ФІЛОСОФІЯ ТА ПОЛІТОЛОГІЯ В КОНТЕКСТІ СУЧАСНОЇ КУЛЬТУРИ
ISSN 2663-0265 (print) ISSN 2663-0273 (online)
Journal home page: https://fip.dp.ua/index.php/FIP

ПОЛІТИЧНІ НАУКИ

Олексій Анатолійович ТРЕТЯК
Доктор політичних наук, професор,
в.о. завідувача кафедри політології, соціології та публічного управління,
Дніпровський національний університет імені Олеся Гончара,
пр. Науки, 72, Дніпро, 49000, Україна

Oleksii TRETIAK
Doctor of political sciences, professor,
Acting Head of the Department of Political Science, Sociology and Public Administration,
Oles Honchar Dnipro National University
Nauka Ave., 72, Dnipro,
49000, Ukraine

E-mail: alexsir25@ukr.net, ORCID: https://orcid.org/0000-0003-2536-0611

УДК 323

АНАЛІТИКА СУЧАСНОЇ ПОЛІТИЧНОЇ БЕЗПЕКИ: «ОРДИНАРНІ» ПІДХОДИ ДО ФОРМУВАННЯ ПУБЛІЧНОГО ЕКСПЕРТНОГО КОНТЕНТУ

Received 03 June 2024; revised 21 June 2024; accepted 29 June 2024
DOI: 10.15421/352426

Анотація

Стаття присвячена основам реалізації публічного сприйняття політичної безпеки держави в умовах повномасштабного вторгнення сучасної росії до України. Метою дослідження є встановлення встановлення особливостей аналізу комунікаційних загроз сучасні політичній безпеці в публічній сфері. Охарактеризовано значення «ординарних» або «буденних» підходів до політико-безпекового аналізу та продукування політико-безпекового контенту. Було підкреслено, що «ретроспективний підхід», або «метод історичних аналогій», в ситуативному вимірі передбачає порівняння безпекового меседжу або безпеково-кризової ситуації в цілому з певними історичними подіями минулого. Проаналізовано поведінку суб'єктів (акторів) ретроспективної аналітики, які ризикують зробити невірний висновок та невірно відобразити безпекову реальність. Розкрито засади коментування політико-безпекової обстановки на основі врахування відносно вузького кола фактів та обставин. З'ясовано чинники підготовки до різних результатів розвитку подій і підвищення готовності до несподіваних ситуацій. Розкрито настанови виховання культури «експериментування» та постійного вдосконалення, що особливо важливо в контексті експертного захисту бізнес-процесів від потенційних політичних загроз. Доведено, що екосистеми безпекової аналітики та інтеграція спостережень за відкритими даними надають можливість підвищення ефективності безпекового аналізу. Встановлено, що мережна горизонтальна комунікація та «екосистеми» обміну даних між спорідненими неурядовими експертно-аналітичними структурами зосереджені на розумінні та використанні соціальних і організаційних мереж для виявлення потенційних загроз і можливостей для співпраці. Обґрунтовано, що у виробництві безпекового аналітичного контенту важливим є застосування принципів гнучкого управління проєктами. Встановлено, що можливості підвищення ефективності ретроспективної аналітики з'являються на основі добору історичних аналогій за параметрами умов функціоналу. З'ясовано, що аналітики намагаються оцінити безпекові події з боку «відстороненого спостерігача» на основі підходу «від зворотного». Зроблено висновок, що важливим засобом дискредитації інформаційних «вкидів» ворога є асиметрична комунікаційна дія (акція) на основі формування порядку денного.

Ключові слова: політична комунікація, політична безпека, інформаційна провокація, інформаційна інвазія, експертний продукт, інформаційно-комунікаційна поведінка.

