УДК 351.751+34.07:004.056(477)

Глобенко Сергій

ORCID iD 0000-0002-9751-4213
e-mail: svhlobenko@ukr.net

МОДЕЛЮВАННЯ ПУБЛІЧНОГО УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЙНОГО ПРОСТОРУ В КОНТЕКСТІ ЗАСТОСУВАННЯ РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ

https://doi.org/10.33269/2618-0065-2024-1(15)-67-81

Анотація. Моделювання публічного управління захистом інформаційного простору в сучасному світі є однією з ключових проблем з огляду на постійний розвиток, удосконалення технологій, геополітичну нестабільність і зростання та урізноманітнення загроз. Практикоорієнтований підхід, обґрунтований з урахуванням набутого досвіду, дає змогу аналізувати сценарії загроз, передбачати їхні наслідки та відшуковувати ефективні методи і способи реагування на сучасні виклики, які стоять перед державою в контексті забезпечення її національної безпеки, та захищати відповідним чином національні інтереси. Це дослідження, в основу якого покладено теорії Чорного Лебедя та Сірого Носорога, вказує на необхідність урахування непередбачуваних ризиків та загроз, з якими має справу чи може потенційно зіткнутися система публічного управління, адже їх недооцінка або нехтування ними може призвести до серйозних наслідків для системи національної безпеки. В умовах сьогодення питання гарантування інформаційної безпеки держави стає пріоритетом унаслідок наявності ризиків щодо дестабілізації національного інформаційного простору. Зокрема, в контексті України нині важливо враховувати принаймні чотири ключові напрями дестабілізації суспільно-політичної ситуації, аби мати можливість розробляти ефективні стратегії реагування, протидії та захисту. Наведена модель моніторингу інформаційного простору, яка складається з низки послідовних і взаємозалежних елементів, може стати підґрунтям для забезпечення ефективного захисту інтересів держави у нинішніх турбулентних обставинах. З огляду на попередні дослідження рекомендовано розвивати ризик-орієнтований підхід до організації системи управління захистом інформаційного простору задля мінімізації та нейтралізації можливих наслідків загроз в означеній сфері.

Ключові слова: інформаційний простір держави, інформаційна безпека, захист інформаційного простору, державна політика в інформаційній сфері, механізми державного управління, управління ризиками, ризик-орієнтований підхід, моделювання.

Постановка проблеми. Моделювання публічного

управління захистом інформаційного простору в контексті застосування ризик-орієнтованого підходу є надзвичайно актуальною проблемою в сучасному світі, де забезпечення інформаційної безпеки перетворюється на одне з найбільш злободенних завдань будь-якої держави світу, вагомість якої посилюється внаслідок геополітичні нестабільності в умовах сьогодення. Практико-орієнтований підхід до моделювання публічного управління уможливлює розроблення інструментарію з управління ризиками, пов'язаними з імовірними загрозами та вразливостями інформаційного простору, надаючи змогу для аналізу сценаріїв загроз, передбачення їхніх наслідків та розроблення ефективних стратегій захисту і протидії.

Моделювання публічного управління захистом інформаційного простору стає нагальною необхідністю в умовах постійного нарощування технологічних можливостей та невпинного зростання складності загроз для інформаційного простору держави. Воно дає змогу забезпечити ефективну реакцію на виклики сучасного інформаційного простору та захистити національні інтереси в динамічному цифровому середовищі.

Аналіз останніх досліджень і публікацій. В основу запропонованого дослідження покладено теорію Чорного Лебедя Н. Талеба, за якою вважається, що будь-яка подія є винятковою, абсолютно несподіваною, непередбачуваною в минулому; вона має значну силу впливу; їй властива ретроспективна, а не проспективна передбачуваність, що полягає у пошуку пояснення цієї події після її настання задля того, аби вона була зрозумілою й передбачуваною [1, с. 7]. Дослідник критикує ризик-орієнтований підхід, наголошуючи на тому, що людство дивиться на світ зсередини моделі, відсікаючи ризики, не передбачені нею, й фокусуючись на відомому. У контексті застосування означеної теорії на практиці щодо інформаційних чинників він обґрунтовує її так: «наша реакція на інформацію», – стверджує автор, – «залежить не від її логічного змісту, а від того, у якому контексті вона постає і як взаємодіє з нашою соціально-емоційною системою» [1, с. 76].

