

## ОСОБЛИВОСТІ ПРОВЕДЕННЯ АНАЛІЗУ ВІДКРИТИХ ДЖЕРЕЛ ПРИ РОЗРОБЛЕННІ ПАСПОРТУ ЦІЛЮВИХ АУДИТОРІЙ В ІНТЕРЕСАХ РЕАЛІЗАЦІЇ СТРАТЕГІЧНОГО НАРАТИВУ ДЕРЖАВИ

*В статті розглядається аналіз відкритих джерел який базується на методі OSINT розвідки при розробленні паспорту цільової аудиторії в інтересах реалізації стратегічного нарративу держави.*

*Для досягнення мети статті автором узагальнені підходи до аналізу відкритих джерел інформації та розроблено пропозиції щодо формування паспорту цільової аудиторії. Визначено процес ведення розвідки з відкритих джерел інформації, обґрунтовані критерії які висуваються до розвідданих отриманих з відкритих джерел інформації. Розглянуто типи ведення такої розвідки. Узагальнені критерії дали можливість визначити перелік програмних продуктів, які раціонально використовувати при проведенні розвідки з відкритих джерел, а також проведено короткий огляд та можливості цих програмних продуктів.*

*З метою узагальнення та систематизації отриманих розвідданих з відкритих джерел автором запропоновано створення паспорту цільової аудиторії. Розглянуто загальну структуру самого бланку паспорту та особливості структури заповнення отриманої інформації з відкритих джерел.*

*Запропонований підхід щодо аналізу відкритих джерел при розробленні паспорту цільової аудиторії в інтересах реалізації стратегічного нарративу держави надасть можливість вірно побудувати та реалізувати систему інформаційної безпеки у війсьній сфері у формі стратегічних комунікацій Міністерства оборони та Збройних Сил України. Проведений аналіз надасть можливість визначити основні потреби та вразливі місця цільових аудиторій та реалізувати інтереси держави у вигляді підтримки населення щодо стратегічного курсу держави на набуття повноправного членства України в ЄС та НАТО.*

**Ключові слова:** OSINT розвідка, цільова аудиторія, стратегічний нарратив.

### Вступ

Розглядаючи зростання інформатизації суспільства та збільшення впливу кіберпростору на людство в цілому, слід визнати, що сучасний розвиток інформаційних технологій призвів до кризи існуючих джерел розповсюдження інформації, насамперед традиційних мас-медіа. Незважаючи на перехід засобів масової інформації на електронну форму, вони й надалі використовують стару модель комунікацій, в якій цільова аудиторія є лише пасивним споживачем інформаційного продукту. Традиційні засоби масової інформації, навіть в електронній формі, значно поступаються сучасним Інтернет – технологіям, оскільки все більше асоціюються з пропагандою та нав'язуванням інформації. Це значно знижує ступінь довіри до існуючих джерел розповсюдження інформації, які намагаються здійснити інформаційний вплив на визначені об'єкти впливу. Відсутність державних джерел розповсюдження інформації тягне за собою проблему щодо інформування суспільства про реалізацію стратегічних цілей держави.

**Постановка проблеми.** При реалізації стратегічних комунікацій держави набуває актуальності проблема визначення цільових аудиторій які формують основні погляди населення на визначений державою стратегічний курс. На сьогоднішній день не існує жодного нормативного документу який регламентує порядок визначення та отримання інформації про цільові аудиторії.

Стратегічні комунікації на сьогоднішній день перебувають в стадії становлення, при чому цей процес, на відміну від провідних країн світу, відбувається в реальних бойових умовах. Тому

наявні проблеми та труднощі потребують оперативного визначення та вирішення. Основна увага стратегічних комунікацій при реалізації стратегічного нарративу держави спрямована на цільові аудиторії [1].

Проблема визначення цільових аудиторій широкого формату набула в дослідженнях маркетингових та підприємців, які розробляли оцінку споживача, щоб точніше втілити потреби покупця та розробити окремі пропозиції для кожного. Оцінка та вибір цільової аудиторії при реалізації стратегічного нарративу держави повинен враховувати сучасні методи аналізу, які будуть базуватись на результатах аналізу відкритих джерел інформації з використанням методик аналізу даних.

