№76. С. 29-33.
2. Підвальна Ю.В. Соціально-педагогічна адаптація дітей з обмеженими можливостями здоров'я в умовах інклюзивного навчання. *Науковий часопис НПУ імені М. П. Драгоманова. Серія 5. Педагогічні науки: реалії та перспективи.* 2021. №79 (Том 2). С. 48-52.
3. Про затвердження Положення про центр розвитку дитини. Постанова КМУ від 05.10.2009 р. № 1124. URL: https://zakon.rada.gov.ua/laws/show/1124-2009-%D0%BF#Text

Дмитро Плітін
аспірант кафедри соціальної роботи та менеджменту соціокультурної діяльності (ОНП Соціальна робота)
Тернопільський національний педагогічний університет імені Володимира Гнатюка
м. Тернопіль

Наталія Олексюк
доктор педагогічних наук, професор, професор кафедри соціальної роботи та менеджменту соціокультурної діяльності,
Тернопільський національний педагогічний університет імені Володимира Гнатюка
м. Тернопіль

ФОРМИ ТА МЕТОДИ ІНФОРМАЦІЙНОЇ АГРЕСІЇ

У статті розкрито проблему безпеки інформаційного простору. Особливу увагу приділено інформаційним небезпеці, загрозам і ризикам. Виділено джерела інформаційних ризиків, класифіковано види загроз інформаційній безпеці, визначено найпоширеніші механізми, форми та методи інформаційної агресії. Запропоновано інструменти захисту індивідуальної та суспільної свідомості від негативних впливів різноманітних форм і методів інформаційної агресії.

Ключові слова: *інформаційний простір; інформаційна небезпека; інформаційний ризик; інформаційна загроза; інформаційна агресія.*

Однією з актуальних проблем сучасності є функціонування глобального інформаційного простору, який, окрім суттєвих переваг та численних можливостей, створює значні інформаційні небезпеки для суспільства у цілому (глобальні загрози, що мають знеособлений характер) та кожної особи зокрема (зовнішні, конкретно спрямовані, ризики) [2, с.

269]. До джерел інформаційних небезпек, загроз і ризиків відносимо: нерегульоване зростання інформаційних потоків, глобальну комп'ютеризацію, несанкціоновані доступи до комп'ютерних систем, а також вплив інформації на свідомість і психіку людини [1, с. 143].

Інформаційну безпеку визначаємо як стан захищеності суспільства, особи від інформаційних загроз, які можуть завдати шкоди їх існуванню чи функціонуванню [4, с. 412]. Інформаційна безпека ґрунтується на таких ключових принципах: соціальне усвідомлення важливості інформаційної безпеки; достовірність інформації; її цілісність; конфіденційність; доступність; захист персональних даних; захист від інформаційних загроз [5, с. 34].

У зв'язку з інтенсивним розвитком технологій, постійною зміною способів взаємодії та обміну інформацією, поява нових і зростання існуючих інформаційних загроз є постійним явищем. Усі відомі нам загрози інформаційній безпеці класифікуємо за такими критеріями, як: джерело виникнення; рівень небезпеки; спосіб реалізації; ступінь і характер впливу на систему; масштаб, тривалість та термін дії; ступінь навмисності прояву тощо [3, с. 24]. Означена класифікація інформаційних загроз дасть змогу розробити ефективні інструменти для їх запобігання. На основі детального аналізу ряду наукових досліджень, нами виділено такі види загроз інформаційній безпеці: загроза неусвідомлення інформаційних небезпек і ризиків; загроза актуальності інформації, її достовірності, цілісності, конфіденційності, надмірності чи відсутності [1, с. 146].

Використання найсучасніших інформаційних технологій у суспільстві відкриває багато можливостей та допомагає перетворити особу, суспільство на об'єкт маніпулювання. Механізми психологічного впливу ґрунтуються на маніпуляції свідомістю людини, включаючи управління образним сприйняттям дійсності та формування відповідної реакції на інформацію, насамперед переконанні в правдивості. Оскільки основним засобом інформаційного впливу є інформація, то об'єктом його є людська

психіка, психологія групи, суспільства, а суб'єктом – будь яка особа, організація або інституція, що активно поширює інформацію чи спрямовує її на інших з метою впливу [5, с. 35].

До каналів або засобів інформаційної війни можуть відноситися: Інтернет-ресурси (соціальні мережі, сайти, блоги); візуальні і звукові носії (радіо, телебачення, кінотеатр, фільми, пісні, новини, ток-шоу); промови (особисті зустрічі із великою аудиторією, концерти, політичні події); мистецтво (плакати, картини); література і преса (книги, брошури, газети, журнали). У процесі дослідження нами виділено такі найпоширеніші форми інформаційної агресії, як: «інтернет-тролі», «боти», дезінформація (більш широке поняття, ніж популярне fake news); поширення чуток і психологічний тиск; маніпуляція; диверсифікація громадської думки; поширення невизначеностей та створення хаосу; пропаганда; кібератака; інформаційний тероризм; міжсайтовий скриптинг (XXS), пов'язаний із вразливістю вебсайтів; соціально-технічна інженерія; встановлення шкідливого програмного забезпечення без згоди власника тощо [2, с. 269-270].