У продовження згаданої теорії М. Вакер пропонує власну – Сірого Носорога, доповнюючи попередню, зокрема в аспекті «невідомого відомого» Сірого Носорога – доступної нам інформації, якій, однак, не надається належного значення. «Сірі Носороги», – зауважує авторка, – «це загрози, які ми повинні бачити, але часто не бачимо, або які ми бачимо, але навмисно ігноруємо. Більшість Сірих Носорогів – це не сигнали, які були надто слабкими, а слухачі, які вирішили їх ігнорувати, і системи, які заохочують і сприймають як норму нашу неспроможність реагувати. Але, як правило, якщо загроза настільки очевидна, що розумна людина може її побачити, то це Сірий Носоріг, а не Чорний Лебідь» [2, с. 29].

Метою цієї публікації є теоретико-методологічне обґрунтування й розроблення практикоорієнтованих підходів до моделювання публічного управління захистом інформаційного простору в контексті застосування ризик-орієнтованого підходу.

Методи дослідження. У роботі використано загальнонаукову методологію проведення наукових досліджень. Так, застосовано методи емпіричних досліджень – спостереження, опису, узагальнення й класифікації (для розгляду предмета дослідження), моделювання (з метою вивчення об'єкта наукового пошуку за допомогою створення та дослідження його теоретичної моделі, побудованої з урахуванням практикоорієнтованого підходу, що за своїми властивостями відтворює властивості досліджуваного об'єкта). Також використано методи теоретичних досліджень – аналізу і синтезу (з метою розгляду проблеми моделювання публічного управління захистом інформаційного простору в контексті застосування ризик-орієнтованого підходу через її розчленовування на окремі складові елементи й подальшого їх об'єднання у цілісну систему), ідеалізації (в процесі творення ідеалу через виокремлення та узагальнення окремих ознак реальних явищ), індукції та дедукції (для формулювання висновків і результатів із проведеного дослідження шляхом сходження від загального до конкретного і навпаки).

Виклад основного матеріалу. Інформаційна сфера держави та проблематика забезпечення її захисту завжди

перебуває у фокусі пильної уваги. Нехтування чи недостатнє акцентування на інформаційних чинниках гарантування національної безпеки може завдати незворотних втрат і мати суттєвий вплив на подальший розвиток її складових частин.

Інформаційна дестабілізація України протягом періоду повномасштабного вторгнення держави-агресора концентрується на чотирьох ключових напрямах, зокрема:

– дискредитація військово-політичного керівництва держави;

– розкол української еліти з руйнуванням підвалин державності;

– деморалізація сил безпеки й сил оборони;

– інформаційно-психологічний вплив з метою дезорієнтації населення [3].

У контексті нашого дослідження викладене вище має суттєве значення, адже дає змогу зосередити увагу на головних проблемних аспектах забезпечення захисту інформаційного простору держави, виокремивши їхній основний фокус та пропонуючи ймовірнісні шляхи їх подолання чи мінімізації їхніх наслідків із застосуванням ризик-орієнтованого підходу до моделювання сфери публічного управління.

У розвиток наведеної тези автори монографії наголошують на тому, що нині «… майже усі провідні держави світу перебувають у кризових ситуаціях, обумовлених неадекватною та несвоєчасною оцінкою характеру, масштабів, інтенсивності, спрямованості, структурно-змістовних особливостей сучасних небезпек, загроз, викликів і ризиків міжнародній, регіональній та національній безпеці» [4, с. 54]. Вони визначили п’ять груп глобальних ризиків, які з часом можуть трансформуватися, однак матимуть потужний вплив на ефективність і стабільність соціальних систем, а саме: економічні, геополітичні, екологічні, соціальні й технологічні (зокрема системні збої інформаційної інфраструктури; втрата баз даних; кібернетичні війни; втручання в інформаційний приватний простір тощо) [4, с. 133].

Вважається, що причинами виникнення факторів ризику у функціонуванні системи державного управління в умовах надзвичайних ситуацій є:

– відсутність можливості вичерпного прогнозування процесів, які відбуваються в нестабільному зовнішньому середовищі;

– відсутність вичерпної інформації про ймовірні надзвичайні ситуації під час планування та організації діяльності системи державного управління в умовах надзвичайних ситуацій, неякісний її аналіз унаслідок появи нових загроз та небезпек;

– вплив суб'єктивних чинників на результати аналізу (низький рівень кваліфікації, необ'єктивність та приховування частини інформації тощо) [5, с. 463].

