УДК 342.951

ПОЛЯКОВ О.М., начальник відділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: http://orcid.org/0000-0002-8984-1476.

ОСОБЛИВОСТІ ПРОТИДІЇ ПОШИРЕННЮ ДЕСТРУКТИВНОГО КОНТЕНТУ

Анотація. *Визначено поняття та ознаки деструктивного контенту. Висвітлено загрози та ризики, пов'язані із поширенням деструктивного контенту. Розкрито зарубіжний досвід методологічного забезпечення протидії деструктивному контенту в контексті засад державної інформаційної політики. Деталізовано механізми поширення деструктивного контенту російського походження. Акцентовно увагу на ворожій діяльності ботоферм та тролеферм, "кремлеботів" на шкоду державним інтересам. Розкрито особливості поширення деструктивних матеріалів фізичними особами – політологами, блогерами, лідерами громадських організацій. Проаналізовані новели вітчизняного законодавства, норми якого присвячені боротьбі з деструктивним контентом та російською пропагандою. Визначено сфери діяльності вітчизняної спецслужби щодо блокування деструктивного контенту та протиправних інформаційних матеріалів. Окреслено здобутки Служби безпеки України у сфері захисту вітчизняного інформаційного простору від злочинних посягань з боку РФ та її колаборантів. Визначено шляхи удосконалення вітчизняного законодавства для посилення кримінальної відповідальності за поширення деструктивного контенту в Інтернеті та у соціальних мережах.*

Ключові слова: *ботоіндустрія, ботоферма, тролеферма, інформаційний простір, національна безпека, цифрові технології, наративи, деструктивний контент, спецслужба, астротурфінг, соціальні мережі.*

Summary*. The definitions and the signs of destructive content are defined. The threats and risks associated with the spread of destructive content are highlighted. The foreign experience of methodological protection against destructive content in the context of the principles of state information policy is revealed. The mechanisms of the distribution of destructive content of Russian origin are detailed. Special attention is paid to the hostile activities of bot farms and troll farms, "Kremlin bots" to the detriment of state interests. The peculiarities of the distribution of destructive materials by individuals – political scientists, bloggers, leaders of public organizations – have been revealed. The novellas of domestic legislation, the norms of which are devoted to the fight against destructive content and Russian propaganda, are analyzed. The spheres of activity of the domestic special service regarding the blocking of destructive content and illegal information materials have been determined. The achievements of the Security Service of Ukraine in the sphere of protection of the domestic information space from criminal actions by the Russian Federation and its collaborators are outlined. The directions of improvement of domestic legislation with the aim of strengthening criminal liability for spreading destructive content on the Internet and social networks have been identified.*

Keywords*: bot industry, bot farm, troll farm, information space, national security, digital technologies, narratives, destructive content, special service, astroturfing, social media.*

Постановка проблеми. В умовах війни, яку розв'язала держава-агресор проти України, підрив інформаційного суверенітету нашої країни залишається одним із пріоритетних завдань військово-політичного керівництва РФ. Держава-агресор активно веде розвідувально-підривну діяльність проти України, використовуючи наявний арсенал

сил та засобів на інформаційному фронті, який залишається не менш важливим, ніж військові дії. Ця країна спрямовує максимальні зусилля та використовує власні напрацювання й потужності з метою розколу українського суспільства. Ботоферми, тролеферми, псевдоексперти, інформаційно-психологічні операції, нав'язування проросійських меседжів – усе це є в арсеналі ворога. Він намагається використати будь-який привід аби підігріти внутрішні чвари чи маніпулювати громадською думкою. Також це діяльність агентури, координованої представниками російських спецслужб, створення ботоферм й тролеферм для поширення деструктивного контенту на користь РФ, використання соціальних мереж для просування наративів ідеології "руського мира", поширення репостів російських пропагандистів через своїх прихильників в Україні, фейків та дезінформації.

Загальновідомо, що з метою маніпулювання свідомістю світової спільности, пересічних українських громадян, інспірування соціальної напруги, а також поширення забороненої законом інформації РФ та її сателіти використовують сучасні новітні технології, зокрема соціальні мережі та системи мікроблогів на шкоду державним інтересам України, прагнучи заподіяння масштабних негативних наслідків за результатами своєї протиправної діяльності. Соціальні мережі, месенджери, Інтернет-площадки залишаються найбільш вразливими з точки зору можливостей оприлюднення інформації антиукраїнського змісту та проведення потужних інформаційних кампаній на шкоду державним інтересам.

Серед проблемних моментів у цій сфері експерти виокремлюють також надчутливу реакцію громадськості на будь-які ініціативи щодо запровадження жорсткого контролю, що можуть тлумачитися як порушення прав та свобод людини, в т.ч. на рівні міжнародних недержавних правозахисних організацій. Останнім часом в умовах правового режиму військового стану в Україні має стійкий прояв загрозлива тенденція поширення деструктивного (протиправного) контенту російського походження на шкоду державним інтересам України. У зв'язку із викладеним, заслуговують на увагу питання щодо висвітлення механізмів виявлення та блокування деструктивного контенту, визначення шляхів удосконалення вітчизняного законодавства у цій площині.

Результати аналізу наукових публікацій. Проблемні питання, присвячені вивченню загрозливих тенденцій в контексті поширення деструктивного контенту, зокрема в мережі Інтернет та у соціальних мережах, досліджували у своїх наукових працях: С. Гуржій [1], Д. Дубов [2], Ю. Калайда [3], А. Митко та Н. Шуляк [4], В. Пивоваров [5], А. Юшкова [6]. Проте практичні питання та особливості протидії поширенню деструктивному контенту російського походження висвітлені не достатньо, що посилює актуальність цієї статті.

