Функціонування і розвиток механізмів державного управління

УДК 338.2:351.863

Хряпинський Антон Петрович
кандидат юридичних наук, директор
ТОВ «ХРЯПИНСЬКИЙ І КО»
Khriapynskyi Anton
Candidate of Law Sciences, Director
LTD «Khriapynskyi and partners»
ORCID: 0000-0002-2492-051X

ПОПЕРЕДЖЕННЯ ТА ПРЕВЕНЦІЯ ПРОТИДІЇ ГІБРИДНИХ ЗАГРОЗ: ЗАГАЛЬНОТЕОРЕТИЧНИЙ ПІДХІД ТА СИНТЕЗ
WARNING AND PREVENTION OF COUNTERING HYBRID THREATS: GENERAL THEORETICAL APPROACH AND SYNTHESIS

Анотація. *Вступ. У сучасному середовищі, де відбувається поглиблення процесів глобалізації економіки, особливого значення набуває економічна безпека держави як на національному рівні, так і на міжнародно-геополітичному, яка виступає основою суверенітету, конкурентоспроможності, а також засобом пришвидшення процесу входження країни в систему світової економіки. В той же час, задля прискорення економічного зростання та дотримання безпеки, особливого значення набувають гібридні загрози, які вимагають комплексного підходу та опрацювання.*

Мета. Метою даної роботи є поглиблення дослідження сутності та характеристики системи попередження та протидії внутрішнім загрозам через загальнотеоретичний аналіз та синтез.

Матеріали і методи. В процесі здійснення дослідження було використано наступні наукові методи: емпіричний (для збору та

систематизації даних), спостереження (для узагальнення інформації), аналізу та синтезу (для оцінки ситуацій та прикладів до них, а також вжиття необхідних заходів).

Результати. Досліджено теоретичні питання попередження та превенції гібридних загроз крізь призму загальнотеоретичного аналізу та синтезу. Акцентовано увагу на тому, що система попередження є важливою складовою протидії гібридним загрозам. Інформування осіб, які приймають рішення постраждалих від гібридних впливів країн, а також населення в цілому дає їм змогу вжити відповідних заходів. Зосереджено увагу на тому, що окрім визначення показників, які базуються на встановлених знаннях, важливо застосовувати індуктивні методи, які починаються зі спостережень і рухаються назад до узагальнень. У світлі стрімкого зростання обсягів великих даних і прогресу в машинному навчанні організації, що займаються попередженням, мають у своєму розпорядженні все більше моделей, які дозволяють прогнозувати загрози. Зроблено висновок про те, що хоча гібридні загрози є комплексними проблемами, побудова відповідної система попередження не здається неможливою. Аналіз численних робіт за даною проблематикою дозволив визначити чотири фази процесу попередження: визначення напрямку попередження; збір інформації; аналіз загроз; комунікація та розповсюдження.

Перспективи. В подальших наукових дослідженнях пропонується зосередити увагу на виробленні конкретних методик та показників для протидії внутрішнім загрозам та критеріїв побудови системи їх попередження.

Ключові слова: *управління, гібридні загрози, протидія та превенція, інноваційний розвиток, протидія загрозам, превенція загрозам, гібридні загрози в управлінні.*

Summary. *Introduction. In the modern environment, the processes of globalization of the economy are deepening, the economic security of the state is gaining special importance both at the national level and at the international-geopolitical level, which acts as the basis of sovereignty, competitiveness, as well as the arrival of the process of the country's entry into the world economy. At the same time, to accelerate economic growth and maintain security, hybrid threats, which require a comprehensive approach and processing, are of particular importance.*

Purpose. The purpose of this work is to deepen the study of the essence and characteristics of the system of prevention and countermeasures against internal threats through a general theoretical analysis and synthesis.

Materials and methods. The following scientific methods were used during the research: empirical (to collect and systematize data), observation (to generalize information), analysis and synthesis (to evaluate situations and examples of them, as well as take necessary measures).