Одним із варіантів побудови системи реагування на загрози, що є основою для забезпечення стабільного функціонування системи публічного управління з урахуванням ризик-орієнтованого підходу, є підхід, запропонований урядом Великобританії у формі Національного реєстру ризиків (NRR) – оцінювання найбільш серйозних ризиків національній безпеці держави [6], який містить загрози життю, здоров'ю, суспільству, критичній інфраструктурі, економіці та державному суверенітету.

За методологією, покладеною в основу розроблення Національного реєстру ризиків, до нього входять ті ризики, прояви яких мають найгірший прогноз, найбільш несприятливий раціональний сценарій розвитку подій. Запропоновані сценарії не є реальним прогнозом того, що найімовірніше станеться чи може потенційно відбутися, натомість вони показують найгірший вірогідний прояв цього конкретного ризику. Вказаний підхід містить дані про можливості, необхідні для реагування на надзвичайну ситуацію та подальше відновлення після її настання, якщо ризик все ж таки матеріалізується, що загалом дає змогу компетентним органам публічного управління здійснювати відповідні заходи. Він зосереджується на найбільш гострих ризиках, які за своєю суттю є окремими подіями, що потребують екстреного реагування.

Національний реєстр ризиків у редакції 2023 року містить інформацію про 89 ризиків у межах 9 тематичних напрямів, а саме: тероризм, кіберзагрози, загрози державі, географія та

дипломатія, аварії та системні збої, природні та екологічні небезпеки, здоров'я людини, тварин і рослин, суспільні загрози, конфлікти й нестабільність.

За оцінкою, наведеною в Національному реєстрі ризиків, найменший вплив на сферу національної безпеки Великобританії мають такі ризики, як землетрус (з імовірністю настання <0,2%), збій інфраструктури водопостачання або втрата питної води (0,2–1%), неплатоспроможність, що впливає на постачання палива (5–25%), міжнародна терористична атака чи епіфітотія (>25%). А найбільш значущий (катастрофічний) вплив на стабільність системи матимуть ядерні аварії та викиди радіоактивних речовин (імовірність <0,2%), масштабні ХБРЯ атаки та збої в роботі національної електроенергетичної системи (1–5%), пандемії (5–25%) [6, с. 15–16].

Задля ілюстрування підходу, викладеного в Національному реєстрі ризиків, вважаємо за необхідне унаочнити його на прикладах кейсів щодо кіберзагроз (див. табл. 1), які корелюють із тематикою нашого дослідження.

Згадана нами дослідниця М. Вакер рекомендує декілька простих кроків для організації управління ризиками Сірих Носорогів:

1. Напрацювання способів розпізнавання ознак загрози, що насувається.
2. Подання людям сигналу тривоги, який важко ігнорувати.
3. Проактивне навчання людей реагуванню на ризик.
4. Забезпечення захисту людей та надання їм чітких інструкцій у разі розгортання загрози [2, с. 40].

Окрім того, в літературі наводяться обґрунтування щодо підходу, за яким ризики можна розмежовувати за ступенем, зокрема на такі категорії:

- потенційний виклик (дуже малий ризик);
- реальний виклик (малий ризик);
- потенційна загроза (середній ризик);
- реальна загроза (великий ризик);
- реальна небезпека (дуже великий ризик) [4, с. 98–99].