Метою статті є визначення та масштабування загрозливих тенденцій поширення російського деструктивного контенту в умовах правового режиму військового стану, огляд діяльності вітчизняної спецслужби у зазначеній сфері, визначення шляхів удосконалення чинного законодавства з протидії деструктивному контенту та внесення пропозицій з посилення відповідальності за поширення наративів й концептів російського пропаганди та ідеології "руського миру".

Виклад основного матеріалу. Одним із основних ризиків цифрового простору у цілому та у соціальних медіа, зокрема є контентні ризики. Загалом до них відносяться матеріали, які містять ознаки насильства, прояви тероризму, агресію, жорстокість, дитячу порнографію, прояви расової чи релігійної нетерпимості, ксенофобію, нецензурну лексику тощо. Таким чином, деструктивний контент – це контент, який несе загрозу та спричиняє шкоду особі, суспільству, державі. Під деструктивним контентом

розуміють інформацію, яка чинить негативний вплив на психіку людини або на суспільну свідомість, а його поширення порушує права та законні інтереси користувачів, суспільства, держави. Проте сама по собі інформація рідко буває шкідливою. Вона стає шкідливою тільки завдяки користувачам, які її поширюють. Будь-який вид деструктивного контенту пов'язаний з широким прошарком людей, які є споживачами відповідної інформації.

За таких умов актуальну проблему становлять Інтернет-ресурси, соціальні мережі, ЗМІ, Інтернет-площадки, які поширюють деструктивні матеріали, оскільки така інформація має необмежений доступ.

Розуміючи актуальність цієї проблематики, у зарубіжних країнах негативний контент поділяють на два види: незаконний або протиправний (illegal) та шкідливий (harmful). Перший – це інформація, яка заборонена до поширення законом, а другий – інша суспільно небезпечна інформація, яка не забороняється кримінальним або адміністративним законодавством, але для якої встановлені певні обмеження на її поширення. Якщо щодо першого виду все зрозуміло, то щодо другого – спостерігаються значні відмінності між країнами та загальна невизначеність у цій сфері. Виходячи із статистики, з країн-членів ОБСЄ тільки 34 % блокують будь-який шкідливий або негативний контент та переважно для цього підставою вбачаються локальні моральні або етичні норми, релігійні переконання, певні уявлення або гіпотези. Хоча певні переконання, погляди, постулати, ідеї, які не порушують будь-яких законів та не становлять суспільної загрози, реально можуть бути шкідливими та небезпечними та такими, що, на жаль, безкарно поширюються. Таким чином, будь-яка держава світу має вживати дієвих заходів політичного, економічного та організаційного-правового характеру з метою боротьби з поширенням деструктивного контенту, заборонених інформаційних матеріалів.

Інтернет-ресурси, соціальні мережі, електронні та друковані ЗМІ несуть відповідальність за поширення деструктивної інформації, яка може спричинити шкоду державним або громадським інтересам. Проте кількість інформації, яка поширюється у мережі Інтернет, постійно та динамічно зростає. Виявити у таких обсягах інформацію, яка порушує закон, не зачепивши випадково нейтральні дані – досить складне завдання. Власники сайтів самостійно здійснюють модерацію вхідного контенту, намагаючись уникнути проблем із законом, а проактивні громадяни можуть подати заявки на "гарячу" лінію. Однак навіть у випадку активної співпраці населення та провайдерів, великі масиви інформації можуть залишитися без належного контролю. Адже успішної співпраці може і не бути, оскільки не усі заходи щодо заборони контенту, який визнається деструктивним, популярні у населення.

Загальновідомим методом боротьби з деструктивним контентом є його блокування. Технічно воно відбувається у смузі доступу (на комп'ютері користувача), у мережі (на рівні провайдера) та інфраструктурно (через глобальні інфраструктурні сервіси). Адже в сучасних умовах блокування будь-якого контенту у мережі пов'язано із значними труднощами. По-перше, практично не існує методу, який би гарантував повне блокування ресурсу. Чимало засобів блокування заважають доступу не тільки до контенту, який видаляється, але й до усього сегменту мережі у цілому, що обмежує права законних користувачів, що, у свою чергу, призводить до суспільного обурення. Більш того, набувають обертів технології мережі, які входять у конфлікт з методами блокування.

Що стосується існуючих у зарубіжних державах юридичних та економічних методів боротьби з деструктивним контентом, то вилучення негативного контенту з

мережі може бути досягнуто таким чином: повідомлення постачальника послуг та закриття ним сайту; видалення посилання з пошуку; виключення сайту з контекстної реклами; вилучення домена. Таким чином, боротьба з деструктивним контентом відбувається завдяки спільним зусиллям провайдерів, постачальників платіжних та пошукових послуг, власників серверів та звичайними користувачами мережі, які допомагають виявити сайти, які порушують чинне законодавство. Це вимагає розробки збалансованих соціальних, правових, етнічних та інших стандартів поведінки у мережі Інтернет. Наприклад, у деяких країнах світу механізмом ефективної боротьби з деструктивним контентом є уповільнення роботи соціальної мережі Twitter.