THE CONTEMPORARY POLITICAL SECURITY ANALYTICS: «ORDINARY» APPROACHES TO THE FORMATION OF PUBLIC EXPERT CONTENT

Abstract

The article is devoted to the basics of public perception of the political security of the state in the conditions of a full-scale invasion of modern Russia into Ukraine. The purpose of the study is to establish the specifics of the analysis of communication threats to modern political security in the public sphere. The significance of "ordinary" or "everyday" approaches to political-security analysis and production of political-security content is characterized. It was emphasized that the "retrospective approach" or "method of historical analogies" in

the situational dimension involves comparing the security message or the security crisis situation as a whole with certain historical events of the past. The behavior of the subjects (actors) of the retrospective analysis, who risk drawing the wrong conclusion and incorrectly reflecting the real world, is analyzed. The principles of commenting on the political and security situation based on taking into account a relatively narrow range of facts and circumstances are revealed. The factors of preparation for various outcomes of the development of events and increased preparedness for unexpected situations have been clarified. The guidelines for fostering a culture of "experimentation" and continuous improvement, which is especially important in the context of expert protection of business processes from potential political threats, are revealed. Security analytics ecosystems and the integration of open data observations have been proven to improve the effectiveness of security analysis. Networked horizontal communication and data sharing "ecosystems" between related non-governmental expert-analytical structures have been found to focus on understanding and using social and organizational networks to identify potential threats and opportunities for cooperation. It is substantiated that in the production of secure analytical content it is important to apply the principles of flexible project management. It was established that the possibilities of increasing the effectiveness of retrospective analytics appear on the basis of the selection of historical analogies according to the parameters of the functional conditions. It was found that analysts try to assess security events from the side of a "distant observer" based on a "backward" approach. It was concluded that an important means of discrediting informational "throws" of the enemy is an asymmetric communication action (action) based on the formation of the agenda.

Keywords: political communication, political security, information provocation, information invasion, expert product, information and communication behavior.

Постановка проблеми.

Публічна сфера політики виступає середовищем активної презентації політичних акторів. Її інституційна структура формується на основі публічного аргументативного дискурсу політичних партій, громадських організацій, публічної влади та політичних медіа тощо. В плані продукування та поширення політичного контенту публічна сфера політики – це сукупність повідомлень політичної тематики, а також дискурсивних виступів мовників, які мають політичне маркування у вигляді посади, неформальної участі в політичних процесах або політико-медійної історії.

Сприйняття політичної безпеки держави в умовах повномасштабного вторгнення сучасної росії реалізується на основі підходів, які почасти характерні для доцифрової доби. Аналіз застосування так званих російських інформаційно-психологічних операцій доводить, що їхніми основними напрямками є дискредитація Збройних сил України, діючої державної влади, українських національних цінностей, політичних сил та суспільства в цілому.

Оскільки середовище політичної комунікації України ґрунтується на демократичних принципах, для ворожих мовників досить легким завданням є трансляція прихованих деструктивних меседжів, спрямованих на поширення негативних настроїв, підрив патріотичної громадянської позиції, внесення розколу та конфліктності у відносини між громадянами та групами.

У цих умовах набуває актуальності інструментарій аналізу комунікаційних загроз політичній безпеці, які можуть бути поширені як механізфми захисту на буденному рівні та функціонуванні держави суспільства, самоврядних громад тощо. Ідеться про підходи до сприйняття інформаційних повідомлень в різних цифрових джерелах, які можуть формувати раціонально-критичну позицію й безсторонній аналізи політичних фактів та подій. Це середовище, який буде мати імунітет не спробами ворожих інформаційних провокацій та інвазій.

Аналіз публікацій.

Методологія та методика аналізу стану тполітчиної безпеки цікавить значну кількість сучасних науковців. Зокрема, Б.Бузан, О.Вайвер, та Дж. де Уайлд розробляли концептуальний апарат аналізу безпеки [Buzan, Wyver, de Wilde 1998], М.Ніколетт і К.М.Кавана встановлювали критичні можливості для безпеки інформації та управління подіями [Nicolett, Kavanagh 2021], Н.Кшетрі зіставляє поняття інформаційно-комунікаційних технологій,

стратегічної асиметрії та національної безпеки [Kshetri 2020], Д.Бастьєн, В.Монте, С.Герен, Ч.Жоель вказують на перехід від аналізу моделі до системи аналізу безпеки [Bastien, Monthe, Guérin, Joël 2022]. Однак потребує пильної уваги розробка системи експертно-аналітичної роботи, спрямованої на виробництво якісного комунікаційного продукту, спрямованого на укріплення політичної безпеки в Україні.

