DOI https://doi.org/10.36059/978-966-397-377-7-65

ІНФОРМАЦІЙНА БЕЗПЕКА ГРОМАДЯН ПІД ЧАС ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ

Шопіна Ірина Миколаївна
доктор юридичних наук, професор,
професор кафедри адміністративно-правових дисциплін
Інституту права Львівського державного
університету внутрішніх справ
м. Львів, Україна

Проблеми забезпечення інформаційної безпеки в Україні набули особливої актуальності ще у 2014 році, із початком російської збройної агресії проти нашої держави. Постійне проведення противником інформаційно-психологічних операцій продовжується і після набуття збройною агресією держави-терориста повномасштабного характеру. Нині ціна помилки в інформаційній сфері є надзвичайно високою – будь-які відомості та дані активно використовуються Російською Федерацією для розвідування позицій підрозділів Збройних Сил України та інших військових формувань, проведення шантажу на основі компрометуючої інформації, здійснення терористичних актів проти цивільного населення та об'єктів критичної інфраструктури.

Широкомасштабна і тривала російська збройна агресія поставила на порядок денний питання щодо необхідності забезпечувати безпеку цивільного населення у різноманітних сферах. У наукових розвідках та моніторингах ситуації як основні звичайно розглядаються фізична, психологічна та економічна безпека, однак все більшу важливість, на нашу думку, у нинішніх умовах набувають питання інформаційної безпеки. Це пов'язано з тим, що ризики у сфері інформаційної безпеки здатні впливати на фізичне, психологічне та матеріальне благополуччя громадян і спричиняти різноманітну шкоду їх життєдіяльності[1].

Поняття інформаційної безпеки може розглядатися на двох рівнях: процесному і статусному. У процесному аспекті поняття інформаційної безпеки слід розуміти як сукупність дій уповноважених органів і самих громадян, спрямованих на убезпечення від існуючих інформаційних ризиків. Зауважимо, процесний аспект включає до свого змісту як активну, так і пасивну складові (прикладом першої може бути виконання уповноваженими органами держави своїх функцій, прикладом другої – утримання громадянином від дій з інформаційними ресурсами, які можуть спричинити йому психологічну або матеріальну школу). У статусному аспекті поняття інформаційної безпеки можна розглядати як стан

[1] Онопрієнко С. Г. (2019). Протидія загрозам національній безпеці в інформаційній сфері: правовий аспект. *Наука і правоохорона,* № 4, С. 399–403.

максимального благополуччя суб’єктів інформаційних відносин, за якого їх права і свободи на безпечне інформаційне середовище реалізовані, а інформаційні ризики не спрямляють значного впливу на їх життя, професійну діяльність і особистісний простір.

Методологія досліджень актуального стану інформаційної безпеки визначених суб’єктів передбачає можливість порівняння окремих характеристик або у динаміці, або порівняно з іншими суб’єктами, які перебувають у відмінних від досліджуваної групи умовах. З огляду на це, інформаційна безпека громадян має визначатися за сукупністю низки параметрів. До них перш за все слід віднести тривалість бойових дій, внаслідок яких підвищуються вразливість частини українських громадян до маніпуляцій з боку противника (наприклад, внаслідок зростання кількості українських військовослужбовців та цивільних осіб, що зникли безвісті, відсутності достовірних відомостей про військовополонених, перебування українських громадян на окупованих територіях, що обумовлює проблеми з доступом до українських інформаційних джерел на фоні активних спроб противника залучити їх до російського інформаційного простору).

Іншим параметром виступає вид дезінформації, вплив якої відчували на собі громадяни. Методологічні підходи до сутності цього явища переважно включають розуміння поняття дезінформації як цілеспрямованого розповсюдження неправдивої інформації, що здійснюється з метою введення суспільства, соціальних груп або окремих суб'єктів в оману. Важливим чинником, який сприяє підвищеній небезпеці дезінформації, є її соціальний характер: будь-які способи розповсюдження неправдивих даних здійснюються за допомогою таких соціальних ресурсів, як засоби медіа, інформаційні агенції, соціальні мережі тощо.

Дослідження, пов'язані з виокремленням структурних елементів дезінформації, включають її поділ декілька видів. До них належать сфабрикований контент, який включає повністю вигадану, неправдиву інформацію. На відміну від нього, фальсифікований контент містить істинну текстову, візуальну або аудиальну інформацію, яка стала предметом схованих змін, що викривлюють її сутність. Контент зі спотвореним джерелом походження передбачає видачу відомостей (як правило, сфабрикованих або сфальсифікованих) за достовірну інформацію з надійних джерел, якими є органи державної влади та місцевого самоврядування, авторитетні засоби медіа тощо. Неправдивий контекст включає істинні відомості та дані у поєднанні з неправдивою контекстною інформацією. Сатира і пародія, як види дезінформації, уявляють собою гумореві тексти, спосіб оприлюднення яких передбачає, що частина аудиторії може прийняти їх за правдиві відомості. Неправдиві зв'язки виникають, коли заголовки, фото та анотації розміщених у мережі інтернет відомостей і повідомлень не пов'язані з текстами, які може прочитати переглядач, натиснувши на посилання. Спонсорський контент як вид дезінформації уявляє собою відомості рекламного характеру, спосіб публікації яких не передбачає позначення відповідних текстів як реклами. Пропаганда – це контент, який

використовується для впливу на суспільство та великі соціальні групи з метою досягнення цілей держави або інших суб'єктів. Помилковий контент уявляє собою випадкове неправдиве повідомлення, здійснене верифікованими суб'єктами: інформаційними агенціями, мас-медіа, представниками органів публічної влади (які звичайно у випадках виявлення таких фактів публікують публічно фіксують це і приносять вибачення своїй авдиторії)[2]. Ступінь інформаційної шкоди, спричиненої жителям деокупованих територій, залежить від видів дезінформації, реципієнтами якої вони були, а також від поєднання декількох з означених видів з метою найбільш деструктивного впливу на структуру особистості.

Третім параметром, який характеризує стан інформаційної безпеки громадян, є мета деструктивної інформаційної діяльності. Наші спостереження дозволили виокремити п’ять основних цілей інформаційних впливів противника: підвищення рівня депресивних настроїв у суспільстві, створення протестної активності, дискредитація органів української влади, дискредитація української культури, знецінювання демократичних надбань західної цивілізації. Визначення можливого досягнення означених цілей потребує здійснення емпіричних досліджень, результати яких мають враховуватися органами публічної влади під час вибору пріоритетів інформаційної політики в умовах правового режиму воєнного стану.

[2] Factsheet 4: Types of Misinformation and Disinformation / Using Social Media in Community Based Protection: a Guide. / UNHCR. URL: https://www.unhcr.org/innovation/wp-content/uploads/2022/02/Factsheet-4.pdf