Таблиця 1 – Кейси сценаріїв розвитку подій щодо кіберзагроз

Кібератака на системи телекомунікацій	*Кібератака на транспортний сектор*
спустошлива та складна кібератака на операторів телекомунікаційних сервісів вплине на мільйони клієнтів, у тому числі тих, хто користується іншими мережами, підключеними до тієї, що зазнала атаки; відчутним буде вплив на послуги, що надаються іншими секторами мережі. Вплив на широкосмуговий, стаціонарний і мобільний зв'язок означатиме, що клієнти не зможуть отримати доступ до Інтернету або здійснювати голосові дзвінки. Усі клієнти, які не мають фіксованого та мобільного зв'язку, не можуть отримати доступ до служб екстреної допомоги (999/112) з-поміж інших критично важливих послуг. Залежно від характеру атаки збій може тривати до 72 годин, але може розтягнутися на тижні або місяці	найгірший вірогідний сценарій заснований на кібератаці на критично важливу інформаційну мережу або систему в транспортному секторі. Це призведе до серйозних збоїв у наданні послуг операторами ринку транспортних послуг. Атака може призвести до миттєвого збою в роботі служб і систем, причому цей збій може тривати декілька годин і потребуватиме декілька днів для відновлення роботи цих служб. Збій у роботі критично важливих послуг і систем може призвести до економічних та репутаційних втрат, а також створити підвищену загрозу безпеці пасажирів постраждалих операторів ринку транспортних послуг у Великобританії чи тих, з якими вони співпрацюють
Кібератака на систему охорони здоров'я та соціального забезпечення	
найгірший вірогідний сценарій включатиме значні збої в роботі системи через шкідливе програмне забезпечення, яке швидко поширюється. Системи стануть недоступними, а організації перейдуть на офлайн-сервіси. Втрата даних буде значною, вони також можуть бути скомпрометовані та/або викрадені. Деякі дані неможливо буде відновити з резервних копій. Наслідки будуть відчутні негайно, що, наприклад, матиме вияв у скасованих прийомах, затримках у здійсненні медичних процедур і проведенні тестів, а також у неможливості передавання даних лікарям. Таким чином, збій може мати негайний прямий вплив на пацієнтів, а також завдати суттєвої шкоди системі. Подальші наслідки виявлятимуться з часом, оскільки затримки та скасування означатимуть погіршення умов надання медичних послуг або несвоєчасну діагностику захворювань	

Джерело: побудовано за даними [6, с. 55–60]

З метою здійснення ефективного управління ризиками в умовах надзвичайних ситуацій пропонується розвивати:

– систему моніторингу, аналізу ризику та прогнозування надзвичайних ситуацій як основи діяльності зі зниження ризиків надзвичайних ситуацій;

– систему запобігання надзвичайним ситуаціям та механізми державного регулювання ризиків;

– систему ліквідації надзвичайних ситуацій, враховуючи оперативне реагування на них, технічні засоби та технології проведення аварійно-рятувальних та інших невідкладних робіт;

– систему підготовки керівного складу органів управління, фахівців та населення у сфері зниження ризиків та зменшення масштабів надзвичайних ситуацій;

– систему страхування ризиків [5, с. 463–464].

Звертаючись до стандартизованої методології управління ризиками [7], зазначимо, що процес цей є перманентним та допомагає у визначенні стратегії діяльності, досягненні цілей та ухваленні обґрунтованих управлінських рішень. Процес управління ризиками містить систематичне застосування відповідних політик, процедур та методів до діяльності, пов'язаної з комунікаціями та консультуванням, формуванням контексту та оцінюванням, опрацюванням, моніторингом, аналізом, документуванням та формуванням звітності.

Загальноприйняті принципи, на яких має бути побудована система управління ризиками, є такими:

– інтегрованість. Управління ризиками є невід'ємною частиною всієї діяльності організації;

– структурованість та повнота. Структурований та комплексний підхід до управління ризиками сприяє отриманню узгоджених та порівнюваних результатів;

– налаштованість. Структура системи і процес управління ризиками можуть налаштовуватися та відповідають зовнішньому і внутрішньому контексту організації, пов'язаному з її цілями;

– залучення. Відповідне та своєчасне залучення стейкголдерів дає змогу враховувати їхні знання, погляди та сприйняття. Це призводить до підвищення обізнаності та обґрунтованості управління ризиками;

– динамічність. Ризики можуть виникати, змінюватись або зникати в міру зміни зовнішнього та внутрішнього контексту діяльності організації. Управління ризиками прогнозує, виявляє, розпізнає та реагує на ці зміни й події своєчасно та у відповідний спосіб;

– найкраща доступна інформація. Вихідні дані для управління ризиками ґрунтуються на інформації про минуле та поточну інформацію, а також на майбутніх очікуваннях. Управління ризиками однозначно враховує будь-які обмеження та невизначеності, пов'язані з такою інформацією та очікуваннями. Інформація має бути своєчасною, зрозумілою та доступною для відповідних стейкголдерів;

– людські та культурні аспекти. Поведінка людей і культура істотно впливають на всі аспекти управління ризиками на кожному рівні та етапі;

– постійне покращення. Управління ризиками постійно покращується через навчання та набуття досвіду [7].

