійного супротиву впровадженню документів з безконтактним електронним носієм (біометричні), …..	19,74	24,68	20,63	14,51	10,71	12,12	24,92	11,12
46 Поширення інформаційних атак у якості гібридних загроз СГБіЦЗ	35,83	45,05	35,22	31,56	32,75	31,88	39,44	27,21

Рис. 2. Ризики поширення гібридних загроз, пов'язаних з інформаційним середовищем

Незважаючи на значну варіативність оцінювання різними експертними групами ризиків поширення гібридних загроз щодо ключових з них в інформаційному середовищі, найвищим рівнем ризику (більше 50%) характеризуються та є найзначнішими такі:

- стимулювання та заохочення громадян України, що мешкають в прикордонних регіонах, до отримання 2-го громадянства всупереч законам України – 53%;
- контроль агресором контенту у регіонах близьких до бойових дій та прикордонних районів – 51%;
- створення та підтримка (в т.ч. фінансова) різноманітних політичних проектів з метою розхитування соціально-політичної ситуації, дискредитації керівництва держави, підбурювання населення до громадянської непокори тощо – 51%;
- провокаційна діяльність контрольованого агресором медіа ресурсу через приховування кінцевого бенефіціара – 48%;
- вплив на свідомість населення з метою дискредитації влади, органів і працівників системи МВС – 49%.

Значними за рівнем ризику (40-50%) убачаються такі загрози:

- вплив на свідомість працівників органів системи МВС, шляхом цілеспрямованої дискредитації, спрямованої на зниження довіри до політичної еліти в державі – 44%;
- використання цільових інформаційно-психологічних операцій – 43%;
- просування кандидатів (лояльних до країни-агресора) на керівні посади у міжнародних організаціях (у т.ч. недержавних) – 42%;
- нагнітання соціально-економічної напруги через економічні інструменти: формування негативного ставлення у населення – 39%;
- просування агресивного деструктивного наративу щодо органів і працівників системи МВС через інформаційні засоби – 41%;
- використання компромату для просування окремих рішень (негативних для держави, органів системи МВС) – 40%;
- використання компромату для усунення з посади працівників органів системи МВС – 38%;
- проведення комплексних інформкампаній зі штучної поляризації та радикалізації суспільства, використовуючи збудженість громадян – 45% - до проблеми:
- ціни на газ, електроенергію та інші енергоносії – 48%;
- державна політика по ОРДЛО – 44%;
- «провалені реформи» - 41%.

Наразі зазначений перелік та рівень ризику поширення оцінених гібридних загроз прямо вказує на аспекти та напрями розвитку стратегічних комунікацій, зокрема щодо контенту у регіонах близьких до бойових дій та прикордонних районів, впливу на свідомість населення з метою дискредитації влади, просування агресивного деструктивного наративу, використання цільових інформаційно-психологічних операцій тощо.

Водночас ризик-орієнтований підхід акцентує увагу не лише на оцінюванні ризиків поширення гібридних загроз, а й на рівні можливостей та спроможностей протидії гібридним загрозам.

Можливості – це зовнішні фактори, що сприятимуть підвищенню ефективності протидії гібридним загрозам у секторі громадської безпеки та цивільного захисту України, а їх упровадження (реалізація) має місце в майбутньому.

Важливою характеристикою оцінювання ризиків у системі протидії гібридним загрозам у сферах громадської безпеки та цивільного захисту є оцінювання спроможності щодо протидії ідентифікованим гібридним загрозам – це внутрішні фактори, що характеризують різні сторони системи кримінальної юстиції (оцінювання нинішнього фактичного стану).

Враховуючи зовнішній характер загроз в умовах гібридної війни, тобто їх поширення за безпосередньої чи опосередкованої ініціативи агресора або третьою стороною в інтересах агресора, класичний академічний підхід щодо протидії цим загрозам, а тим більше щодо запобігання їх поширенню, є малоефективним.

За таких умов причини поширення гібридних загроз завжди матимуть зовнішню характеристику детермінації, і найбільш імовірно, що їх провокація буде актуальною увесь період активності воєнної агресії. За таких обставин важко говорити про упереджувальний вплив на причини поширення загроз без ліквідації факту агресії.

Для забезпечення ефективної діяльності протидії гібридним загрозам, які є інструментом гібридної війни, важливим є формування відповідних та адекватних методологічних засад. Із цього приво-

ду доречно звернутися до досвіду країн-членів ЄС та НАТО, які саме в період активізації гібридної агресії на території України, оцінюючи це як розбалансування глобального безпекового середовища, визначили безпекові пріоритети й актуалізували проблему розбудови «стійкості». Поняття «стійкість» є не просто вдалим текстовим конструктом, що використовується розвиненими країнами та міжнародними організаціями. За своєю сутністю стійкість – новітній концепт сучасної теорії національної безпеки, що має прикладне значення для формування державної політики у сфері розбудови безпекового середовища в умовах протистояння гібридним загрозам [15].