Results. The theoretical issues of warning and prevention of hybrid threats are studied through the prism of general theoretical analysis and synthesis. Attention is focused on the fact that the warning system is an important component of countering hybrid threats. Informing decision-makers in countries affected by hybrid impacts, as well as the general population, enables them to take appropriate measures. Emphasis is placed on the fact that, in addition to defining indicators based on established knowledge, it is important to use inductive methods that begin with observations and move back to generalizations. Considering the rapid growth of big data and advances in machine learning, warning organizations have more and more models at their disposal to predict threats. It was concluded that although hybrid threats are complex problems, building an appropriate warning system does not seem impossible. The analysis of numerous works on this issue made it possible to determine four phases of the warning process: determining the direction of the warning; collection of

information; threat analysis; communication and dissemination.

Discussion. In further scientific research, it is proposed to focus attention on the development of specific methods and indicators for countering internal threats and criteria for building a system for their prevention.

Key words: *management, hybrid threats, counteraction and prevention, innovative development, countermeasures against threats, prevention of threats, hybrid threats in management.*

Постановка проблеми. У сучасному середовищі, де відбувається поглиблення процесів глобалізації економіки, особливого значення набуває економічна безпека держави як на національному рівні, так і на міжнародно-геополітичному, яка виступає основою суверенітету, конкурентоспроможності, а також засобом пришвидшення процесу входження країни в систему світової економіки. В той же час, задля прискорення економічного зростання та дотримання безпеки, особливого значення набувають гібридні загрози, які вимагають комплексного підходу та опрацювання.

Аналіз останніх досліджень і публікацій. Проблематика аналізу та розгляду гібридних загроз завжди привертала увагу вітчизняних та закордонних науковців, що знайшло своє відображення у працях таких вчених як Л. Акімова – щодо протидії загрозам у економічній сфері та державно-управлінських засадах в цілому [1], Е. Бухвальд – щодо окремих питань макропоказників впливу загроз у державно-управлінських засадах [2], З. Гбур – щодо концептуальних аспектів протидії загрозам [3], В. Ліпкан – щодо сутнісних особливостей гібридної війни на прикладі вітчизняного досвіду [4], Є. Магда – щодо загальних характеристик сутності гібридної війни як сутнісного явища [5], В. Мартинюк – щодо загальних характеристик сутності гібридної війни крізь суспільно-економічні показники [6], В. Горбулін – щодо інформаційних характеристик безпеки

суспільства як об'єкт впливу гібридних загроз [7], О. Курбан – щодо концепції сучасної системи забезпечення безпеки країни[8], але чимало досліджень все ще перебувають на етапі становлення та осмислення, що свідчить про незавершеність формування наукової думки та усталених постулатів, а відтак, набуває особливої актуальності.

Виділення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття. Невпинний розвиток науково-технічного прогресу та потенціалу, а також глибинні процеси інноваційно-просторового розвитку постійно змінюють усталені погляди та концепції на явища та процеси, наповнюють їх новим змістом та осмисленням. За даних умов випливає, що поглиблення досліджень у сфері науково-теоретичного та практичного розуміння гібридних загроз та виокремлення системи їх попередження та протидії має надзвичайно актуальне значення та передбачає ряд систем стримувань та противаг.

Формулювання цілей статті (постановка завдання). Метою даної роботи є поглиблення дослідження сутності та характеристики системи попередження та протидії внутрішнім загрозам через загальнотеоретичний аналіз та синтез.

Матеріали і методи. В процесі здійснення дослідження було використано наступні наукові методи: емпіричний (для збору та систематизації даних), спостереження (для узагальнення інформації), аналізу та синтезу (для оцінки ситуацій та прикладів до них, а також вжиття необхідних заходів).