Транслюючи окреслену методологію на інформаційну сферу держави задля забезпечення захисту її інформаційного простору, підкреслимо, що нам імпонує підхід, описаний у [8, с. 137–138], відповідно до якого загальна методика проведення оборонної інформаційної операції має такий вигляд:

1. Збір інформації з публікаціями в неафільованих ЗМІ про об'єкт.
2. Побудова графіка – динаміки появи повідомлень про об'єкт у мережевих ЗМІ.
3. Аналіз динаміки у ретроспективі 6–12 місяців за допомогою методів аналізу часових рядів, аналіз контенту публікацій у граничних точках, визначення моментів, тривалості, періодичності впливу, прив'язка моментів впливу до інших подій зі сфери інтересів об'єкта.
4. Визначення джерел, які оприлюднюють найбільшу кількість публікацій з негативною тональністю про об'єкт.
5. Визначення першоджерел публікацій у ЗМІ.
6. Визначення ймовірних «замовників» або осіб, які впливають на редакційну політику окремих ЗМІ.
7. Визначення сфер спільних інтересів об'єкта і потенційних «замовників», їх ранжування за інтересами.

8. Визначення критеріїв інформаційних впливів на основі найбільш рейтингових інтересів.

9. Моделювання інформаційних впливів, виявлення зв'язків «замовників», аналіз динаміки їхнього впливу, формування прогнозу вказаної динаміки, аналіз контенту публікацій, визначення критичних точок впливу.

10. Прогнозування подальших кроків впливу шляхом аналізу аналогічної динаміки публікацій для інших об'єктів у ретроспективі.

11. Оцінювання ймовірних наслідків.

12. Організація інформаційної протидії.

Одним із запропонованих в науковій літературі варіантів побудови системи моніторингу інформаційного простору є підхід, висвітлений у [9, с. 83], за яким така система має бути «…сукупністю державних систем і засобів зв'язку та виявлення, які забезпечують одержання органами управління … і відповідними органами державної влади та іншими користувачами просторово-часової достовірної інформації про реальні та потенційні інформаційні загрози та інформаційні (кібер) впливи». Складові означеної системи наведено на рис. 1.

Рисунок 1 – Система моніторингу інформаційного простору

Джерело: [9]

І хоча автори зосереджують свою увагу на діяльності Центру моніторингу інформаційного простору, однак детально його функції не описують. Водночас відповідним указом Президента України передбачено «розширення та подальший розвиток єдиної мережі ситуаційних центрів, до складу якої мають входити Головний ситуаційний центр України, Урядовий

ситуаційний центр, ситуаційні центри органів сектору безпеки і оборони, ситуаційні центри центральних органів виконавчої влади, Ради міністрів Автономної Республіки Крим, обласних, Київської та Севастопольської міських державних адміністрацій, а також резервні та рухомі ситуаційні центри» [10].

У постанові Кабінету Міністрів України «Питання мережі ситуаційних центрів» наводиться визначення ситуаційного центру як спеціального організаційно-технічного комплексу, призначеного для супроводження організаційного, експертно-аналітичного та інформаційного забезпечення діяльності відповідного органу державної влади, основним завданням якого є експертно-аналітичне та інформаційне супроводження його діяльності у мирний час, особливий період, у тому числі в умовах надзвичайного стану, а також у разі виникнення ризиків та кризових ситуацій, що загрожують національній безпеці [11]. Його функції полягають у:

– визначенні шляхів, механізмів та способів вирішення проблемних питань;

– зборі, узагальненні, проведенні аналізу, систематизації та обробці інформації;

– обміні інформацією та її відтворенні;

– проведенні аналізу та візуалізації даних з різних джерел, побудові, підтримці та актуалізації прогностичних моделей на їх основі.

Задля забезпечення означених вище потреб запропоновано створити трирівневу підсистему моніторингу інформаційних процесів в інформаційному просторі держави, в якій:

– перший рівень – операторний (виявлення, первинна класифікація та індикація деструктивних інформаційних процесів за визначеними джерелами можливого впливу);

– другий рівень – узагальнення даних першого рівня за класифікаційними ознаками, вагова обробка отриманих формалізованих повідомлень;

– третій рівень – виявлення факту негативного інформаційно-психологічного впливу та оцінювання його рівня за формалізованою інформацією другого рівня, що забезпечується головним інформаційним (ситуаційним) центром [12, с. 32].

З огляду на напрацювання попередників ми пропонуємо модель моніторингу інформаційного простору, наведену

на рис. 2, складовими елементами якої мають бути:

– оперативне виявлення інформаційного впливу;
– аналіз та оцінювання рівня впливу;
– формування висновків та рішення щодо необхідності протидії;
– прогнозування розвитку ситуації;
– планування заходів протидії впливу;
– реагування на виявлені інформаційні загрози;
– контроль дієвості реалізованих заходів та їх корегування;
– здійснення превентивних інформаційних заходів.