**Аналіз останніх досліджень і публікацій.** Проблематикою реалізації стратегічних комунікацій держави на сьогоднішній день займається велика низка вітчизняних та закордонних вчених. в роботах Ланде Д.В., Даника Ю.Г., Сальнікової О.Ф., Сніцаренка П.М. висвітлено матеріал щодо понятійно-категорійного апарату та основні засади реалізації стратегічних комунікацій держави. Ці роботи стали твердим науковим підґрунтям для розвитку вітчизняної системи стратегічних комунікацій.

Значного успіху у визначенні цільових аудиторій та їх оцінці в сфері маркетингу досягнув Марк Шеррінгтон [2]. В своїх роботах він детально описав практичні методи, визначив труднощі, які можуть траплятись при визначенні цільових аудиторій ринку збуту продукції та шляхи їх подолання.

В попередніх працях [3,4] автором було обґрунтовано стратегічний нарратив держави та

проведено аналіз сталості процесу розвитку громадської думки при реалізації стратегічного нарративу держави. В працях [5,6] розглянуто підходи щодо оцінки ефективності функціонування системи стратегічних комунікацій Міністерства оборони та Збройних Сил України і оцінки загроз інформаційній безпеці України у воєнній сфері. Також розглядалися питання особливостей сприйняття та реагування на отриману інформацію[7], однак досліджень щодо аналізу відкритих джерел та розроблення паспорту цільової аудиторії не проводилось.

**Метою статті** є наукове обґрунтування особливостей застосування методу OSINT розвідки проведення аналізу відкритих джерел при розробленні паспорту цільових аудиторій в інтересах реалізації стратегічного нарративу держави.

## Виклад основного матеріалу дослідження

З кожним роком кількість користувачів мережі Інтернет зростає. На початок жовтня 2020 року 4.9 млрд людей, а це 63,2% жителів землі, користується глобальною мережею. А розмір даних в цій мережі досяг 2.7 зеттабайт (1 ЗБ ~ 1012ГБ). З року в рік кількість користувачів і пристроїв, підключених до мережі, збільшується на 6% і 10% відповідно. Велика частина цієї інформації є відкритою. Джерела, що посилаються на ці дані або на дані з газет, журналів, радіо і телепередач, публічних звітах уряду, називаються відкритими [8]. Світова статистика використання мережі Інтернет в третьому кварталі 2020 року представлена в таблиці 1.

Таблиця 1

Світова статистика використання Інтернету

Реґіон	Чисельність населення (2020 р.)	% від чисельності населення світу	Інтернет-користувачі	Рівень розповсюдження (% від чис. нас.)	Зростання 2000-2020	% від світового інтернету
Африка	1340598447	17,2%	63194772	47,1%	13898%	12,8%
Азія	4294516659	55,1%	2555636255	59,5%	2136%	51,8%
Європа	834995197	10,7%	727848547	87,2%	593%	14,8%
Латинська Америка/Карибський Басейн	654287232	8,4%	467817332	71,5%	2489%	9,5%
Середній Схід	260991690	3,3%	184856,813	70,8%	5527%	3,7%
Північна Америка	368869647	4,7%	332908868	90,3%	208%	6,8%
Океанія / Австралія	42690838	0,5%	28917600	67,7%	279%	0,6%
Всього	7796949710	100%	4929926187	63,2%	1266%	100%

Оцінка використання Інтернету та світової статистики населення наведена в таблиці узагальнена станом на 20 жовтня 2020 р. Демографічні показники (населення) базуються на даних Відділу ООН з питань народонаселення. Інформація про використання Інтернету узагальнена на підставі даних, опублікованих Nielsen Online, Міжнародним союзом телекомунікацій, GfK, місцевими регуляторами ІКТ та інших джерел.

Відкриті джерела містять достатню кількість інформації, обробка та аналіз якої дозволяють синтезувати нові знання, що сприяють прогнозуванню можливих впливів людського та фізичного чинників на розвиток оперативної обстановки на місцях проведення інформаційних та психологічних операцій. Синергетичний ефект при веденні OSINT розвідки досягається у результаті комплексування добутої відкритої інформації та розвідувальної інформації, що добута технічними засобами та оперативними методами. При відпрацюванні паспорту цільової аудиторії пропонується застосувати саме методу OSINT розвідки, що являє собою аналіз відкритих джерел.

OSINT повна англійська версія Open Source INTelligence – це технологія пошуку, акумулювання і аналізу даних, зібраних з доступних джерел в мережі Інтернет. Можна стверджувати, що OSINT розвідка – це вид розвідки, що ведеться шляхом систематичного збору інформації з відкритих джерел, її аналізу, підготовки та своєчасного надання кінцевого продукту замовнику з метою забезпечення його потреб у такій інформації.