Сьогодні немає єдиного узагальненого визначення понять "деструктивного контенту" або "інформація деструктивної спрямованості", проте у чинних нормативно-правових актах України згадується інформація як "шкідлива", "заборонена" і "протиправна". Проактивне зростання обсягів деструктивного контенту – глобальна проблема світових масштабів, реакцією на яку стало схвалення більшістю зарубіжних країн (Німеччина, Великобританія, Франція, Австрія, Туреччина) відповідних законопроектів, спрямованих на врегулювання Інтернет-середовища та створення безпечного інформаційного простору. Так, 29 липня 2020 року Парламент Туреччини ухвалив закон, який передбачає контроль соціальних мереж та контенту на платформах, а також зобов'язує соцмережі дотримуватися суворих правил, невиконання яких тягне штрафи. Цим законом передбачається обов'язок компаній мати представництва у Туреччині, які розглядатимуть скарги щодо контенту на своїх платформах. Більше того, компанії зобов'язують мати представника, який має громадянство Туреччини, аби він міг визначати, чи потрібно видаляти контент та наскільки він є прийнятним для громадян країни, а також виконувати ухвали суду щодо його вилучення. У випадку невиконання вимог законом передбачено серйозні штрафи, заборону на рекламу та скорочення трафіку до 90 %. Від соцмереж вимагається зберігати дані користувачів в Туреччині, що значно спростило правоохоронним органам доступ до цієї інформації [11].

У жовтні 2022 року Парламент Туреччини схвалив закон, норми якого передбачають тюремне ув'язнення журналістів та користувачів соціальних мереж на строк до трьох років за поширення фейків та дезінформації. Зокрема, диспозиція статті 29 вказаного законодавчого акта регламентує, що особи, які поширюють фальсифіковану або неправдиву інформацію в мережі Інтернет з метою створення ідеологічного підґрунтя для побоювань та страху, закликів до порушення громадського порядку, караються позбавлення волі строком від одного до трьох років [12].

В США з метою протидії негативним наслідкам злочинної діяльності ботофермам та тролефермам держслужбовцям законодавчо заборонено встановлювати на робочі телефони або інші пристрої додаток TikTok. Підставами для цього стала підтверджена інформація ФБР США про те, що РФ та Китай можуть використовувати TikTok та його дані у своїх протиправних цілях, зокрема, за допомогою алгоритмів проводити операції маніпуляційного впливу на американських користувачів [13].

За таких умов, організація системного моніторингу та фіксації різноманітних інформаційних ресурсів й соціальних мереж на предмет наявності деструктивного контенту та їхнє блокування стає більш актуальним завданням будь-якої держави. Застосування інформаційних технологій з метою поширення деструктивного контенту у сучасному світі все частіше сприяє розпалюванню міжрасової ворожнечі, поширенню соціальної напруги, ескалації військової агресії, тероризму, ксенофобії. З урахуванням складності процесів, пов'язаних з виявленням деструктивного контенту у мережі

Інтернет, правоохоронні органи вимушені впроваджувати та застосовувати системи інтелектуального пошуку та штучного інтелекту, а також активізувати роботу з компаніями, які спеціалізуються на інформаційно-пошукових системах.

Аналіз вітчизняного законодавства свідчить про те, що заходи, які вживаються у сфері контролю обігу інформації деструктивної спрямованості, фактично зводяться до рекомендацій щодо блокування деструктивного контенту та залучення до цього процесу спеціалізованих експертів та правоохоронців. Вбачається, що, враховуючи масштаби та швидкість приросту й оновлення поширюваного інформаційного деструктивного контенту, контролювати цей процес лише силами експертів та правоохоронців практично неможливо, особливо в умовах правового режиму військового стану.

Окрім того, процедура ідентифікації в інформаційному просторі деструктивного контенту та подальшої класифікації інформації на цій підставі вбачається доволі складним та повільним процесом, який ускладнюється невизначеністю в системі критеріїв віднесення інформації до категорії деструктивної. Залучення до цих процесів експертів та правоохоронців підвищує вірогідність помилок суб'єктивного характеру, впливає на коректність та адекватність підсумкових експертних заключень. Тому виникає нагальна потреба у розробці уніфікованого алгоритмічного та відповідного програмного забезпечення, зокрема й штучного інтелекту, що надасть змогу здійснювати класифікацію великих обсягів неструктурованої текстової інформації з урахуванням її використання з протиправною метою.

Активне використання швидкозмінного контенту надає змогу поширювати деструктивну інформацію, яка негативно впливає на міжнародний імідж нашої держави та українське суспільство в цілому, спричиняючи шкоду національним інтересам в інформаційній сфері. Інформаційні продукти, які вірогідно можуть поширюватися вороже налаштованими державами проти України (РФ, Білорусь, Іран, Угорщина, КНДР) у світовій та вітчизняній блогосферах, можуть містити деструктивні матеріали, які несуть суттєву загрозу для національної безпеки України. Окрім антиукраїнської пропаганди та дезінформації, які поширюють в світовому та вітчизняному інформаційному полі вказані держави, ними використовуються, у тому числі, окремі закордонні інформаційні структури, медійні та навколомедійні організації, провайдери програмних послуг (насамперед РФ, Угорщина), які намагаються сформувати механізми впливу на суспільно-політичну ситуацію в Україні шляхом створення позицій в інформаційному просторі держави, використання вітчизняних ЗМІ, мережі Інтернет, власних інформаційних можливостей для здійснення антиукраїнських інформаційних акцій, інспірування в середовищі національних меншин автономістських та сепаратистських настроїв, поширення деструктивної інформації в інтересах іноземних держав, особливо в умовах масштабної військової агресії РФ та її сателітів проти України. На цьому фоні, на жаль, спостерігається загрозлива тенденція постійного збільшення деструктивного контенту російського походження у вітчизняному сегменті мережі Інтернет та у деяких мас-медіа.