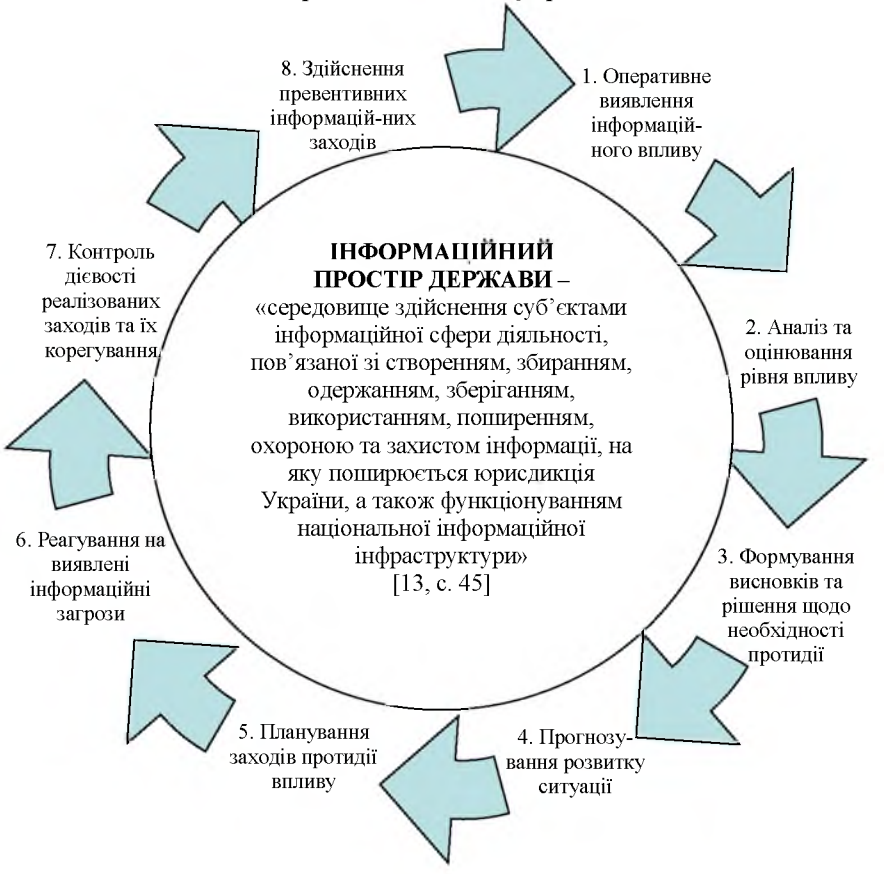

Рисунок 2 – Модель моніторингу інформаційного простору

Джерело: розроблено автором

Висновки та напрями подальших досліджень. Моделювання публічного управління захистом інформаційного простору стає критично важливою проблемою з огляду на перманентний і невпинний розвиток технологій, геополітичну нестабільність та різноманітність загроз. Практичний підхід, підкріплений досвідом, дає змогу аналізувати загрози та їхні наслідки, а також розробляти ефективні стратегії реагування на сучасні виклики задля забезпечення національної безпеки. У дослідженні наголошено на важливості урахування непередбачуваних ризиків, оскільки їх ігнорування може мати серйозні наслідки для системи національної безпеки.

У сучасних умовах зростаючі загрози дестабілізації національного інформаційного простору впливають на підвищення пріоритетності гарантування інформаційної безпеки держави. Важливо враховувати ключові напрями потенційної дестабілізації суспільно-політичної ситуації, щоб розробляти ефективні стратегії реагування та захисту.

Модель моніторингу інформаційного простору, що базується на послідовних та взаємозалежних елементах, може стати основою для забезпечення ефективного захисту інтересів держави в нинішніх турбулентних обставинах. Рекомендується розвивати ризик-орієнтований підхід до організації системи управління захистом інформаційного простору для мінімізації можливих наслідків загроз у цій сфері.

Перспективною, на наше переконання, є апробація запропонованої моделі на практиці задля підтвердження авторської гіпотези та верифікації одержаних теоретичних напрацювань.