Процес ведення OSINT розвідки складається з

чотирьох етапів – планування, підготовки, збору та виробництва кінцевого матеріалу і чотирьох постійних дій – аналізу, накопичення розвідданих їх оцінювання та розподілу за напрямками (Рис.1) [9].

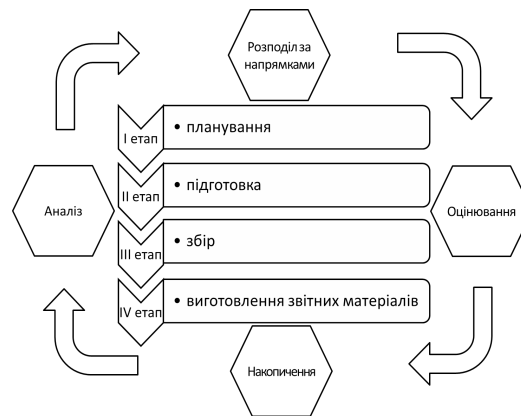


Рис. 1. Етапи та дії при здійсненні OSINT розвідки

Розвіддані отримані з відкритих джерел часом не тільки не відрізняються від секретних матеріалів, але часто можуть перевершувати їх своєю цінністю з точки зору аналізу та розвитку розвідувальних моментів. Під загальними критеріями розвідданих розуміють такі, як швидкість надходження, об'єми, якість, ясність, легкість подальшого використання і вартість отримання.

Під швидкістю розуміємо, час отримання розвідувальної інформації. Коли в якій-небудь точці планети вибухає криза, а можливості розвідки в даному регіоні обмежені, то і аналітики розвідслужб, і представники структур, які формують державну політику, найчастіше вмикають телевізор або відправляються за поточною інформацією в мережу

Інтернет. Більш того, те ж саме може відбуватися і з регіонами, де широко розгорнута мережа агентурної розвідки або HUMINT мережі. Події розвиваються стрімко, тому в моменти криз найбільш змістовно відображаються в поточних новинах, наприклад за падінням Берлінської стіни, скажімо, і в Вашингтоні, і в штаб-квартирі ЦРУ в Ленглі, що достовірно відомо, стежили не зі зведень розвідслужб, а припавши до екранів телевізорів з репортажами CNN з місця подій.

Під критерієм об'єми розуміється кількість матеріалу для отримання розвідданих. У світі завжди буде набагато більше всляких блогерів, журналістів, незалежних експертів, телереporterів та інших обізнаних людей, ніж кількість кадрових розвідників, яке може дозволити собі мати будь-яка спецслужба, нехай навіть найбільша і багата. Два-три професійних розвідника з хорошою агентурною мережею, годі й казати, можуть перевершувати хоч сотню реporterів за своїми можливостями доступу до секретів. Але, як показує досвід, уміло зібрані фрагменти інформації з відкритих джерел за своєю сукупною значущістю можуть бути цілком еквівалентні, а іноді і перевершують суто секретні розвідувальні звіти.

Під якістю розуміємо, те що інформацію отриману з відкритих джерел можна перевірити з декількох джерел. В роботі розвідслужб будь-якої країни раз у раз бувають ситуації, коли кадрові співробітники готують свої звіти на основі отриманої від таємних агентів інформації, яка навмисне сфабрикована або просто фрагментарно використана з місцевих газет і прикрашена для надання їй важливості. У порівнянні з такими розвідданими звичайна інформація з відкритих джерел виявляється якіснішою хоча б у тому, що не викривлена фантазією агентів [10].

Критерій ясності відображає невизначена ступінь достовірності добутої інформації. Для аналітиків розвідки і політичних діячів серйозну проблему представляє невизначена ступінь достовірності добутої інформації, навіть якщо вона отримана через агентурні джерела. Наприклад, коли співробітник Аналітичного управління (DI) ЦРУ читає доповідь про іноземного лідера, складений на основі відомостей від «джерела з неперевіреною надійністю», то більш-менш ясно, як цей документ слід сприймати. Проблема стає куди складніше, якщо цікавий звіт складений за даними від «надійного джерела». Принципово важливо, яким саме є дане джерело. Працівником в офісі лідера, його братом, або ж коханкою брата дружини працівника офісу? Аналітик в Ленглі як правило ніколи не знає відповідь на це питання, тому що співробітники Оперативного управління (DO) ЦРУ ретельно оберігають свої джерела і методи отримання інформації.