При цьому, важливу роль під час формування деструктивного контенту мають саме наративи. Наратив – це ментальна структура, за допомогою якої можна зрозуміти, як саме відбувається мислення людини, як воно структуроване. В сучасних умовах наратив можна уявити як ментальну конструкцію, що описує події у реальному світі у певному порядку. Наративи прийшли з літературознавства, де вони використовувалися для опису структури оповідання. Це мережа причинно-наслідкових зв'язків, що розкривають, що і з чого випливає. Наратив є типовою формою, за допомогою якої люди намагаються пояснювати світ. Наративи задають причини військових дій, щоб виправдати їх в очах

свого населення та всього світу. РФ озвучила свої стратегічні цілі у війні проти України як “демілітаризація” та “денацифікація”. Але вони виявилися надто слабкими і розпливчастими, щоб змусити своє населення йти на війну. Вони були зовсім не опрацьовані саме як наративи та їх було важко застосувати до України. Це призвело не лише до провалів на самій війні, а й масових втеч громадян за кордон під час оголошеної “часткової мобілізації”. Проте російська пропаганда спирається саме на ці наративи, оскільки інших не було заявлено. Сьогодні їх продовжують активно підтримувати, передусім, у російських та білоруських мас-медіа. Російський наратив “заганяє” Україну в “неправильний” світ, тим самим виправдовуючи свою агресію. Спочатку він визнавав Україну державою, яка не відбулася, подаючи себе як держава, яка створює норми іншим. Така негативна оцінка України існувала останніх двадцять років. Тому сьогоднішня російська пропаганда лише продовжує наративи негативної оцінки України в російській масовій свідомості. Зміщення акцентів військових дій в інформаційну та віртуальну сферу створило прецедент “м’якого” типу війни, яка відбувається без жертв у фізичному просторі, оскільки там бойові дії не ведуться. Але вони ведуться у двох інших просторах, причому тепер віртуальний простір є визначальним.

Важливою складовою політики Кремля стає впровадження деструктивних наративів в інформаційний простір нашої держави та деяких європейських країн світу. Завдяки здійсненню таких операцій їх ініціатор намагається сформувати вигідний для себе порядок денний, посилити конфліктні для суспільства теми, забезпечити потрібний фокус емоційної уваги громадян [2, с. 3]. Також РФ намагається поширювати серед населення України та світової спільноти депресивний контент, який спричиняє шкоду психічному здоров’ю громадян, пропагує психічні розлади, сіє паніку, страх, постійну схвильованість та стурбованість.

З метою поширення деструктивного контенту РФ активно використовує ботоферми. Ботоферми з’явилися майже одночасно з появою соцмереж, коли помітили вплив коментарів на думку суспільства. Залучити живих людей на масовані атаки – затратно і довго. Керувати мільйонами акаунтів може програма і команда учасників, яка координує цей процес для того, щоб ботсторінки не блокували. Загалом ботоферми – це компанії, які масово створюють несправжніх користувачів соцмереж і від їхнього імені пишуть тисячі коментарів. Сьогодні будь-яка особа може придбати ботоферму для підтримки свого позитивного рейтингу або політичного іміджу. Формат роботи ботоферми – написання коментарів. Щодня ботоферма готує мінімум 200-300 коментарів для різних політичних сил. У ботів навіть є спеціальні прийоми, щоб здаватися для цільової аудиторії реальними людьми за допомогою створення діалогів між різними фейковими акаунтами.

Під ботофермами, як правило, розуміють сукупність акаунтів в соціальних мережах, які поширюють інформацію для загальнодоступних чи закритих спільнот, здійснюють автоматичне коментування публікацій, діяльність яких підпадає під ознаки скоординованої неавтентичної поведінки. Ботоферми розрізнити доволі просто. Ботоферми – це компанії, які масово створюють несправжніх користувачів соцмереж і від їхнього імені пишуть тисячі коментарів. Ботоферми зазвичай створюються, як шахрайський інструмент масштабування інформаційного впливу на певні аудиторії. Цей тіньовий ринок послуг сягає мільйонів доларів на рік. Водночас чимало ботоферм працюють на російські спецслужби, допомагаючи державі-агресору в її деструктивній діяльності.

Розвиток ботоіндустрії сприяє поширенню наративів російської пропаганди та деструктивного контенту, переважно на замовлення спецслужб РФ. З цією метою держава-агресор використовує так званих "кремлеботів" – фейкових коментаторів, які атакують західну пресу та ЗМІ. У фокусі уваги російських "кремлеботів" перебувають електронні видання США, Великобританії, Франції, Німеччини та інших держав ЄС. Метою їхньої діяльності є коментування новин, у яких вони намагаються виправдати війну РФ проти України та довести західному світу "правильність" військових дій Кремля. Також "кремлеботи" намагаються довести до чисельної світової аудиторії профанацію та надумані ідеї РФ про "крах" НАТО та про те, що США ведуть "неправильну" зовнішню політику, допомагаючи Україні. Аналіз діяльності "кремлеботів" надає змогу констатувати, що один аккаунт "кремлебота" може змінювати назву 500 разів на рік. Більш того, профіль користувача, з якого здійснювалася публікація фейкових коментарів, міг змінювати локацію та "місце проживання" майже 70 разів. Загалом "кремлеботи" – це фейкові аккаунти, інструменти російського впливу у світі. На перший погляд, вони мало відрізняються від реальних людей, такої собі "диванної сотні росіян", проте насправді "кремлеботи" є зброєю в гібридній війні: впливають на суспільну думку, втручаються у хід виборів, підтримують сепаратистські референдуми, поширюють ідеї "руського миру", та зводять нанівець невигідні Кремлю дискусії – як опозиційні, так і провладні. Формат роботи "кремлеботів" – це декілька офісів, сотні працівників – все це заради просування провладних ідей РФ та створення хибного враження про світові події у користувачів соціальних мереж.