Гібридні загрози у формі дезінформації, що є інструментом гібридної агресії та якому неможливо запобігти традиційними правоохоронними заходами (тим більше за умови використання переважно заходів реактивного характеру), спричиняє потребу у формуванні нового підходу, зокрема формування стійкості, що, в свою чергу, має бути імплементованою інституційною складовою державної політики національної безпеки.

Саме тому Стратегія національної безпеки України, введена в дію Указом Президента України від 14 вересня 2020 року № 392/2020, зазначає, що оцінка ризиків, ідентифікація загроз і визначення вразливостей є складовими запровадження національної системи стійкості для забезпечення високого рівня готовності суспільства і держави до реагування на загрози [16].

Тобто, безпекове середовище в умовах гібридної війни першочергово залежить не від характеру чи рівня гібридних загроз, а від уразливості суспільства та спроможності національної правоохоронної системи забезпечувати належний рівень безпеки.

Наприклад, стійкість у сфері протидії загрозам в умовах гібридної війни формується, виходячи з принципової невизначеності характеру та форм гібридних загроз, часу їх прояву та поширення, і набуває змісту цільової установки на засадах нормативного впровадження та як запобіжних заходів, системи оцінювання ризиків поширення гібридних загроз, визначення уразливості суспільства та спроможності правоохоронних органів.

Тож, специфіка вітчизняної правоохоронної діяльності має враховувати вплив гібридної війни на поширення загроз і забезпечувати розбудову стійкості українського суспільства.

Саме тому подальший аналіз зосереджуватиметься на оцінюванні спроможностей щодо протидії гібридним загрозам у сферах громадської безпеки та цивільного захисту та визначення відповідних вразливостей.

Загалом ідентифіковано та оцінено 71-у спроможність протидії гібридним загрозам, які і формують та забезпечують стійкість системи цивільної безпеки в Україні. Загальна картина достатньо варіативна, дещо розмита за експертними групами, хоча має місце загальна тенденція сприйняття генеральною сукупністю експертного середовища, що потребує деталізації аналізу (рис.3).