Легкість використання. Будь-які таємниці прийнято оточувати бар'єрами з грифів секретності, принципів ізоляції інформації та особливих режимів доступу. Все це робить надзвичайно непростою не тільки процес передачі здобутих відомостей в певні структури, які приймають рішення, але і поширення важливих даних серед розвідників або суміжників з контррозвідки, не кажучи вже про поліцію. Що ж

стосується даних OSINT, то зрозуміло, що їх можна легко передавати в будь-які зацікавлені інстанції.

Критерій вартості відображає необхідні фінансові витрати на отримання розвідданих. Супутник видової розвідки, що запускається і підтримується в працездатному стані на орбіті за рахунок витрат в мільярди доларів, може надати фотографії того, як виглядає дах військового заводу або корпус нового підводного човна. З іншого боку, в правильно обраному іноземному журналі з ціною річної передплати близько сотні доларів можна виявити фотографії, зняті в цехах заводу або в середині тієї ж самої нової субмарини.

Проведення OSINT розвідки може здійснюватись за трьома типами здобування інформації: пасивного, напівпасивного і активного. Вибір пріоритетного типу залежить від сценарію, в якому працює процес збору даних, а також від типу даних, які цікавлять. Пасивний збір інформації-це найбільш часто використовуваний тип збору та обробки даних. Такий тип збору інформації використовується тільки через загальнодоступні ресурси. При проведенні напівпасивного типу збору інформації з технічної точки зору цей тип збору відправляє обмежений трафік на цільові сервери для отримання загальної інформації про них. Цей трафік намагається нагадувати типовий інтернет-трафік, щоб не привертати уваги до вашої розвідувальної діяльності. При веденні активного типу здобування інформації здійснюється взаємодія безпосередньо з системою, про яку збирається інформація. Власник може дізнатися про те що у відношенні до нього ведеться розвідка, так як людина / організація, яка збирає інформацію, буде використовувати передові методи для збору технічних даних про цільову IT-інфраструктуру, таких як доступ до відкритих портів, сканування вразливостей (наприклад, неліцензійний Windows), сканування додатків веб-сервера і т. д. Цей трафік буде виглядати як підозріле або зловмисна поведінка і залишить сліди в системі виявлення вторгнень (IDS) або системі запобігання вторгнень (IPS). Проведення атак соціальної інженерії вважається одним з видів активного збору інформації [11].

Для ведення такої розвідки необхідно використовувати певні інструменти, які мають доступ до відкритих джерел інформації. До стеку програмних продуктів та найбільш популярними інструментами збору інформації з відкритих джерел відносяться: Shodan, Maltego, Google Dorks, Foca, Spyse.

Shodan – пошуковик по пристроях, підключених до мережі (в т.ч. інтернет і веб-додатки). Розділ «Explore» допоможе почати пошуки, так як туди збираються запити користувачів. Щоб отримати доступ до розширеного пошуку, треба зареєструватися. У платних версіях надається доступ до більшої кількості пристроїв, а також необмежену кількість пошукових запитів в добу.

Maltego – програмне забезпечення яке збирає всі дані, допомагає побачити взаємозв'язок і зробити висновки. Результат візуалізуються у вигляді дерева, що збирає в єдину систему IP-адреси, e-mails, телефони, домени.

Google Dorks – це запити в Googl з використанням спеціальних операторів. Для пошуку точного словосполучення потрібно поставити слова в лапки, а щоб виключити будь-які дані з видачі, необхідно поставити перед ним «-».

Foca – програма, яка допомагає з вивантаженням, класифікацією і аналізом файлів на віддаленому веб-

сервері. Для цього вона сканує певний домен за допомогою пошукових систем Google, Bing, DuckDuckGo. Цей програмний продукт безкоштовний і швидко встановлюється.

Spyse – пошуковик по технічній інформації веб-сайтів. Використання якого надає можливість встановити різноманітні дані, на кшталт вразливостей, IP-адрес, субдоменів і SSL / TLS.

Отже, запропонований метод ведення OSINT розвідки надасть можливість визначити цільові аудиторії для реалізації стратегічного нарративу держави з мінімальними затратами часу та коштів.