Окрім ботоферм існують і тролеферми або так звані "фабрики тролів". Тролеферма – більш складна структура, яка має свою власну ієрархію. Там працюють живі люди. Найвища ланка – це ті, хто пише пости, виступає з "експертною" думкою, ініціює дискусії й задає напрями обговорення. Як правило, вони особисто пишуть тексти на задану замовником тему, згідно з затвердженими методичними рекомендаціями. Але в них не виявиться спільних один з одним фраз і слів. Хіба що емоційно забарвлені маркери, такі як "тарифний геноцид", "київська влада", "каратели" тощо. Знов-таки, демаскуючою ознакою таких тролів є співпадіння меседжів і часу порушення того чи іншого питання. Нижче в ієрархії є виконавці, які поширюють дописи перших, додаючи свої слова і активно відповідаючи на коментарі користувачів, щоб підтримували публікацію у стрічці новин. Найнижчою ланкою є люди, які здійснюють позиційне коментування. Як правило, вони поширюють заздалегідь прописані для них (10 – 20 варіантів) коментарів і неохоче дискутують. На більш-менш серйозне питання щодо теми вони неспроможні дати відповідь.

Головне завдання тролів – ініціювати в мережі інформаційну хвилю на задану тематику (або хвилю "флуду" чи "флейму"), до якої масово приєднаються реальні користувачі, котрих на професійному жаргоні росіяни називають "арматним м'ясом". РФ активно використовує "фабрику тролів" для поширення дезінформації про війну в Україні у соціальних мережах. Кремлівська "фабрика тролів" проводить кампанію з дезінформації з метою маніпулювання міжнародною суспільною свідомістю щодо вторгнення Росії в Україну, шукає прихільників та підтримку своїх однодумців. "Фабрика тролів" також використовує месенджер Telegram для вербування та координації нових прихильників у соціальних мережах, які згодом можуть підтримати дії Росії щодо окупації України. Таким чином, держава-агресор винайшла новий спосіб поширення дезінформації про Україну через Telegram та Twitter. Російські

пропагандисти завантажують відео про війну відразу в соцмережі, що дозволяє обходити обмеження, які запровадили уряди та технологічні компанії.

Але бото- чи тролеферми не є небезпечними самі по собі. Їхню вражаючу ефективність забезпечує те, що майже всі сегменти бото- й тролеферм (якщо ми говоримо про російські) є функціональною складовою російських автоматизованих комплексів моніторингу мережі Інтернет із прихованими функціями впливу на процеси у середовищі соціальних мереж. Так, у РФ діють системи моніторингу компаній "Крібрум", "Медіалогія", "Квант", "Бастіон", "Brand Analytics" та ін. Кількість автоматизованих бот-акаунтів, які діють по всьому світу, тільки в системі "Крібрум" складає понад 100 млн. акаунтів. Таке поєднання надає змогу реалізувати небезпечну технологію впливу на користувачів соціальних мереж, так званий "астротурфінг" – імітацію широкої громадської підтримки певних ідей, переконань, думок, меседжів, а також осіб чи політичних сил. Астротурфінг надає змогу формувати фейкову громадську думку або інтерпретацію події, яку користувачі мережі Інтернет сприйматимуть як реальну і діятимуть згідно з нею. Наявність таких систем дозволяє РФ на основі моніторингу контенту в мережі Інтернет й аналітичного опрацювання "великих даних", виявляти вразливості супротивника, планувати, здійснювати й коригувати власні інформаційні атаки, а також відстежувати їхню ефективність та результативність.

Тривалий час у вітчизняному інформаційному просторі триває війна проти РФ. Завдяки зусиллям правоохоронних органів на постійній основі здійснюється протидія протиправним інформаційним вкидам і фейкам, блокуються джерела поширення деструктивних інформаційних матеріалів. Досить активно ворог працює для розпалювання міжконфесійної ворожнечі, провокування конфліктів в українській православній церкві та між різними патріархатами. Активно поширюють деструктивні матеріали російські пропагандисти та рупори Кремля, спрямовуючи надзусилля на поширення проросійської ідеології та ворожих наративів. Свідомість українців, як індивідуальну, так і масову, атакують, намагаючись вразити слабкі місця. В сучасних умовах інформаційної війни РФ проти України зазвичай російські інформаційні операції вирізняються тим, що вони плануються й реалізуються в рамках єдиного задуму та стратегічного наративу, відрізняючись лише формами й методами, а також вибором цільової аудиторії.

Складовою інформаційної агресії РФ є ідеологія формування стереотипів. Це можна зрозуміти, наприклад, опрацювавши декілька ворожих медіатекстів. Якщо розпочати фактчекінг, можливо виявити таку закономірність: у виступах, у текстах російських пропагандистів із різних джерел можна спостерігати тотожність формулювань, мовних зворотів, окремих висловлювань. Тобто Кремль доручає певним соціальним мережам та ЗМІ конкретні вказівки щодо "потрібного русла" висвітлювання подій. Щоб не потрапити в пастку проросійських медіа й не поширювати неправдиву інформацію, має бути критичне мислення. Але безпосередні виконавці часто мешкають в Україні, що і дає змогу правоохоронним органам викривати конкретних фізичних осіб, мережі ботоферм, які поширюють деструктивні матеріали та проросійські наративи, та застосовувати до них превентивні заходи, передбачені чинним законодавством.