Виклад основного матеріалу дослідження. Система попередження є важливою складовою протидії гібридним загрозам. Інформування осіб, які приймають рішення постраждалих від гібридних впливів країн, а також населення в цілому дає їм змогу вжити відповідних заходів. Проте, як П. Каллен переконливо стверджував у своєму Стратегічному аналізі, гібридні загрози є комплексними проблемами. Вони є неоднозначними та нечіткими,

бракує підтверджених знань і фіксованих стандартів для їх адекватного вирішення. Це робить розробку системи попередження про такі загрози надзвичайно важкою та складною [9, с. 44].

До того, як гібридні загрози матеріалізуються, вони часто надсилають лише слабкі сигнали, які важко виявити, і їх неможливо легко пов'язати з будь-якою відомою тенденцією чи явищем [10, с. 102]. Також ці слабкі сигнали містяться у величезній кількості нерелевантної або оманливої інформації, яку часто називають шумом. Крім того, як стверджує Каллен, гібридні загрози створені для того, щоб стерти різницю між миром і війною, а також ускладнити та знизити порогові значення виявлення цілі та відповіді. Тому він робить висновок, що гібридні загрози вимагають нових рішень для попередження. Тревертон та ін. [11, с. 70] дійшли подібного висновку, коли стверджували, що попередження про гібридні загрози є «складним, але не неможливим», а Найхейм також наголошує на необхідності адаптувати методи попередження до виниклої реальності гібридних конфліктів і війн [12, с. 8].

Аналіз цих та інших робіт за даною проблематикою дозволив визначити чотири фази процесу попередження: 1) визначення напрямку попередження; 2) збір інформації; 3) аналіз загроз; 4) комунікація та розповсюдження. Розглянемо їх.

1. Визначення напрямку попередження. Відповідно до традиційного погляду на попередження, політики або військові командири визначають напрямок процесу попередження, заявляючи про свої потреби. Вони часто називають це вимогами до інформації. За словами колишнього міністра оборони США Дональда Рамсфельда, це передбачає пошук «відомих невідомих» – речей, про які ми знаємо, що ми їх не знаємо. Однак у випадку гібридних загроз такі початкові вимоги є дискусійними, і їх часто неможливо визначити. У такому разі і ті, хто попереджає, і ті, хто приймає рішення, опиняються в положенні не знати того, чого вони не знають, тобто

«невідомих невідомих» Рамсфельда. Ця проблема ускладнюється великою кількістю акторів, які беруть участь у процесі попередження, і водночас часто відсутністю чітко визначеної відповідальності за цей процес.

У той час як традиційні загрози відстежуються однією або декількома спеціальними (розвідувальними) організаціями, яка надають вказівки для керування процесом попередження, для ГЗГВ це не так. Тут постійно змінюються актори (мережі акторів), які залучають до цієї діяльності відповідні ресурси. Це викликає питання щодо фінансування, координації та забезпечення людськими ресурсами і вимагає альтернативного способу здійснення процесу попередження.

Спираючись на літературу про складність, ми знаємо, що питання самоорганізації є особливо актуальним для організацій, які стикаються з комплексними проблемами [13, с. 84]. Це пояснюється тим, що накопичення частих, локально ініційованих і невеликих імпровізаційних втручань окремих акторів, невід'ємних від самоорганізації, може значно підвищити адаптивну здатність складних систем. Актори досліджують ці нові шляхи та процеси у взаємодії один з одним, з мінімальними зовнішніми механізмами контролю або зовсім без них.

Морган представив кілька принципів дизайну, які допомагають у розвитку самоорганізації. Те, як ці принципи застосовуються, залежить від конкретної організації чи мережі [14, с. 22]. Першим принципом самоорганізації, згідно з Морганом, є «важливість надмірності». Організаціям необхідно інвестувати в слабкі можливості обробки інформації та набори навичок, щоб зменшити залежність оперативного реагування від дій одного актора. Зараз, наприклад, розвідувальні організації публічно заявляють, що стратегічне попередження є надзвичайно важливим. Однак на практиці багато хто сприймає це лише як «галочку» та дозволяє передавати більшість ресурсів іншим структурам, які «стежать за «гарячими» темами дня» [15, с. 204].