Метою статті є встановлення особливостей аналізу комунікаційних загроз сучасні політичній безпеці в публічній сфері. Завданням статті є виявлення підходів до продукування та поширення експертно-аналітичного контенту, спрямованого на протидію інформаційній агресії росії.

Основний зміст статті.

«Ординарні» або «буденні» підходи до політико-безпекового аналізу та продукування політико-безпекового контенту ґрунтуються на «стихійному» поширенні принципів Adhoc-аналітики в умовах цифровізації суспільства. Вони мають дуже давні традиції та пов'язані з масовими уявленнями щодо логіки ситуативного владно-управлінського мислення на стратегічному та тактичному рівні. «Ретроспективний підхід», або «метод історичних аналогій», в ситуативному вимірі передбачає порівняння безпекового меседжу або безпеково-кризової ситуації в цілому з певними історичними подіями минулого. Здобутком цього підходу є висновки щодо аналогічного варіанту поведінки та ухвалення стандартних рішень. Обмеженнями цього підходу є те, що сучасні технологічні зміни, а також зміна обсягів якісної й кількісної інформації не дозволяють повною мірою встановити міру тотожності сучасної та минулої ситуації. Внаслідок цього суб'єкт (актор) ретроспективної аналітики ризикує зробити невірний висновок та невірно відобразити реальність, що оточує.

Адхократичні (від лат. Ad hoc – ситуативні) методи аналізу безпеки – це адаптивні та гнучкі підходи до оцінки та управління ризиками безпеки в динамічному політичному середовищі, що швидко змінюється. Означені методи підкреслюють децентралізоване прийняття рішень, співпрацю та інновації. Вони передбачають коментування політико-безпекової обстановки на основі врахування відносну вузького кола фактів та обставин.

Аналіз кейсів політичної ретроспективи як адхок-метод передбачає постійну оцінку та переоцінку ризиків у режимі реального часу. Це вимагає від команд експертів бути гнучкими та здатними швидко адаптуватися до нової безпекової інформації та мінливих обставин. Зокрема, канадійський дослідник Я.Тобмен наводить приклад із «реального світу», згідно з яким після зіткнення з економічною та фінансовою кризою, Ліван розглядає можливість офіційного запровадження контролю над рухом капіталу, щоб зберегти обмежені валютні резерви, які залишилися в країні. Це суттєво завадило б канадським компаніям, які ведуть бізнес у Лівані, переказувати кошти з країни [Tobman 2022].

В рамках продукування безпекового контенту експертні команди зазвичай розробляють кілька сценаріїв потенційних загроз безпеці та проводять моделювання для тестування відповідей-рекомендацій. Це допомагає підготуватися до різних результатів розвитку подій і підвищити готовність до несподіваних ситуацій. Ризик-аналітик Я.Тобмен наголошує, що аби краще зрозуміти вплив, який певні політичні ризики можуть мати на бізнес, необхідно уважніше розглядати практичні приклади [Tobman 2022].

Адхократичні методи безпекової аналітики й консультування включають швидку розробку та тестування заходів або стратегій безпеки, навчання на невдачах і повторення досвіду успішних рішень. Такі настанови виховують культуру «експериментування» та постійного вдосконалення, що особливо важливо в контексті експертного захисту бізнес-процесів від політичних загроз. Ян Тобмен наголошує, що після спроби державного перевороту в 2016 році турецький уряд «націлився» на національні компанії, пов'язані з опозиційним рухом Ґюлена, які стояли за спробою перевороту. Каральні дії Р.Ердогана включали свавільне встановлення нормативних вимог аж до повної експропріації. Репресивний вплив на канадійські компанії полягав у тому, що їм потрібно було додати додатко-

вий рівень належної перевірки контрагентів до будь-яких ділових відносин з турецькими компаніями, щоб визначити їхні стосунки з урядом [Tobman 2022].