В стратегічних комунікаціях під цільовою аудиторією розуміється не тільки й не стільки спільність людей, об'єднаних національними, соціальними або майновими ознаками, що проживають у деякій країні, а в першу чергу спільність, що поділяє однакову систему цінностей.

До суб'єктів, що формують цільову аудиторію належать: органи державної влади та місцевого самоврядування; політичні партії, громадські організації, об'єднання, рухи та блоки; засоби масової інформації; релігійні, національні та інші організації; соціальні групи; окремі посадові, військові службові особи; органи військового управління, правоохоронні і спеціальні органи; політичні та громадські лідери, які невійськовими (або військовими) засобами відстоюють (або реалізують) державні, колективні, політичні та особисті інтереси, цілі тощо. Тобто можна зробити визначення, що цільова аудиторія – це фізична особа, декілька осіб або визначена група людей, які об'єднані за певними критеріями (вікові, релігійні, суспільні, політичні, соціальні, психологічні чи інші) та мають певний спільний інтерес чи наміри та на яких розробляється та розраховується той чи інший продукт для подальшої зміни в їхній поведінці в процесі проведення інформаційної чи психологічної операцій.

При реалізації Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України заходи інформаційно-психологічного впливу будуть здійснюватись на окупованих територіях, на підконтрольних територіях для популяризації проєвропейського курсу держави буде проводитись інформування населення [12].

Щоб ефективно використовувати наявні сили та засоби системи стратегічних комунікацій Міністерства оборони та Збройних Сил України при розробленні матеріалів інформування пропонується використовувати паспорт цільової аудиторії де будуть описані потреби тієї чи іншої аудиторії, що дозволить виробнику матеріалу визначити потребу цільової аудиторії та відповідний інформаційний продукт. Звісно що найбільшого успіху можливо досягнути тільки у тому випадку, коли зібрано та узагальнено всі характеристики споживача інформаційного продукту (цільової аудиторії) – результатом цієї роботи є паспорт (відомості про загальні данні) цільової аудиторії (Рис. 2).

Паспорт цільової аудиторії являє собою двосторонній бланк, який по заповненню включає п'ять пунктів, що містять відомості про загальні характеристики цільової аудиторії, її цілі та

цінності, інформацію про труднощі та больові точки, потреби та інформаційні джерела, тобто з яких джерел отримує інформацію цільова аудиторія [9].

Паспорт цільової аудиторії		
<b>ЦІЛІ ТА ЦІННОСТІ</b> Що хоче: Що важливо: Зв'язок з іншими ЦА: Результат оцінки:	Віковий діапазон: Загальна чисельність: Стать: Місце проживання: Відношення до релігії: Цитата:	<b>ТРУДНОЦІ ТА БОЛЬОВІ ТОЧКИ:</b> Психологічна уразливість: Демографічна уразливість: Чого уникає: Що боїться: Символи:
	<b>ДЖЕРЕЛА ІНФОРМАЦІЇ</b> Газети: Журнали: Блоги/веб-сайти: Телеканали: Неформальні лідери: Додатково:	Чим займаються: Середній дохід: Освіта: Наявні критерії оцінки: Додатково:

Рис. 2. Паспорт цільової аудиторії

В загальних відомостях відображаються данні про середній вік, стать, місце проживання, відношення до релігії, освіта, середній дохід та чим займається цільова аудиторія. Також важливими характеристиками що зазначаються у цьому пункті є наявні критерії оцінки, які можуть бути: специфічними; піддаватися вимірюванню (дані можуть бути визначені кількісно); помітні (наочні) – (дані можна побачити чи почути). За потреби визначаються додаткові необхідні відомості про цільову аудиторію та цитата, яка дасть коротку характеристику цієї аудиторії і буде використовуватись в подальшому плануванні інформаційних та психологічних операцій як псевдонім (шифр) з метою запобігання щодо розголошення відомостей з обмеженим доступом.

В пункті “Цілі та цінності” відображаються данні про те, чого бажає досягти цільова аудиторія, що є для неї важливим та її цінності, будь-які матеріальні або ідеальні явища, які мають значення для цільової аудиторії, заради якого вона діє, витрачає сили, час, гроші, здоров'я тощо, заради якого вона живе. Також зазначаються відомості про політичні погляди (відношення до влади та Збройних Сил).