Другий принцип полягає в дотриманні закону Ешбі про «необхідну різноманітність», що означає, що внутрішня різноманітність повинна відповідати різноманітності та складності середовища. У випадку гібридних загроз це означає, що організації, які займаються їхнім попередженням, повинні демонструвати рівень різноманітності, який відповідає рівню їхніх противників. Велика кількість різноманітних несправностей у мережі попереджень, а також відсутність необхідних знань і розуміння перешкоджають ефективному впровадженню цього принципу.

Третій принцип має назву «мінімальні характеристики», що означає, що керівництво має визначати лише найнеобхідніше та пропонувати достатньо свободи для розподілених дій. Зокрема, комітети з нагляду та етики в багатьох країнах обмежують розвідувальні служби в їхніх методах роботи, наприклад у зборі та обміні інформацією. Тим часом приватні організації, такі як Bellingcat, менш зв'язані правилами, а їхня мережа волонтерів робить їх досить гнучкими у вирішенні майбутніх криз. Розслідування збиття рейсу MH17 добре це проілюструвало. Застосовуючи нетрадиційні методи, такі як проникнення в російські соціальні мережі, Bellingcat змогла розкрити численні факти та ідентифікувати людей, причетних до збиття.

Четвертий і останній принцип – «навчатися вчитися». Цей принцип підкреслює, що для того, щоб самоорганізуватися, члени організації повинні володіти мисленням подвійного циклу навчання, але їм також повинна бути надана свобода кидати виклик існуючим нормам, правилам і процедурам. Закрита та таємна культура, а також бюрократична організація багатьох розвідувальних і військових спільнот чітко забороняють таке навчання та віддаляють їх від реалізації даного принципу.

2. Збір інформації. Індикатори є основою процесу збору даних попередження, забезпечуючи систематичну основу для моніторингу ситуації та створення попереджень. Вони важливі для того, щоб звести

«складну ситуацію до конкретних особливостей, якими можна керувати, і визначити корисні проблеми, на тлі яких можна спостерігати будь-які трансформації» [16, с. 83]. Науковці, що досліджують дане питання, визначають кілька вимог до індикаторів, основними з яких є прогностичність, діагностичність, однозначність та збірність. Хоча індикатори, які використовувалися під час холодної війни, в основному відповідали цим вимогам, але це часто не стосується індикаторів, які сигналізують про гібридні загрози. Тут необхідно розуміти та контролювати велике розмаїття інструментів, як військових, так і невійськових, а також суб'єктів загроз, щоб забезпечити належне попередження.

Цей виклик є величезним і вимагає подолання розриву між дедуктивними та індуктивними методами, які використовують як якісні, так і кількісні дані. При застосуванні дедуктивних методів показники формулюються заздалегідь і ґрунтуються на загальних ідеях або розумінях. Для цього потрібні глибокі та усталені знання теми. Гарним прикладом є системи виявлення вторгнень, оскільки їхня конструкція ґрунтується на загальних знаннях про захист комп'ютерних мереж.

Окрім визначення показників, які базуються на встановлених знаннях, важливо застосовувати індуктивні методи, які починаються зі спостережень і рухаються назад до узагальнень. У світлі стрімкого зростання обсягів великих даних і прогресу в машинному навчанні організації, що займаються попередженням, мають у своєму розпорядженні все більше моделей, які дозволяють прогнозувати загрози [17, с. 15].

Однак, оскільки багато з цих моделей є здебільшого «чорною скринькою» та забезпечують кореляції, а не пояснення, вони забезпечують зусилля щодо усунення загроз лише в обмеженій мірі. Отже, виникає потреба застосовувати дедуктивний та індуктивний методи паралельно.