Також поширення деструктивних та протиправних інформаційних матеріалів можуть здійснювати фізичні особи – політологи, блогери, лідери громадської думки та різноманітні експерти. Вони в основному діють у форматі "м'якої сили" (soft power), ненав'язливо (а іноді наполегливо) транслюючи аудиторії загальний стратегічний наратив впливу, формуючи відповідну мапу уявлень аудиторії та

причинно-наслідкових зв'язків різних подій так, щоб аудиторія мала спрощене, але цілісне уявлення про те, що відбувається навколо. Їхнє завдання – це інтерпретація та перекручування фактів і подій у вигідному для противника руслі. Експерти зазвичай дуже обережно висловлюються, щоб їхня діяльність не підпадала під дію кримінального закону. Ворожа пропаганда та деструктивні матеріали маскуються під "свободу слова", "альтернативну точку зору" або "політичну агітацію". Зазвичай, правоохоронці тримають таких спікерів у полі зору, проводять з ними профілактику й реагують відповідно до чинного законодавства України.

Розуміючи масштаби деструктивної підривної інформаційної діяльності РФ проти України та її негативні наслідки, у березні 2022 року в Україні було схвалено закон, норми якого забороняють виправдовувати, заперечувати збройну агресію РФ, прославляти осіб, які воюють проти України. Цим законом, зокрема, запроваджується заборона для ЗМІ на виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, зокрема шляхом представлення збройної агресії РФ проти України як внутрішнього конфлікту, громадянського конфлікту, громадянської війни, заперечення тимчасової окупації частини території України. За виправдання та прославлення російської агресії передбачається кримінальна відповідальність. Також цим законом встановлено заборону на виготовлення та поширення інформаційної продукції, спрямованої на пропаганду військових дій РФ, а також застосування до політичних партій, громадських обєднань, релігійних організацій, винних у порушені вказаних заборон у якості санкцій – заборону їхньої діяльності в судовому порядку [8].

За наслідками шалених потоків деструктивної інформації та пропагандистських матеріалів, які на перманентній основі поширює держава-агресор у світових масштабах, на початку вересня 2022 року Президент України звернувся до європейської спільности з вимогою посилити боротьбу з російською пропагандою, зокрема заборонити трансляцію усіх державних телеканалів РФ у країнах Євросоюзу. Володимир Зеленський також закликав заборонити російські державні ЗМІ в Європі, оскільки російське телебачення намагається дискредитувати європейську демократію та все ще доступне для широкої аудиторії європейських глядачів [9].

З метою консолідації зусиль протидії ворожій пропаганді та дезінформації на державному рівні 25 листопада 2022 року між Національною радою України з питань телебачення та радіомовлення й Центром протидії дезінформації при РНБО було укладено меморандум про співпрацю. Спільні зусилля вказаних інституцій будуть спрямовані на комплексну протидію дезінформації та пропаганді, деструктивним інформаційним впливам і кампаніям. Завдяки спільній роботі зазначених структур ретельно вивчатимуться такі питання, як: виявлення реальних і прогнозованих загроз інформаційній безпеці, прогнозування ризиків та загроз внаслідок їхньої реалізації; сприяння взаємодії держави та інституцій громадянського суспільства щодо протидії деструктивним впливам і кампаніям російського походження; узагальнення та аналіз досвіду інших держав і міжнародних організацій з протидії дезінформації та підготовки пропозцій щодо його використання в Україні [10].

Враховуючи виклики та загрози, пов'язані із поширенням деструктивного контенту, Служба безпеки України на перманентній основі успішно запобігає його поширенню, блокує його, притягуючи винних осіб та колаборантів до відповідальності, при цьому не допускаючи розхитування суспільно-політичної та соціально-економічної ситуації в нашій державі, запобігає поширенню у мережі Інтернет, у тому числі, й сепаратистських матеріалів, які мають за мету сприяння

розпалюванню міжнаціональної ворожнечі, поширення протестних настроїв, соціального невдоволення. Важливим та актуальним завданням вітчизняної спецслужби залишається виявлення та блокування т.зв. "кремлеботів", ботоферм, тролеферм, які поширюють деструктивний контент та працюють на замовлення кураторів спецслужб РФ з метою проведення підривної діяльності на шкоду державним інтересам України, виявлення причетних до цього фізичних осіб на території України. Служба безпеки України на постійній основі викриває ворожих агентів, які через мережу Інтернет або соціальні мережі поширюють деструктивний контент, репостять заборонені матеріали російських пропагандистських сайтів, поширюючи їх через соціальні мережі, у тому числі, заборонені в Україні.

У 2022 року вітчизняна спецслужба заблокувала 45 масштабних ботоферм потужністю понад 2 млн. фейкових акаунтів, майже 500 проросійських Youtube-каналів з аудиторією більше ніж 15 млн. підписників і близько тисячі інформресурсів, які працювали проти України [14]. Серед пріоритетних завдань Служби безпеки України в умовах правового режиму військового стану залишається виявлення та притягнення до кримінальної відповідальності зрадників, ворожих агітаторів та колаборантів, які здійснюють протиправну діяльність на шкоду державним інтересам у медіа просторі. Станом на 31 грудня 2022 року вітчизняною спецслужбою України порушено 1200 кримінальних проваджень, 600 фігурантів повідомлено про підозру та 230 фізичних осіб засуджено до різних термінів ув'язнення [15].