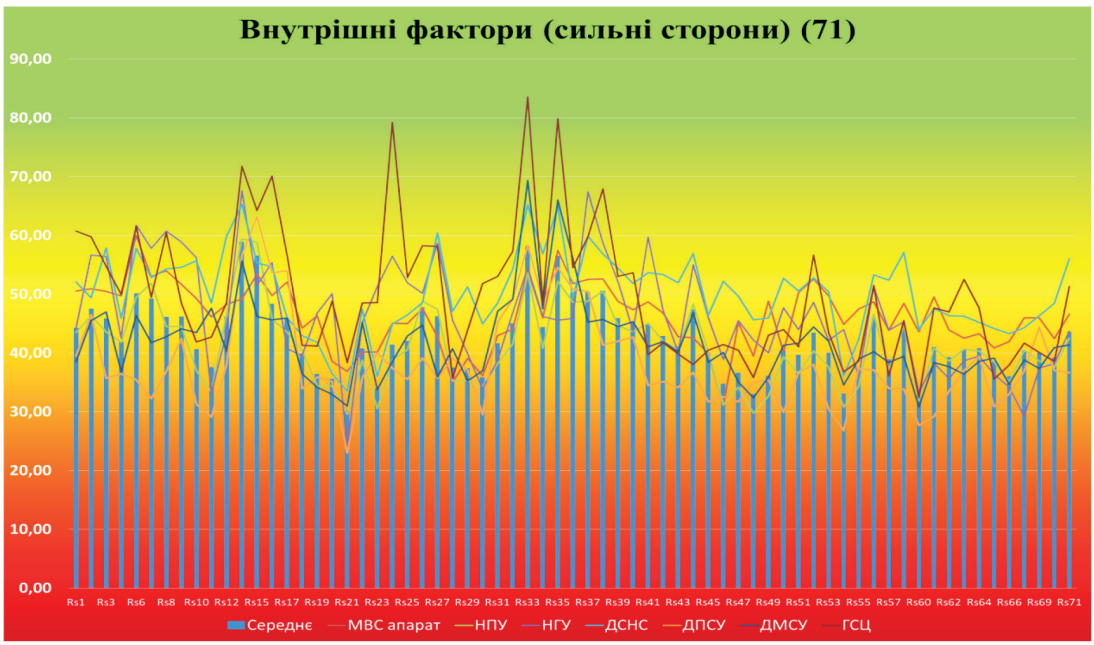


Рис. 3. Рівень спроможностей / вразливостей системи протидії гібридним загрозам

Наразі аналіз спроможностей не завершується їх описовими статистиками. Важливим є зіставлення кожної загрози із системою спроможності/вразливості (низкою індикаторів). Директиви ЄС щодо протидії гібридним загрозам прямо вказують на необхідність пошуку прихованих зв'язків, зокрема і щодо конкретних загроз з ключовими, за своїм впливом на них, спроможностями / вразливостями [17, 18]. Таке завдання вирішується побудовою відповідної прогнозної моделі поширення інформаційних гібридних загроз за умови підвищення ключових спроможностей та зниження рівня ризику вразливості системи протидії інформаційним гібридним загрозам.

Гіпотетично внутрішні фактори характеризуються певним статистичним зв'язком з окремими гібридними загрозами і можуть прямо або протилежно впливати на зниження рівня ризику поширення загрози. Застосувавши модель лінійної регресії, визначено оптимальну залежність гібридної загрози «Вплив на свідомість працівників органів системи МВС, шляхом цілеспрямованої дискредитації, спрямованої на зниження довіри до політичної еліти в державі» від змінних, що характеризують ефективність діяльності органів системи цивільної безпеки щодо протидії гібридним загрозам (табл. 1).

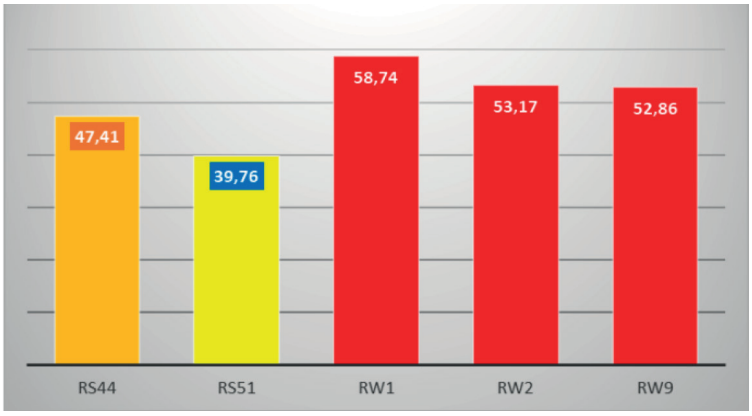
Таблиця 1

Модель лінійної регресії «Вплив на свідомість працівників органів системи МВС, шляхом цілеспрямованої дискредитації, спрямованої на зниження довіри до політичної еліти в державі»

Model	Factor[a]				
	Unstand factors		Standard factors	т	P value
	B	Std. Err.	Beta		
(Constant)	13,886	3,333		4,188	0,000
RS44	-0,154	0,051	-0,160	-3,110	0,000
RS51	0,290	0,055	0,277	5,396	0,000
RW1	0,105	0,037	0,128	2,776	0,006
RW2	0,131	0,034	0,177	3,830	0,000
RW9	0,141	0,035	0,180	4,020	0,000

Із загального переліку індикаторів (71), що характеризують ефективність правоохоронної системи у протидії гібридним загрозам (можливості та спроможності), 5 із них мають найбільший вплив на загрозу «Вплив на свідомість працівників органів системи МВС, шляхом цілеспрямованої дискредитації, спрямованої на зниження довіри до політичної еліти в державі», зокрема:

- RS44 - Рівень особистісної стійкості персоналу органів системи МВС до несприйняття дезінформації;
- RS51 - Відповідність початкової (базової) підготовки;
- RW1 - Недосконале нормативно-правове забезпечення діяльності органів системи МВС;
- RW2 - Дискредитація реформи органів системи МВС окремими працівниками;
- RW9 - Недостатній рівень професійної підготовки управлінського (начальницького) рівня.



Водночас усі предиктори за своїм невисоким рівнем оцінювання ризику характеризують більше вразливість системи стійкості, але по-різному (відповідно до визначеного моделлю коефіцієнта) впливають на зниження рівня ризику зазначеної загрози (Рис.4).

Рис. 4. Оцінка ризику визначених моделлю спроможностей

Прогнозуючи підвищення спроможності за ключовими предикторами на 20% (табл. 2), ризик поширення гібридної загрози «Вплив на свідомість працівників органів системи МВС, шляхом цілеспрямованої дискредитації, спрямованої на зниження довіри до політичної еліти в державі» зменшився до 28,09 % (більше ніж на 10%).