Важливо, що для кожної форми інформаційного впливу використовуються специфічні методи. Наприклад, у випадку маніпуляції можуть бути використані: метод «гнилого оселедця», коли підбирається неправдиве звинувачення, максимально брудне і скандальне; метод «40 на 60», який полягає в тому, що засоби масової інформації 60% своєї інформації подають в інтересах супротивника, завойовують таким чином його довіру до себе, а решту 40% використовують для надзвичайно ефективної, завдяки цій довірі, дезінформації; метод «великої брехні», коли максимально впевнено подається настільки жахлива брехня, що видається правдою саме тому, що неможливо навіть уявити, як можна брехати про таке; метод «абсолютної очевидності», який полягає не в доведенні думки, а в поданні її як чогось очевидного, само собою зрозумілого, тому підтримуваного більшістю; метод невідомого героя, що

полягає в хибній героїзації особи/групи осіб; метод багаторазового повторення, коли навіювання думки відбувається шляхом її постійного повторення, оскільки «брехня, повторена тисячу разів, стає правдою» [6, с. 34-35].

Для підтримки безпеки інформаційного впливу особі/суспільству необхідно не лише знати форми й методи деструктивного інформаційного впливу на них, але й постійно оновлювати й удосконалювати заходи безпеки. З цією метою нами визначено інструменти захисту індивідуальної свідомості від негативних інформаційних впливів, а саме: здорове середовище; критичне мислення; отримання інформації з різних джерел; інформаційна грамотність; інформаційна культура та гігієна; контроль емоцій [4, с. 415]. До механізмів захисту суспільної свідомості від впливу інформаційної агресії ми відносимо: моніторинг медіа-ресурсів на предмет наявності матеріалів, які містять згубний інформаційний вплив; створення незалежних, професійних, конкурентноздатних українських засобів масової інформації, спрямованих на захист як особистісних, так і національних ідей та інтересів; заохочення громадськості до створення ресурсів з викриття неправдивих інформаційних повідомлень, а також доведення результатів у доступній формі до населення; формування пропозицій до чинного законодавства органам законодавчої та виконавчої влади щодо удосконалення системи інформаційної безпеки країни; адаптація сучасних методик інформаційного протиборства до вітчизняних реалій та надання рекомендацій щодо їх застосування відповідним державним органам; створення державної програми інформаційного протиборства ворогам України [6, с. 208-209].

Таким чином, захист індивідуальної та суспільної свідомості від негативних інформаційних впливів найрізноманітніших форм і методів інформаційної агресії є важливим завданням у сучасному світі. Виходячи з наведеного, можна зробити висновок, що протидія інформаційним небезпекам, загрозам і ризикам є одним із найважливіших напрямів

забезпечення інформаційної безпеки як складової частини національної безпеки держави. Механізми протидії зазначеним загрозам мають бути високотехнологічними та мати системний характер.

Список використаних джерел

1. Валюшко І. О. Основні виклики і загрози в епоху інформаційних війн // *Науковий вісник Дипломатичної академії України. Зовнішня політика і дипломатія: традиції, тренди, досвід. Серія «Політичні науки»* / За заг. ред. В.Г. Ціватого, Н.О. Татаренко. 2016. Випуск 23. Частина ІІ. С. 142–147. URL: http://nbuv.gov.ua/UJRN/Nvdau_2016_23(2)__21.

2. Захаренко К. Стратегія формування ефективної системи державної інформаційної безпеки // *Гілея: науковий вісник*. 2018. Вип. 131. С. 268–272. URL: https://core.ac.uk/download/pdf/144871426.pdf.

3. Морозов О.Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності // *Віче.* 2007. №12. С. 23–25. URL: https://veche.kiev.ua/journal/598/.

4. Плітін Д., Олексюк Н. Інформаційна культура особистості як основа її інформаційної безпеки. *The I International Scientific and Practical Conference «Current methods of improvingoutdated technologi es and methods»*, January 08-10, 2024, Bilbao, Spain. 472 p. Pp. 412–415. URL: http://dspace.tnpu.edu. ua/handle/123456789/31702.

5. Plitin D., Oleksiuk N. The content of personal information security in the conditions of war. *IX International Scientific and Practical Conference «New problems of science and ways of their solution»*, January 02-03, 2024, Paris. France. Pp. 34–36. URL: http://dspace.tnpu.edu.ua/handle/123456789/31699

6. Таркін В. П. Інформаційні війни у сучасному політичному просторі як феномен XX-XXI століття : дис…доктора філос. Національний університет «Одеська юридична академія». Одеса, 2023. 220 с. URI: https://dspace.onua. edu.ua/items/e2fc50ae-9f7b-4b42-9acd-a42286957686.

Анна Попович
доцент, кандидат соціологічних наук,
ДВНЗ «Ужгородський національний університет»
м. Ужгород

ТАРГЕТОВАНА СОЦІАЛЬНА ДОПОМОГА В УМОВАХ СУЧАСНИХ ВИКЛИКІВ

Актуальність публікації пов'язана з тим, що тема таргетованої соціальної допомоги є новою і має значний науковий потенціал у сфері наукових досліджень. Авторка узагальнила фактори, які зумовили