На системній основі спецслужба виявляє та блокує діяльність проросійськи налаштованих громадян у месенджерах та соціальних мережах. Так у січні 2023 року Служба безпеки України затримала у Києві організаторів російської "фабрики тролів" [16]. Так звані "тролі" поширювали інформацію з Telegram-каналу російського блогера-пропагандиста Юрія Подоляка, на який підписані понад 2,7 млн користувачів. Агенти Кремля репостили його публікації або поширювали під виглядом "власних" публікацій у соцмережах. Щоб збільшувати чисельність "аудиторії", використовували сотні бот-акаунтів, від імені яких поширювали і коментували дописи з російською пропагандою. За даними слідства, підривну діяльність на Київщині організували двоє місцевих жителів. Фігуранти встановили обладнання, яке передали їм російські куратори, у своїх домівках у Києві та Білій Церкві. З метою забезпечення масового "покриття" Інтернет-простору агенти мали намір залучити нових учасників пропагандистського "осередку" Кремля. Для поширення дописів вони використовували сотні бот-акаунтів, які ділились інформацією на своїх сторінках та коментували пропагандистські публікації. Під час обшуків у зловмисників знайшли мобільні телефони і комп'ютери із наявними доказами. На підставі зібраних доказів слідчі спецслужби повідомили двом фігурантам з Києва про підозру за ч. 2 ст. 436-2 Кримінального кодексу України (виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників).

Від початку повномасштабної військової агресії РФ проти України Служба безпеки України звернулася із проханням до соцмережі Telegram заблокувати понад 1,5 тисячі анонімних каналів, які поширювали дезінформацію. Мотивацією такого звернення став той факт, що з позиції національного законодавства механізми блокування Telegram-каналів та інших соціальних мереж наразі відсутні, а величезний масив непідтвердженої інформації у Telegram-каналах є серйозною проблемою, яку складно подолати, оскільки сервери компанії розташовані не в Україні [17].

Таким чином, Служба безпеки України як державний правоохоронний орган успішно викриває та припиняє злочинну діяльність інформаційних колаборантів, ботоферми та

тролеферми, які поширюють деструктивний контент на шкоду державним інтересам України, притягає до відповідальності колаборантів та прихильників “руського миру”. На цьому фоні вітчизняна спецслужба ініціює зміни до КК України щодо посилення відповідальності за скоєння такого злочину, оскільки на сьогоднішній день створення та незаконна діяльність ботоферми класифікується, як несанкціоноване втручання у роботу електронно-обчислювальних мереж (ст. 361 КК України) і карається штрафом або позбавленням волі від 2 до 6 років максимум. Водночас чимало ботоферм та “фабрик тролів” працюють на російські спецслужби, а тому такі дії мають кваліфікуватися як пособництво державі-агресору. Потребують підтримки і пропозиції спецслужби щодо криміналізації суспільно небезпечних дій зі створення та функціонування бото- і тролеферм.

Висновки.

Захист інформаційного простору України та протидія поширенню незаконного контенту – актуальне та важливе завдання держави в сучасних умовах. Під час правового режиму військового стану до незаконного (деструктивного) контенту у мережі Інтернет та соціальних мережах переважно відносяться пропагандистські інформаційні матеріали, які містять заклики до повалення конституційного ладу та посягання на територіальну цілісність України, розпалювання національної чи релігійної ворожнечі, проявів ксенофобії, виправдовування російської військової агресії проти України, глорифікації її учасників тощо. Також до цієї категорії належать пропагандистські матеріали та дописи із закликами до окупації України у соціальних мережах. На жаль, в сучасних реаліях спостерігається значна інформаційна присутність РФ у медіа просторі держав ЄС та США, що провокує розробку організаційно-правових засад протидії російській пропаганді, дезінформації, фейкам та деструктивному контенту. Провокація загострення протиріч, інформаційна і фінансова підтримка конфліктів на територіях західних демократій стали можливими завдяки використанню РФ армії фейкових аккаунтів, кремлеботів та неготовності цивілізованих країн до інформаційної війни у соціальних мережах.

В Україні протидіяти масштабному впливу російських ботоферм та “фабрик тролів” мають, у першу чергу, державні інституції та правоохоронні органи. Насамперед, через створення єдиного центру протидії російської пропаганди у соціальних мережах, який має об’єднати діяльність урядових й громадських організацій. Наступний крок полягає у широкому інформуванні користувачів соціальних мереж щодо інформаційної “гігієни”, роз’ясненні методології виявлення та ідентифікації російських тролів. Також доцільним вбачається створення єдиного обліку ідентифікованих “кремблеботів” та спеціальних програм й додатків, які би допомагали ідентифікувати “тролів” серед користувачів. Активна співпраця з менеджментом самих соціальних мереж у площині протидії “тролям” сприятиме їх швидкому блокуванню. Одним із найважливіших інструментів у боротьбі з протиправною та злочинною діяльністю РФ у соціальних мережах залишається активна контрпропаганда на державному рівні.

За таких умов зростає актуальність питань правового врегулювання змісту деструктивної інформації у текстових інформаційних джерелах. У зв’язку із зростанням обсягів поширення та рівня суспільної небезпеки деструктивного контенту російського походження, виникає нагальна потреба у відповідному правовому регулюванні та розробки ефективних заходів боротьби з ним. На жаль, у вітчизняному законодавсті відсутній систематизований перелік критеріїв, на підставі яких можливо визначити інформаційний деструктивний контент.

Враховуючи вищевикладене, на законодавчому рівні доцільно: визначити чіткі критерії розуміння та тлумачення незаконного (деструктивного) контенту з можливістю їхнього оновлення; створити реєстр за категоріями деструктивного контенту, покращити систему моніторингу соціальних мереж з використанням можливостей систем та алгоритмів штучного інтелекту; розробити єдиний базовий список вимог та правил блокування деструктивного контенту. З метою формування такого переліку (списку) доцільно запровадити у вітчизняне законодавство поняття "деструктивний індикатор" або "індикатор деструктивної спрямованості" – критерій, за яким відбувається пошук наявності у текстовій інформації протиправної семантики, ідентифікація якого є основою для віднесення інформації до класу деструктивної.