В пункті “Джерела інформації” визначається, в який спосіб цільова аудиторія отримує інформаційний продукт, та встановлюється, які способи інформування користуються більшою довірою серед цільової аудиторії, що надасть можливість визначити самі ефективні способи інформування для проведення інформаційних та психологічних впливів з практичної точки зору. Також в цьому блоці зазначаються відомості про формальних чи неформальних лідерів, керівництво яких визнають всі члени цільової аудиторії та покладаються на нього у прийнятті серйозних рішень і вирішенні важливих проблем. За потреби визначаються додаткові необхідні відомості про цільову аудиторію.

В розділі “Труidнощі та больові точки” відображаються відомості про критерії уразливості цільової аудиторії. Уразливість – це характеристика, мотив чи умова, які можуть бути використані для здійснення впливу на думку (поведінку) цільової аудиторії. До них відносяться психологічна уразливість, демографічна уразливість та символи. Психологічна уразливість включає показники страху,

ненависті, гніву невдоволеності. Демографічна уразливість включає в себе показники етнічності, політичної приналежності, освіти, місця проживання та географічні умови. Символи – це любі візуальні, слухові чи змішані знаки, які мають культурне чи контекстуальне значення для цільової аудиторії. Вони служать для передачі складних ідей і емоцій у відносно простих зображень або звуків. Пов'язуючи або уникаючи символів, які викликають певні емоції або передають певні ідеї цільовій аудиторії, інформаційна чи психологічна операція може значно збільшити переконливість аргументу (інформаційного продукту).

В пункті “Потреби” містяться відомості про загальне розуміння цільовою аудиторією необхідних матеріальних та нематеріальних потреб для подальшого існування. Причини, що заважають досягнути бажаної думки (поведінки) цільової аудиторії, до них відносяться: економічні (доходи, робота, інфраструктура), політичні (закони, вибори, лідери), соціальні та культурні (культурні норми, віросповідання), або фізичні (місцевість, погодні умови, санітарні умови). Відображаються фактори, які послідовно склалися в навколишньому середовищі цільової аудиторії, які впливають на поведінку та події, які склалися ментально і впливають на поведінку. Також відображаються дані про головний аргумент. Головним аргументом є причина того, чому саме цільова аудиторія повинна змінити свою думку (поведінку) на бажану. Тобто аргумент надає керівництво і загальну основу для побудови інформаційних та психологічних операцій, щоб в кінцевому рахунку переконати цільову аудиторію думати або поводитися бажаним чином.

### Література

**1. Войтко О.В.** Оцінювання ефективності функціонування системи стратегічних комунікацій Міністерства оборони та Збройних Сил України. Науковий журнал “Системи управління, навігації та зв’язку”. 2018. – №3(49). – С. 97-99. **2. Марк Шеррінгтон** Незримые ценности бренда. 2006. 304 с. URL: <https://www.livelib.ru/author/122455/top-m-sherrington>. **3. Солонніков В.Г., Войтко О.В., Пащенко Т.П.** Обґрунтування реалізації стратегічного нарративу держави. Науковий журнал “Сучасні інформаційні технології у сфері безпеки та оборони”. 2020. №1(37). – С. 203-212. **4. Войтко О.В., Солонніков В.Г., Полякова О.В.** Особливості застосування методу фрактального аналізу сталості процесу розвитку громадської думки при реалізації стратегічного нарративу держави. Науковий журнал “Сучасні інформаційні технології у сфері безпеки та оборони”. 2020. №2(38). – С. 145-150. **5. Войтко О.В.** Оцінювання ефективності функціонування системи стратегічних комунікацій Міністерства оборони та Збройних Сил України. Науковий журнал “Системи управління, навігації та зв’язку”. 2018. №3(49). – С. 97-99. **6. Кацалап В.О., Войтко О.В., Чернега В.М.** Методика оцінки загроз інформаційній

### Висновки і перспективи подальших досліджень

Основною ціллю для системи стратегічних комунікацій Міністерства оборони та Збройних Сил України є досягнення стратегічного нарративу. Як зазначалось вище, статистика громадської думки щодо підтримки вступу до ЄС та НАТО дещо зменшується тому таким нарративом для цієї системи має бути зміна громадської думки для підтримки стратегічного курсу держави.

Отже, запропонований підхід щодо аналізу відкритих джерел при розробленні паспорту цільової аудиторії в інтересах реалізації стратегічного нарративу держави надасть можливість вірно побудувати та реалізувати систему інформаційної безпеки у воєнній сфері у формі стратегічних комунікацій Міністерства оборони та Збройних Сил України. Проведений аналіз надасть можливість визначити основні потреби та вразливі місця цільових аудиторій та реалізувати інтереси держави у вигляді підтримки населення щодо стратегічного курсу держави на набуття повноправного членства України в ЄС та НАТО.