Екосистеми безпекової аналітики та інтеграція спостережень за відкритими даними надають можливість окремим особам (уповноваженим посадовцям) і командам на всіх рівнях приймати рішення, пов'язані з безпекою. Такий підхід дозволяє швидше реагувати та використовує локальну інформацію (дані) та різнобічний досвід. Використання «колективного інтелекту» широкого кола зацікавлених сторін (стейкхолдерів безпеки), включаючи співробітників, партнерів і громадськість, для виявлення та оцінки загроз безпеці зазвичай призводить до інноваційних та ефективних рішень.

В рамках організаційних зусиль щодо продукування публічного безпекового контенту лідери (менеджери) експертів в адхократичних системах, аналітики й фахівці з консультування демонструють гнучкість, креативність і чуйність. Вони підтримують експертні команди в складних і невизначених середовищах, сприяючи розвитку атмосфери довіри та розширення можливостей неординарної протидії загрозам застосування насильства. Внаслідок цього загрози політичного насильства визначаються як будь-які насильницькі чи ворожі дії, вчинені з основною метою або змінити чи повалити уряд країни або змінити його політику [Tobman, 2022]. Я.Тобмен також вказує, що прикладом політичного насильства є конфлікт в Україні. Вторгнення росії в Україну на початку 2022 року значно підвищив ризики для канадських компаній, які працювали в Україні. Політичне насильство також може приймати форму соціальних заворушень, як це видно з останніх подій у Пакистані [Tobman 2022].

Сучасна мережна горизонтальна комунікація та «екосистеми» обміну даних між спорідненими неурядовими експертно-аналітичними структурами зосереджені на розумінні та використанні соціальних і організаційних мереж для виявлення потенційних загроз і можливостей для безпекової співпраці між різними політичними акторами. Такі підходи допомагають визначити ключових впливових осіб і потенційні джерела ризику. Згідно з методичними напрацюваннями щодо «холістичної» (комплексної, всезагальної) безпеки, незважаючи на проведення ситуаційного моніторингу, необхідно критично ставитися до джерел інформації. Чи отримуємо ми всю інформацію з одного джерела? Якщо так, чи можемо ми бути впевнені, що джерело надійне? Якщо ми покладаємося виключно на повідомлення ЗМІ, щоб визначити нашу безпекову ситуацію, чи буде нам корисно диверсифікувати наші джерела? Колеги, друзі та партнерські організації, а також науковці, експерти, дружні органи влади та посольства, серед іншого, можуть бути багатими джерелами контекстної інформації, яка може мати стосунок до стратегії та безпеки організації [The holistic security manual 2024].

Значну частину публічної безпекової аналітики зосереджено на розвитку здатності протистояти інцидентам загрози та небезпеки та сприяти відновленню неурядових організацій після них. Це включає створення надійних систем, навчання персоналу та виховання культури стійкості. Посібник з «холістичної» безпеки вказує низку методичних структур, які можна використовувати для ситуаційного аналізу. На безпековий аналітичний контент впливають два поширені типи аналізу ситуації, які часто проводяться в контексті стратегічного планування. Це передусім PESTLE (політичний, економічний, соціальний, технологічний, правовий та екологічний) аналіз та SWOT (сильні сторони, слабкі сторони, можливості та загрози) аналіз [The holistic security manual 2024].