Сучасна державна інформаційна політика спрямована, у першу чергу, на організацію та здійснення ефективної протидії поширенню незаконного (деструктивного) контенту. У цьому сегменті важлива роль належить вітчизняній спецслужбі, яка на системній основі проводить моніторинг спеціальними методами і способами вітчизняних та іноземних засобів масової інформації та Інтернету з метою виявлення загроз національній безпеці України в інформаційній сфері, забезпечує протидію проведенню з боку РФ проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації. У цьому контексті важливим та актуальним напрямком боротьби з незаконним (деструктивним) контентом є виявлення та запобігання діяльності "інформаційних" диверсантів, колаборантів, прихильників "руського миру" в Україні, підвищення медіаграмотності пересічених громадян.

Загалом можна констатувати позитивні здобутки діяльності вітчизняної спецслужби за вказаним напрямком, що пов'язано з тим, що російські інформаційні диверсії вже не створюють такої масштабної загрози, як раніше. Такі результати свідчать про те, що Сужба безпеки України діє інноваційно та проактивно – працює на випередження. Саме тому слушними виглядають пропозиції вітчизняної спецслужби щодо посилення відповідальності за поширення незаконного (деструктивного) контенту в мережі Інтернет та соціальних мережах в умовах правового режиму військового стану.

Використана література

1. Гуржій С.В. Сучасні загрозливі тенденції використання Telegram-каналів на шкоду державним інтересам. *Інформація і право.* № 4(39)/2021. С. 162-169

2. Дубов Д.В., Баровська А.В., Каздобіна Ю.К. Деструктивні впливи та негативні наративи: інструменти виявлення та протидії: метод. мат. Київ: УФБС, 2020. 60 с.

3. Калайда Ю.П. Забезпечення цифрового суверенітету в умовах геополітичного протиборства: кращі практики зарубіжного досвіду. *Інформація і право.* № 2(37)/2021. С. 145-154.

4. Митко А.М., Шуляк Н.О. Деструктивні елементи цифрового контенту й інформаційних послуг у ракурсі впровадженні і-демократії. *Вісник Донецького національного університету імені Василя Стуса.* 2017. № 2. С. 72-75.

5. Пивоваров В.В. Деструктивний контент у соціальних мережах як фактор криміногенного впливу на суспільну свідомість. *Право і суспільство.* 2019. № 6. Ч. 2. С. 131- 137.

6. Юшкова А.Г. Загрозливі тенденції використання ботоферм на шкоду державним інтересам України: механізми запобігання та протидії. *Інформація і право.* № 3(38)/2021. С. 90-98.

7. СБУ ліквідувала мільйонну ботоферму, яка розхитувала обстановку в Україні на замовлення однієї з політ сил. URL: https://ssu.gov.ua/novyny/sbu-likviduvala-milionnu-botofermu-yaka-rozkhytuvala-obstanovku-v-ukraini-na-zamovlennia-odniiei-z-politsyl-video

8. Про внесення змін до статі 161 Кримінального кодексу України для реалізації положень Закону України “Про запобігання та протидію антисемітизму в Україні”: Закон України від 19.02.21 р. № 5110.

9. Зеленський закликав ЄС заборонити трансляції російських телеканалів. URL: https://www.rbc.ua/ukr/news/zelenskiy-prizval-es-zapretit-translyatsii-1661957841.html

10. Нацрада і Центр протидії дезінформації разом боротимуться проти пропаганди. URL: https://www.ukrinform.ua/rubric-society/3623484-nacrada-i-centr-protidii-dezinformacii-razom-borotimutsa-proti-propagandi.html

11. Turkey passes controversial bill tightening grip on social media. URL: https://www.aljazeera.com/news/2020/7/29/turkey-passes-controversial-bill-tightening-grip-on-social-media

12. Новий турецький закон про фейки дозволить карати ув’язненням за її поширення. URL: https://netfreedom.org.ua/article/novij-tureckij-zakon-pro-fejki-dozvolit-karati-uvyaznennyam-za-yih-poshirennya

13. Сенат США проголосував за заборону держслужбовцям користуватися TikTok. URL: https://suspilne.media/339194-senat-ssa-progolosuvav-za-zaboronu-derzsluzbovcam-koristuvatisa-tiktok

14. Із початку повномасштабного вторгнення рф кіберфахівці СБУ викрили понад 1200 агітаторів, які поширювали в Інтернеті фейки та російські наративи. URL: https://www.ukrinform.ua/rubric-technology/3642155-sbu-vikrila-pid-cas-vijni-bils-ak-1-200-vorozih-internetagitatoriv.html

15. СБУ викрила під час війни більше 1 тис. ворожих Інтернет-агітаторів, які поширювали фейки про війну в Україні. URL: https://ssu.gov.ua/novyny/sbu-vykryla-pid-chas-viiny-bilshe-1-tys-vorozhykh-internetahitatoriv-yaki-poshyriuvaly-feiky-pro-viinu-v-ukraini-illia-vitiuk

16. Служба безпеки України затримала у Києві організаторів російської “фабрики тролів”. URL: https://ssu.gov.ua/novyny/sbu-zatrymala-u-kyievi-orhanizatoriv-rosiiskoi-fabryky-troliv

17. СБУ просила Telegram заблокувати понад 1,5 тисячі анонімних каналів з дезінформацією. URL: https://ms.detector.media/propaganda-ta-vplivi/post/30628/2022-11-09-sbu-prosyla-telegram-zablokuvaty-ponad-15-tysyachi-anonimnykh-kanaliv-z-dezinformatsiieyu

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~