Подальший розвиток цього дослідження необхідно проводити на основі сучасних наукових методів теорії соціальних досліджень та досліджень каналів розповсюдження інформації. Встановлення ступеню ефективності цих каналів. Особливо важливо провести дослідження каналів отримання інформації на тимчасово окупованих територіях Донецької та Луганської областей, а також Автономної республіки Крим, які характеризують потреби кожної цільової аудиторії. Це дасть можливість ефективно розповсюджувати аргументовані повідомлення та отримати необхідний рівень підтримки населення, щодо реалізації стратегічного нарративу держави.

безпеці України у воєнній сфері. Науковий журнал “Сучасні інформаційні технології у сфері безпеки та оборони”. 2018. №1(31). – С.149-154. **7. Войтко О.В., Кацалап В.О., Чернега В.М.** Особливості сприйняття та реагування на отриману інформацію. Науковий журнал “Сучасні інформаційні технології у сфері безпеки та оборони”. 2019. №3(36). – С. 171-174. **8.** Разведка на основе открытых источников. Інтернет ресурс URL: <https://www.internetworldstats.com>. **9. Войтко О.В.** Реалізації державної інформаційної політики та забезпечення інформаційної безпеки в умовах конфлікту з Російською Федерацією. Міжнародний науковий журнал “Грааль науки” № 1 (Лютий, 2021). – С. 164-166. **10. Киви Берд** Модель OSINT. Разведка без тайн. Інтернет ресурс URL: <https://www.litmir.me/br/?b=132711&p=1>. **11. K.Molodetska, V.Solonnikov, O.Voitko** Counteraction to information influence in social networking services by means of fuzzy logic system. “International Journal of Electrical and Computer Engineering” Vol. 11. № 3 – 2020. – P.2490-2499. **12.** Про затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України: Наказ Міністра оборони України від 22.11.2017 р. №612/2017. URL: <http://www.mil.gov.ua>.

## ПАСПОРТА ЦЕЛЕВЫХ АУДИТОРИЙ В ИНТЕРЕСАХ РЕАЛИЗАЦИИ СТРАТЕГИЧЕСКОГО НАРРАТИВА ГОСУДАРСТВА

*Александр Владимирович Войтко (кандидат военных наук)*

*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

*В статье рассматривается анализ открытых источников основанный на методе OSINT*

разведки при разработке паспорта целевой аудитории в интересах реализации стратегического нарратива государства.

Для достижения цели статье автором обобщены подходы к анализу открытых источников информации и разработаны предложения по формированию паспорта целевой аудитории. Определены процессы ведения разведки из открытых источников информации, обоснованы критерии предъявляемые к разведанным полученным из открытых источников информации. Рассмотрены типы ведения такой разведки. Обобщенные критерии разрешили определить перечень программных продуктов, рационально использовать при проведении разведки из открытых источников, а также проведен краткий обзор и возможности этих программных продуктов.

С целью обобщения и систематизации полученных разведанных из открытых источников автором предложено создание паспорта целевой аудитории. Рассмотрена общая структура самого бланка паспорта и особенности структуры заполнения полученной информации из открытых источников.

Предложенный подход к анализу открытых источников при разработке паспорта целевой аудитории в интересах реализации стратегического нарратива государства позволит верно построить и реализовать систему информационной безопасности в военной сфере в форме стратегических коммуникаций Министерства обороны и Вооруженных Сил Украины. Проведенный анализ позволит определить основные потребности и уязвимые места целевых аудиторий и реализовать интересы государства в виде поддержки населения по стратегическому курсу государства на приобретение полноправного членства Украины в ЕС и НАТО.

**Ключевые слова:** OSINT разведка, целевая аудитория, стратегический нарратив.

## FEATURES OF ANALYSIS OF OPEN SOURCES IN THE DEVELOPMENT OF THE PASSPORT OF TARGET AUDIENCES IN THE INTEREST OF THE IMPLEMENTATION OF STRATEGIC DERATOR

*Oleksandr Voitko (Candidate of Military Sciences)*

*National Defence University of Ukraine named after Ivan Cherniakhovskiy, Kyiv, Ukraine*

The article considers the analysis of open sources based on the method of OSINT intelligence in the development of passports of the target audience in the interests of the implementation of the strategic narrative of the state.