Список використаних джерел

1. Талеб Н. Н. Чорний лебідь. Про (не)ймовірне у реальному житті / пер. з англ. М. Климчук. Київ : Наш формат, 2017. 392 с.
2. Wucker M. The Gray Rhino. How to Recognize and Act on the Obvious Dangers We Ignore. New York : St. Martin's Press, 2016. 304 p.
3. Belton C. Kremlin runs disinformation campaign to undermine Zelensky, documents show. *The Washington Post*. 2024. Feb. 16th. URL : https://www.washingtonpost.com/world/2024/02/16/russian-disinformation-zelensky-zaluzhny/ (last accessed : 24.02.2024).
4. Теоретико-методологічні засади паспортів загроз національній безпеці України : монографія / Г. П. Ситник, В. І. Абрамов, В. А. Мандрагеля [та ін.]; під заг. ред. Г. П. Ситника, Л. М. Шипілової. Київ : НАДУ, 2012. 163 с.
5. Шляхи удосконалення системи державного управління забезпеченням національної безпеки

України : монографія / Г. П. Ситник, В. І. Абрамов, О. Г. Бортнікова та ін. / за ред. Г. П. Ситника, В. І. Абрамова. Київ : НАДУ, 2012. 590 с.
6. National Risk Register. 2023 edition. *GOV.UK* : websit. URL : https://www.gov.uk/government/publications/national-risk-register-2023 (last accessed : 24.02.2024).
7. Менеджмент ризиків. Принципи та настанови=Risk management – Guidelines. ДСТУ ISO 31000:2018 (ISO 31000:2018, IDT). [Чинний від 2019.01.01]. Вид. офіц. Київ, 2018. 16 с.
8. Горбулін В. П., Додонов О. Г., Ланде Д. В. Інформаційні операції та безпека суспільства : загрози, протидія, моделювання : монографія. Київ : Інтертехнологія, 2009. 164 с.
9. Сніцаренко П. М., Кацалап В. О. Методичний підхід щодо синтезу систем моніторингу інформаційного простору за критерієм оптимальності в інтересах Сил оборони України. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2022. № 2(44). С. 82–88.
10. Про рішення Ради національної безпеки і оборони України від 4 червня 2021 року «Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони» : Указ Президента України від 18.06.2021 р. № 260/2021. *Офіційний вісник України.* 2021. № 50. С. 20.
11. Питання мережі ситуаційних центрів : постанова Кабінету Міністрів України від 11.07.2023 р. № 705. *Офіційний вісник України*. 2023. № 68. С. 58.
12. Сніцаренко П. М., Саричев Ю. О., Ткаченко В. А., Мотузяник О. А. Підсистема моніторингу інформаційного простору як необхідна складова системи протидії негативному інформаційно-психологічному впливу на особовий склад Збройних Сил України. *Наука і оборона*. 2018. № 1. С. 29–33.
13. Солодка О. М. Інформаційний простір держави як сфера реалізації інформаційного суверенітету. *Інформація і право.* 2020. № 4 (35). С. 39–46.

References

1. Taleb, N. N. (2017). Chornyi lebid. Pro (ne)imovirne u realnomu zhytti [The Black Swan. The Impact of the Highly Improbable]. Kyiv: Nash format [in Ukrainian].
2. Wucker, M. (2016). The Gray Rhino. How to Recognize and Act on the Obvious Dangers We Ignore. New York: St. Martin's Press [in English].
3. Belton, C. (2024). Kremlin runs disinformation campaign to undermine Zelensky, documents show. *The Washington Post*. Feb. 16th. Retrieved from https://www.washingtonpost.com/world/2024/02/16/russian-disinformation-zelensky-zaluzhny/ [in English].
4. Sytnyk, H. P., Abramov, V. I., Mandrahelia, V. A. et al. (2012). Teoretyko-metodolohichni zasady pasportiv zahroz natsionalnii bezpetsi Ukrainy [Theoretical and methodological principles of threats passports to the national security of Ukraine]. Sytnyk H. P., Shypilova L. M. (Ed.). Kyiv: NADU [in Ukrainian].
5. Sytnyk, H. P., Abramov, V. I., Bortnikova, O. H. et al. (2012). Shliakhy udoskonalennia systemy derzhavnoho upravlinnia zabezpechenniam natsionalnoi bezpeky Ukrainy [Improving ways of public administration system for ensuring national security of Ukraine]. Sytnyk, H. P., Abramov, V. I. (Ed.). Kyiv: NADU [in Ukrainian].
6. National Risk Register. 2023 edition. *GOV.UK* : websit. URL : https://www.gov.uk/government/publications/national-risk-register-2023 [in English].
7. Menedzhment ryzykiv. Pryntsypy ta nastanovy=Riskmanagement – Guidelines [Risk management. Principles and guidelines=Risk management – Guidelines] (2018). DSTU ISO 31000:2018 (ISO 31000:2018, IDT) from 1st January 2019. Kyiv [in Ukrainian].
8. Horbulin, V. P., Dodonov, O. H., Lande, D. V. (2009). Informatsiini operatsii ta bezpeka suspilstva: zahrozy, protydiia, modeliuvannia [Information operations and security of society: threats, countermeasures, modeling]. Kyiv: Intertekhnolohiia [in Ukrainian].
9. Snitsarenko, P. M., Katsalap, V. O. (2022). Metodychnyi pidkhid shchodo syntezu system monitorynhu informatsiinoho prostoru za kryteriiem optymalnosti v interesakh Syl oborony Ukrainy [Method approach to the synthesis of information space monitoring systems according to the criteria of optimality in the interests of the Defense Forces of Ukraine]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*, 2 (44), 82–88. [in Ukrainian].
10. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 4 chervnia 2021 roku «Shchodo udoskonalennia merezhi sytuatsiinykh tsentriv ta tsyfrovoi transformatsii sfery natsionalnoi