Крім того, зростає консенсус щодо того, що методи попередження повинні об'єднувати як кількісні, так і якісні дані. Більшість методів

попередження надають перевагу кількісним даним. За умови, що ці дані надійні, дійсні, своєчасні та адекватно проаналізовані, ці методи є незамінними. Прості показники можуть зробити зайвими довгі обговорення. Водночас багато викликів попередження вимагають інтерпретації, осмислення та якісної інтерпретації, щоб забезпечити глибину, а також чутливість до даного контексту та даного актора. Події з найбільшим впливом зазвичай відбуваються несподівано, і їх рідко можна вивести заздалегідь з числових рядів.

Виходячи з цього найбільш доцільним є застосування підходу використання змішаних методів, які ефективно поєднують кількісні дані та складні моделі з надійною якісною інтерпретацією.

3. Аналіз загроз. Хоча багато політиків люблять посилатися на «з'єднання точок», щоб отримати точні картини майбутніх подій, ця картина є дуже неточною та марною [18, с. 40]. У випадку гібридних загроз точки відсутні, тому що вони нижчі за порогове значення, вони виглядають інакше через обман чи дезінформацію або їх неможливо зрозуміти через певне шифрування. Щоб подолати ці виклики, аналітики застосовують різноманітні методи. Добре відомі приклади включають метод Delphi, сканування горизонту або аналіз тенденцій. На додаток до цих методів попередження, аналітики почали запозичувати складні методи з інших таких широких і різноманітних областей, як прогноз погоди, екологія, управління бізнесом і прогнозування поведінки споживачів.

Крім того, фахівці, що займаються попередженнями, можуть скористатися більш точно адаптованими та цілеспрямованими підходами, які дозволяють краще розуміти гібридні загрози. Частиною такого аналізу є здатність враховувати місцеві знання або погляди людей на місцях, щоб можна було подолати прірву між тим, що аналітики за допомогою своїх комп'ютерних моделей і пошуків в Інтернеті вигадують у центрі, і тим, що відбувається на місцях.

Це вимагає, перш за все, побудови кращих комунікацій з місцевими громадами та людьми на місцях через НУО, місцеві представництва чи інші структури. Можливо, необхідно буде перемістити акцент із пошуку лише формальних знань серед професіоналів та експертів на готовність до «депрофесіоналізації» інформації та бути відкритими до «повсякденних знань».

Особливе значення для гібридних загроз має неправильна та оманлива інформація, надана навмисно (дезінформація) або ненавмисно. Існує багато випадків, які демонструють таку динаміку, включаючи, наприклад, спробу вбивства Сергія та Юлії Скрипаль у Солсбері в березні 2018 року, вибори в США 2016 року, використання хімічної зброї в Сирії режимом Асада або наслідки збиття рейсу MH17 Malaysia Airlines. Розпізнавання такого типу інформації є вкрай важливим для аналітиків, але також надзвичайно складним.

Зокрема, Тревертон зазначає з цього приводу, що під час процесу аналізу головним завданням є впоратися з усією інформацією та дезінформацією, яка існує. Аналітики розкидані по різних організаціях і часто мають у своєму розпорядженні значний і різноманітний обсяг інформації, який у них не збігається. У цьому аспекті концепція інформаційного перевантаження є добре відомим явищем і не є унікальним для процесу попередження про гібридні загрози.

4. Комунікація та розповсюдження. Ідея попередження полягає в тому, що воно дозволяє своєчасно реагувати, щоб запобігти шкоді або принаймні зменшити можливу шкоду. Тому ефективне донесення попередження до осіб, які приймають рішення, або населення загалом має велике значення. З точки зору попереджувача, ключові вимоги до комунікації включають достовірність джерела, зміст повідомлення та спосіб комунікації [19, с. 198].