To achieve the goal of the article, the author generalized approaches to the analysis of open sources of information and developed proposals for the formation of the passport of the target audience. The process of conducting intelligence from open sources of information is defined, the criteria which are put forward to the intelligence received from open sources of information are substantiated. The types of conducting such reconnaissance are considered. The generalized criteria made it possible to determine the list of software products that can be rationally used in open source exploration, as well as a brief overview and capabilities of these software products.

In order to summarize and systematize the information obtained from open sources, the author proposes to create a passport of the target audience. The general structure of the passport form and features of the structure of filling in the received information from open sources are considered.

The proposed approach to the analysis of open sources in the development of the target audience's passports in the interests of the strategic narrative of the state will allow to correctly build and implement a system of information security in the military sphere in the form of strategic communications of the Ministry of Defense and the Armed Forces of Ukraine. The analysis will provide an opportunity to identify the main needs and vulnerabilities of target audiences and realize the interests of the state in the form of public support for the strategic course of the state to gain full membership of Ukraine in the EU and NATO.

**Key words:** OSINT intelligence, target audience, strategic narrative.

### References

- 1. Voitko O.V.** Ocinnuvannja efektyvnosti funkcionuvannja systemy strategichnykh komunikacij Ministerstva obrony ta Zbrojnykh Syl Ukrainy. Naukovyj zhurnal "Systemy upravlinnja, navigacij i ta zv'jazku". 2018. – № 3(49). – S. 97-99.
- 2. Mark Sherrington** Nezrimvie tsennosti brenda 2006. 304 c.
- 3. Solonnikov V.G., Voitko O.V., Pashhenko T.P.** Obruntuvannja realizaciji strategichnogho naratyvu derzhavv. Naukovyj zhurnal "Suchasni informacijni tekhnologhiji u sferi bezpeky ta obrony". 2020. № 1(37). – S. 203-212.
- 4. Voitko O.V., Solonnikov V.G., Poljakova O.V.** Osoblyvosti zastosuvannja metodu fraktalnogho analizu stalosti procesu rozvytku ghromadsjkoji dumky pry realizaciji strategichnogho naratyvu derzhavy. Naukovyj zhurnal "Suchasni informacijni tekhnologhiji u sferi bezpeky ta obrony". 2020. № 2(38). – S. 145-150.
- 5. Voitko O.V.** Ocinnuvannja efektyvnosti funkcionuvannja systemy strategichnykh komunikacij Ministerstva obrony ta Zbrojnykh Syl Ukrainy. Naukovyj zhurnal "Systemy upravlinnja, navigacij i ta zv'jazku". 2018. № 3(49). – S. 97-99.
- 6. Kacalap V.O., Voitko O.V., Chernegha V.M.** Metodyka ocinky zagroz informacijnij bezpeci Ukrainy u vojennij sferi. Naukovyj zhurnal "Suchasni informacijni tekhnologhiji u sferi bezpeky ta obrony". 2018. № 1(31). – S.149-154.
- 7. Voitko O.V., Kacalap V.O., Chernegha V.M.** Osoblyvosti sprvinjattja ta reaghuvannja na otrymanu informaciju. Naukovyj zhurnal "Suchasni informacijni tekhnologhiji u sferi bezpeky ta obrony". 2019. № 3(36). – S.171-174.
- 8.** Razvedka na osnove otkrytyih istochnikov. Internet resurs.
- 9. Voitko O.V.** Realizaciji derzhavnoji informacijnoji polityky ta zabezpechennja informacijnoji bezpeky v umovakh konfliktu z Rosijskoju Federacijeu. Mizhnarodnyj naukovyj zhurnal "Ghraal nauky" № 1 (Ljutyj, 2021). – S. 164-166.
- 10. Kyvy Berd** Modelj OSINT. Razvedka bez tajn. Internet resurs
- 11. K.Molodetska, V.Solonnikov, O.Voitko** Counteraction to information influence in social networking services by means of fuzzy logic system. "International Journal of Electrical and Computer Engineering" Vol. 11. № 3 – 2020. – P.2490-2499.
- 12.** Pro zatverdzhennja Koncepciji strategichnykh komunikacij Ministerstva obrony Ukrainy ta Zbrojnykh Syl Ukrainy: Nakaz Ministra obrony Ukrainy vid 22.11.2017 r. № 612/2017.