У рамках виробництва безпекового аналітичного контенту важливим є застосування принципів гнучкого управління проєктами, зокрема таких, як ітеративна розробка, періодична переоцінка та гнучке реагування на зміни без пекової ситуації, до аналізу безпеки та розробки стратегії [Security Technologies, 2020]. Як вказують напрацювання зі сфери діяльності правозахисних організацій, у рамках стратегічного безпекового планування потрібно проводити регулярний і поглиблений ситуаційний аналіз, тобто свідомо визначати останні безпекові події, які мають стосунок

до роботи організації, коментувати й аналізувати, що вони можуть означати. Це допоможе позиціонувати роботу та активність у поточних місцевих, регіональних, національних і глобальних подіях, а також визначити ті, які можуть вказувати на зміни в нашій безпековій ситуації [The holistic security manual 2024].

Важливим чинником самовідтворення безпекового експертно-аналітичного середовища є створення механізмів постійного зворотного зв'язку та навчання [Kazai, Craswell, Spielman, Wang 2024]. Це включає в себе аналіз після виконання комунікаційних дій, процеси безперервного вдосконалення та сприяння середовищу, в якому публічні відгуки (коментарі) активно вивчаються та використовуються.

Водночас необхідно зазначити, що стихійна діджитальна безпекова аналітика «страждає» ретроспективною референційністю не через «любов» авторів цифрових послань до історії, а через відсутність валідної інсайдерської інформації. Можливості підвищення ефективності ретроспективної аналітики з'являються на основі добору історичних аналогій за параметрами умов функціоналу інститутів та або дійових осіб, ситуації та масштабу за безпекової загрози тощо (див.:[Buzan, Wyver, de Wilde 1998]). Зокрема, застосування ретроспективної аналітики на основі аналогій між відомими подіями Другої світової війни та сучасної міжнародної ситуації навколо конфлікту в Україні, вимагає чіткої категоризації дійових осіб, інститутів та всієї сукупності обставин. При цьому слід постійно наголошувати на імовірності припущень та їх умовності.

Поширений метод безпекової аналітики на основі усвідомлення стану суб'єкта (або «ставити себе на місце діючого суб'єкта») полягає в тому, що експерт намагається уявити і зрозуміти логіку мислення та дій певної інституції та особистості. Зазначений підхід вимагає розвиненої уяви дослідника, а також навичок «герменевтичного розуміння» реальності як тексту на основі психологічних рис, нормативних передумов, етичних та ціннісних запобіжників тощо. Перебування «на місці об'єкта рішень» дає змогу продукувати неординарну та креативну інформацію. Водночас її підтвердження завжди буде під питанням та потребувати підтвердження або спростування версії [Granka 2010].

Одним з найбільш поширених та давніх підходів до буденної аналітики безпекової ситуації є метод «читання між рядків». На його основі аналітик намагається оцінити події з боку «відстороненого спостерігача» на основі підходу «від зворотного». Цей метод означає «граничну недовіру» до текстових та вербальних послань, а також до подій в їх публічному і явному прояві з точки зору «публічної розвідки» («public intelligence») (див.:[General Dynamics 2010]). Пошук пояснень та причинно-наслідкових зв'язків «за лаштунками» дає змогу напрацювати крайні екстремальні версії подій. В подальшому вони вимагають роботи з підтвердження та або спростування [Jerit, Zhao 2020].

Заслуговує на згадку так звана «проюридична» («проюстиційна») безпекова аналітика, відома з часів римського права. Вона пропонує такий поширений публічний спосіб аналізу безпекових подій та вчинків, як «шукати кому вигідно» («Cui prodest»). Означений підхід вимагає знання правил гри та уявлення про типові траєкторії дій суб'єктів у певній безпековій ситуації. Цей підхід дає змогу ідентифікувати потенційні небезпеки пов'язані з наявними акторами, сформувати «карту («шахівницю») дійових осіб». Водночас цей підхід страждає вадою упередженості, певною «презумпцією провини», коли певним суб'єктом можуть бути прописані неіснуючі інтенції та намагання, що може істотним чином перевантажити аналітичний апарат.

Висновки.