Ступінь, до якого попереджувальне повідомлення врешті-решт впливає на прийняття фактичного рішення та викликає відповідь, залежить від

багатьох інших факторів. Хоча ці фактори були визначені в контексті насильницького конфлікту, кожен із них також цілком застосовний до контексту гібридних загроз.

Висновки з цього дослідження і перспективи подальших розвідок у даному напрямку, таким чином, хоча гібридні загрози є комплексними проблемами, побудова відповідної системи попередження не здається неможливою. Вона просто не функціонує в традиційному розумінні. Щоб краще відповідати дійсності, необхідно переробити процес попередження, а фахівці з попередження і особи, що приймають рішення, повинні знати про підводні камені та труднощі, властиві даному процесу.

Література

1. Акімова Л. М. Сутнісна характеристика основних загроз в економічній безпеці держави. *Державне управління: удосконалення та розвиток*. 2016. № 10. С. 16-28.
2. Бухвальд Є. Макроаспекти економічної безпеки: фактори, критерії та показники. *Питання економіки*. 1994. №12. С. 25-44.
3. Гбур З. В. Актуальні гібридні загрози економічній безпеці України. *Інвестиції: практика та досвід*. 2018. № 7. С. 97-99.
4. Ліпкан В. А. Сутність гібридної війни проти України. *GOAL*. 2015. URL: https://goal-int.org/sutnist-gibridnoi-vijni-proti-ukraini/ (дата звернення 05.08.2023).
5. Магда Є. Гібридна війна: питання і відповіді. *Інтернет-видання «MEDIASAPIENS»*. 2015. URL: http://ms.detector.media/trends/1411978127/gibridna_viyna_pitannya_i_vidpovidi/ (дата звернення 05.08.2023).
6. Мартинюк В. Гібридні загрози Україні і суспільна безпека. досвід ЄС і східного партнерства. *Центр глобалістики «Стратегія XXI»*. 2018. С. 106-112.

7. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. Київ : Інтертехнологія, 2012. 360 с.
8. Курбан О. В. Основи сучасної національної інформаційної безпеки країни. *Вісн. ХДАК*. 2017. Вип. 50. С. 55-62.
9. Alley R., Emanuel K. Zhang, F. Advances in Weather Prediction. *Science*. 2019. № 363. P. 342–344.
10. Brown S. L., Eisenhardt K. M. The Art of Continuous Change: Linking Complexity Theory and Time-Paced Evolution in Relentlessly Shifting Organizations. *Administrative Science Quarterly*. 1997. № 1. P. 1–3.
11. Bryman A. Social Research Methods. Oxford : Oxford University Press, 2012.
12. Cullen P. Hybrid threats as a new 'wicked problem' for early warning. Helsinki : The European Centre of Excellence for Countering Hybrid Threats, 2018.
13. Gentry J. A., Gordon, J. S. Strategic Warning Intelligence: History, Challenges, and Prospects. Washington : Georgetown University Press, 2019.
14. Kuosa T. Towards Strategic Intelligence – Foresight, Intelligence, and Policy-Making. Helsinki : Dynamic Futures, 2014.
15. Marr B. Big Data in Practice. Hoboken : John Wiley and Sons Ltd, 2016.
16. Meyer C. O., Otto F. How to warn: 'Outside-in warnings' of Western governments about violent conflict and mass atrocities. *Media, War & Conflict*. 2016. № 2. P. 198–216.
17. Morgan G. Images of Organization. Thousand Oaks : Sage Publications, 2006.
18. Nyheim D. Early warning and response to violent conflict. Time for a rethink? London : Saferworld, 2015.
19. Odote P. O. Role of early warning systems in conflict prevention in Africa:

Case study of the Ilemi Triangle. PhD Thesis. Nairobi : University of Nairobi, 2016.