Таблиця 2

Оцінка ризику поширення гібридної загрози за умови підвищення спроможності на 20%

Model and forecast Coeff	P value	Rating +/-20%	
13,886	0,000		
-0,154	0,000	67,41	-10,35239099
0,290	0,000	39,76	11,5234602
0,105	0,006	38,74	4,05219901
0,131	0,000	33,17	4,355323461
0,141	0,000	32,86	4,624063938
RA = 28,09 %			

Висновки. Таким чином, розглянута модель лінійної регресії визначає пріоритетні фактори підвищення ефективності діяльності суб'єктів системи цивільної безпеки та оптимізує ключові напрями розвитку спроможностей, зосереджуючи увагу лише на окремих з них, а також формує базові засади для прогнозу зниження рівня ризику поширення гібридної загрози «Вплив на свідомість працівників органів системи МВС, шляхом цілеспрямованої дискредитації, спрямованої на зниження довіри до політичної еліти в державі» за умови підвищення спроможності правоохоронної системи щодо протидії інформаційним гібридним загрозам.

Список використаних джерел:

1. Стратегічні комунікації для безпекових і державних інституцій: практичний посібник / [Л. Компанцева, О. Заруба, С. Череватий, О. Акульшин; за заг. ред. О. Давліканової, Л. Компанцевої]. Київ: ТОВ «ВІСТКА», 2022. 278 с.
2. Арзуманян Р.В. Определение войны в 21 веке. Обзор XXI ежегодной конференции по стратегии Института стратегических исследований Армейского военного колледжа, 6-8 апреля 2010. Ереван, 2011. 48 с.
3. Гбур З.В. Актуальні гібридні загрози економічній безпеці України. *Інвестиції: практика та досвід*. № 7/2018. С. 97–99.
4. Магда Є.М. Гібридна війна: сутність і структура феномену. *Міжнародні відносини: Серія «Політичні науки»*. 2014. № 4. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/2489.
5. Мартинюк В. Гібридні загрози в Україні і суспільна безпека. Досвід ЄС і східного партнерства. Київ. 2018. 106 с.
6. Предборський В.А. «Гібридна» війна як відбиття закономірностей розвитку суспільства незавершеної модернізації. *Формування ринкових відносин в Україні.* 2014. № 10. С. 13–18.
7. Руснак І.С. Воєнна безпека України у світлі реформування сектора безпеки і оборони. *Наука і оборона*. 2015. № 2. С. 9–14.
8. Транскордонна безпека: політико-правовий, соціально-економічний, гуманітарний та екологічний вимір: Зб. мат. Міжн. наук.-практ. Конф., Львів, 21 квіт. 2017 р. / Упорядники: М.З. Мальський, О.С. Кучик, Р.В. Вовк. Львів: Факультет міжнародних відносин, 2017. 96 с.
9. Addressing Hybrid Threats. Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue Printed by: Arkitektkopia AB, Bromma 2018.
10. Користін О.Є., Свиридюк Н.П., Ковальчук Т.І. Гібридні загрози у секторі цивільної безпеки в Україні. *Наука і правоохоронна*. 2019. № 3 (45). С. 69–79.
11. Korystin O. Y., Sviridyuk N. P., Kovalchuk T. I. Hybrid threats in the civil security sector in Ukraine. *Проблеми законності*. 2019. Вип. 147. С. 163–175.
12. Korystin, Oleksandr and Svyrydiuk, Nataliia (2021), "Activities of Illegal Weapons Criminal Component of Hybrid Threats", Proceedings of the International Conference on Economics, Law and Education Research (ELER 2021), Series: Advances in Economics, Business and Management Research, vol.170, 22 March, pp. 86–91.

13. Nataliia Svyrydiuk, Yaroslav Likhovitskyy, Pavel Polián «Information Threats in the Context of Hybrid War». Proceedings of the International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research (BAMBEL2021). Series: Advances in Economics, Business and Management Research, vol. 188.
14. Helsinki in the era of hybrid threats – Hybrid influencing and the city City of Helsinki, publications of the Central Administration 2018.
15. Демедюк С.В., Користін О.Є. Стійкість системи кібербезпеки та її забезпечення в НАТО. Наука і правоохоронна. 2023. № 1. С. 69–79.
16. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 р. «Про Стратегію національної безпеки України. Указ Президента України від 14 верес. 2020 р. № 392/2020.
17. Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats - a European Union response / European Commission. URL: http://eur_lex.europa.eu/legal_content/EN/TXT/PDF/?uri=CELEX:52016JC00_18&from=EN.
18. Joint Report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats - a European Union response. EU Council. URL: http://data.consilium.europa.eu/doc/document/ST_11539_2017_INIT/en/pdf.