Таким чином, аналітична рамка публічних виступів в контексті протидії комунікаційним інвазіям росії будується на поєднанні раціонально-логічних принципів аналізу, а також комплексних адаптивних підходів до відповідальної політико-комунікаційної поведінки за цифрової доби. В основу оцінки імовірності застосування ворогом інформаційно-психологічної операції, акції або кампанії, які мають політичний зміст та або контекст, покладені такий принцип як ретроспективний аналіз, (або метод історичних аналогій), реалізація

герменевтичного розуміння в рамках ставлення себе на місце суб'єкта інформаційної інвазії або провокації. Важливе значення має застосування принципу «кому вигідно» тощо.

На буденному рівні подібні міркування стихійно посідають найбільший обсяг контенту коментарів, виступів, реакцій, заяв тощо. Водночас необхідно розуміти, що з точки зору уявлень про середовище політичної публічної сфери, визначального значення набуває доречність застосування того чи іншого принципу, компетентність та кваліфікація аналітика, рівень доступу до відкритої та/або інсайдерської інформації тощо.

У цілому розв'язання завдань комплексного аналізу інформаційно-аналітичного забезпечення діяльності української держави та суспільства в умовах війни вимагає заходів щодо моніторингу політичних повідомлень на основі цілеспрямованого залучення ресурсів та фахівців. Тенденція до «розвінчання ворожих фейків» є важливим елементом державної інформаційної політики та протидії ворожій інформаційній агресії. Водночас важливим засобом дискредитації інформаційних «вкидів» ворога є асиметрична комунікаційна дія (акція) на основі формування порядку денного публічної сфери, оперативна оцінка поточних подій, масована критична обробка та супровід дій політичних посадовців ворога та їх союзників на міжнародній арені.

Зазначені підходи можуть бути корисними для інституалізації демократичної публічної сфери політики в Україні. Ці аспекти можуть бути основою для подальших наукових досліджень за темою даної статті.

Бібліографічні посилання / References

ANSI/ISA-TR99.00.01. (2020). Security Technologies for Manufacturing and control Systems. *Instrument Society of America*. 21-76.

Bastien, D., Monthe, V., Guérin, S., Joël, Ch. (2022). Security Analysis: From model to system analysis. CRiSiS 2022: International Conference on Risks and Security of Internet and Systems, Sousse, Tunisia. *HAL Open Access.* Retrieved May 17, 2024 from https://hal.science/hal-03866297/document

Buzan, B. Wyver, O., de Wilde, J. (1998). Security Analysis: Conceptual Apparatus. Security: A New Framework for Analysis, Boulder, USA: Lynne Rienner Publishers, 21-48. https://doi.org/10.1515/9781685853808-003

General Dynamics. (2010). R&D Support of DARPA Cyber Genome Program. Retrieved May 12, 2024 from https://info.publicintelligence.net/DARPA-CyberGenome.pdf

Granka, L.A. (2010). The Politics of Search: A Decade Retrospective. *The Information Society.* 26(5), 364-374.

Jerit, J., and Zhao, Y. (2020). Political Misinformation. *View Affiliations,* 23, 77-94. https://doi.org/10.1146/annurev-polisci-050718-032814

Kazai, Th., Craswell, P.G., Spielman, S., Wang, H.Y. et al. (2024). What Matters in a Measure? A Perspective from Large-Scale Search Evaluation. Proceedings of the 47th International ACM SIGIR Conference on Research and Development in Information. https://dl.acm.org/doi/10.1145/3626772.3657845

Kshetri, N. (2020). Information and communications technologies, strategic asymmetry and national security. *Journal of International Management,* 11, 563-580.

Nicolett, M., Kavanagh, K.M. (2021). Critical Capabilities for Security Information and Event Management. *Gartner Group,* May 2021, 25-31.

Situation monitoring and analysis. The holistic security manual. Retrieved May 12, 2024 from https://holistic-security.tacticaltech.org/chapters/explore/2-2-situation-monitoring-and-analysis.html

Tobman, I. (2022). 3 types of political risks and how to manage them. *EDC.* Retrieved May 12, 2024 from https://www.edc.ca/en/blog/managing-political-risks.html