References

1. Akimova, L. M. (2016). Sutnisna kharakterystyka osnovnykh zaghroz v ekonomichnij bezpeci derzhavy [Essential characteristics of the main threats to the economic security of the state] // *Public administration: improvement and development*, № 10, pp. 342-344 [in Ukrainian].
2. Buchvald, E. (1994). Makroaspekty ekonomichnoji bezpeky: faktory, kryteriji ta pokaznyky [Macroeconomic aspects of economic security: factors, criteria, and indicators] // *Putanya ekonomyky*, № 12, pp. 25-44 [in Ukrainian].
3. Hbur, Z. (2018). Aktualjni ghibrydni zaghrozy ekonomichnij bezpeci Ukrajiny [Actual hybrid threats to Ukraine's economic security] // *Investytsii: praktyka ta dosvid*, № 7, pp. 97-99 [in Ukrainian].
4. Lipkan, V. A. (2015). Sutnistj ghibrydnoji vijny proty Ukrajiny [The essence of the hybrid war against Ukraine]. URL: http://goal-int.org/ sutnist-gibridnoi-vijni-proti-ukraini/ [in Ukrainian].
5. Magda E. (2015). Ghibrydna vijna: pytannja i vidpovidi [Hybrid war: questions and answers]. URL: http://ms.detector. media/trends/1411978127/gibridna_viyna _pitannya_i_vidpovidi/ [in Ukrainian].
6. Martyniuk,V. (2018). Ghibrydni zaghrozy Ukrajini i suspiljna bezpeka. dosvid ES i skhidnogho partnerstva [Hybrid threats to Ukraine and public safety. Experience of the EU and the Eastern Partnership] // *Tsentr hlobalistyky "Stratehiia KhKhI",* pp.106 [in Ukrainian].
7. Gorbulin V. P. (2012). Informacijni operaciji ta bezpeka suspiljstva: zaghrozy, protydija, modeljuvannja [Information operations and social security: threats, countermeasures, modeling]. Kyiv, 360 p. [in Ukrainian].

8. Kurban O. V. (2017). Osnovy suchasnoji nacionaljnoji informacijnoji bezpeky krajiny [Fundamentals of modern national information security of the country] //*Visn. KhDAK* 2017. № 50. pp. 55-62 [in Ukrainian].
9. Alley, R., Emanuel, K. & Zhang, F. (2019). Advances in Weather Prediction. *Science*, № 363, pp. 342–344 [in English].
10. Brown, S. L., & Eisenhardt, K. M. (1997). The Art of Continuous Change: Linking Complexity Theory and Time-Paced Evolution in Relentlessly Shifting Organizations. *Administrative Science Quarterly*, № 1, pp. 1–34 [in English].
11. Bryman, A. (2012). Social Research Methods. Oxford: Oxford University Press [in English].
12. Cullen, P. (2018). Hybrid threats as a new 'wicked problem' for early warning. Helsinki: The European Centre of Excellence for Countering Hybrid Threats [in English].
13. Gentry, J. A. & Gordon, J. S. (2019). Strategic Warning Intelligence: History, Challenges, and Prospects. Washington: Georgetown University Press [in English].
14. Kuosa, T. (2014). Towards Strategic Intelligence – Foresight, Intelligence, and Policy-Making. Helsinki: Dynamic Futures [in English].
15. Marr, B. (2016). Big Data in Practice. Hoboken: John Wiley and Sons Ltd [in English].
16. Meyer, C. O. & Otto, F. (2016). How to warn: 'Outside-in warnings' of Western governments about violent conflict and mass atrocities. *Media, War & Conflict*, № 2, pp. 198–216 [in English].
17. Morgan, G. (2006). Images of Organization. Thousand Oaks: Sage Publications [in English].
18. Nyheim, D. (2015). Early warning and response to violent conflict. Time for a rethink? London: Saferworld [in English].
19. Odote, P. O. (2016). Role of early warning systems in conflict prevention in

Africa: Case study of the Ilemi Triangle. PhD Thesis. Nairobi: University of Nairobi [in English].