bezpeky i oborony» [On the decision of the National Security and Defence Council of Ukraine from June 4th, 2021 «On the improvement of the network of situation centers and the digital transformation of the sphere of national security and defense»]: Ukaz Prezydenta Ukrainy vid 18.06.2021 r. № 260/2021. *Ofitsiinyi visnyk Ukrainy*, 50, 20. [in Ukrainian].
11. Pytannia merezhi sytuatsiinykh tsentriv [On the issue of situation centers' network]: postanova Kabinetu Ministriv Ukrainy vid 11.07.2023 r. № 705. *Ofitsiinyi visnyk Ukrainy*, 68, 58. [in Ukrainian].
12. Snitsarenko, P. M., Sarychev, Yu. O., Tkachenko, V. A., Motuzianyk, O. A. (2018). Pidsystema monitorynhu informatsiinoho prostoru yak neobkhidna skladova systemy protydii nehatyvnomu informatsiino-psykholohichnomu vplyvu na osobovyi sklad Zbroinykh Syl Ukrainy [Information space monitoring subsystem as a necessary component of the system of counteracting negative information and psychological influence on the personnel of the Armed Forces of Ukraine]. *Nauka i oborona*, 1, 29–33 [in Ukrainian].
13. Solodka, O. M. (2020). Informatsiinyi prostir derzhavy yak sfera realizatsii informatsiinoho suverenitetu [Information space of the state as a sphere of information sovereignty's implementation]. *Informatsiia i pravo*, 4 (35), 39–46. [in Ukrainian].

PUBLIC ADMINISTRATION OF INFORMATION SPACE PROTECTION MODELING IN THE CONTEXT OF THE RISK-BASED APPROACH APPLICATION

Hlobenko Serhii

Abstract. Public administration of information space protection modeling in the modern world is one of the key issues due to the constant development and improvement of technologies, geopolitical instability, and the increasing as well as diversification of threats. A practice-oriented approach, grounded on accumulated experience, allows to analyze threat scenarios, to predict their consequences, and to search for effective methods and means of responding to contemporary challenges facing the state in the context of ensuring its national security as well as to safeguard national interests properly. The presented study, based on the theories of the Black Swan and the Gray Rhino, underscores the necessity of considering unforeseen risks and threats that the public administration system may encounter or potentially face, as underestimating or neglecting them could lead to serious consequences for national security system. In today's conditions, ensuring information security of the state becomes a priority due to the risks of destabilizing the national information space. Specifically, in the context of Ukraine, it is crucial to consider at least four key destabilization directions of the socio-political situation in order to develop effective response, counteraction, and protection strategies. The presented model of information space monitoring, consisting of a series of sequential and interdependent elements, can serve as a basis for ensuring effective protection of state interests in current turbulent circumstances. Building on previous research, it is recommended to develop a risk-oriented approach to organizing the information space protection management system to minimize and neutralize potential consequences of threats in the defined sphere.

Key words: information space of the state, information security, protection of information space, state policy in the information sphere, mechanisms of public administration, risk management, risk-oriented approach, modeling.