ІНФОРМАЦІЙНА БЕЗПЕКА В КОНТЕКСТІ ПРОТИДІЇ ЧУТКАМ

КРАВЧУК Віталій Леонтійович - викладач кафедри кримінального права та процесу Західноукраїнського національного університету
ORCID: 0009-0001-5906-6245
УДК 342.9
DOI: https://doi.org/10.71404/EP.2024.4.36

У статті зазначено, що інформаційна безпека відіграє важливу роль у національній безпеці України, особливо в контексті сучасних геополітичних викликів і кіберзагроз. Постійні кібератаки та інформаційні війни проти України роблять захист інформаційного простору критично важливим для стабільності та захисту суверенітету держави. Встановлено, що протидія чуткам є важливою складовою інформаційної безпеки та вимагає комплексного підходу. Держава відіграє ключову роль у цьому процесі, впроваджуючи законодавчі механізми, спрямовані на боротьбу з дезінформацією, здійснюючи моніторинг інформаційного простору та оперативно реагуючи на загрози.

Ключові слова: інформаційна безпека, чутки, протидія, органи державної влади, суспільство, журналісти, адміністративне законодавство.

Постановка проблеми

Інформаційна безпека є важливою складовою національної безпеки та стабільності держави. Вона спрямована на захист інформації від деструктивного впливу, зокрема поширення чуток і дезінформації, які можуть призводити до соціальної напруги, економічних криз та політичної нестабільності.

Чутки – це непідтверджена або викривлена інформація, що поширюється в суспільстві і часто використовується для маніпулювання громадською думкою. Вони можуть бути політичними, економічними, соціальними або кризовими. Наприклад, під час політичних виборів чутки можуть впливати на електоральні настрої, а в умовах економічної нестабільності – провокувати паніку на фінансових ринках.

Протидія чуткам є важливою складовою інформаційної безпеки та вимагає комплексного підходу. Держава відіграє ключову роль у цьому процесі, впроваджуючи законодавчі механізми, спрямовані на боротьбу з дезінформацією, здійснюючи моніторинг інформаційного простору та оперативно реагуючи на загрози.

Стан дослідження проблеми

Серед учених, які досліджували окремі аспекти забезпечення інформаційної безпеки, а також питання щодо наявності в цій сфері існуючих проблем і шляхів їх вирішення, загалом, потрібно відзначити: С. Албул, Р. Басенко, П. Біленчук, О. Гринь, В. Гурковський, В. Клочко, А. Лаутар, В. Ліпкан, В. Лук'янова, В. Настюк, В. Рубан, Л. Смола, П. Яковлєв та інших. Разом з тим, на науковому рівні питанням забезпечення інформаційної безпеки, протидія розповсюдженню неправдивої інформації приділялось досить мало уваги.

Метою статті є дослідження й аналіз інформаційної безпеки в контексті протидії чуткам.

Виклад основного матеріалу

Інформаційна безпека відіграє важливу роль у національній безпеці України, особливо в контексті сучасних геополітичних викликів і кіберзагроз. Постійні кібератаки та інформаційні війни проти України роблять захист інформаційного простору критично важливим для стабільності та захисту суверенітету держави. З огляду на розвиток технологій і зростання обсягів даних Україна має постійно вдосконалювати законодавчі та технічні механізми захисту інформації від потенційних та реальних загроз.

До речі, науковець Котерлін І. Б. під словом «загроза» в інформаційній безпеці розуміє, «що будь-хто або будь-що підпадає під небезпеку будь-яких негативних впливів у сфері інформаційної діяльності. Загрози включають в себе впливи, до яких можна віднести хакерство і бездіяльність уповноважених органів щодо виявлення та реакції на загрози; помилки у стратегії політичного курсу щодо системи прийняття законів та їх реалізації; рівень інформаційної культури суспільства та владного істеблішменту; соціально-економічний стан суспільства та держави [1, с. 152]. Відповідно до положень Стратегії інформаційної безпеки «інформаційна загроза – потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні» [2]. Щодо поняття «інформаційна безпека», то, як вважають В. Лук'янова та А. Лаутар, «це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави. Інформаційне середовище – це сфера діяльності учасників інформаційних відносин, пов'язане зі створенням, зміною і споживанням інформації. Дане середовище умовно поділяється на три основні предметні частини: створення і розповсюдження первинної та вторинної інформації; формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг; споживання інформації та дві забезпечувальні предметні частини: створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення, а також забезпечення недоторканості інформації (інформаційної безпеки)» [3, с. 97].

Основні проблеми у сфері забезпечення інформаційної безпеки пов'язані зі застарілими інформаційними системами, які не відповідають сучасним стандартам безпеки, браком кваліфікованих спеціалістів, недостатнім фінансуванням галузі. Також актуальною загрозою для забезпечення життєво важливих інтересів держави є розповсюдження неправдивої інформації, що надалі провокує створення панічних настроїв у суспільстві та сприяє дестабілізації ситуації в Україні. Вирішення цих викликів та посилення інформаційної безпеки можливе завдяки впровадженню комплексних стратегій, що включають інноваційні технологічні рішення, підвищення рівня кіберграмотності населення та удосконалення нормативно-правової бази.

В Україні основні засади інформаційної безпеки базуються на основі Конституції України [4], законів України «Про національну безпеку України»[5], «Про інформацію»[6], «Про медіа»[7] та інших нормативно-правових актів.

Стратегія інформаційної безпеки визначила, що «основними напрямами забезпечення інформаційної безпеки України є стійкість та взаємодія, для досягнення яких необхідним є виконання таких стратегічних цілей та завдань» [2]. Загалом усі стратегічні цілі інформаційної безпеки спрямовані на створення стійкої системи захисту даних, протидію кібератакам, забезпечення конфіденційності, цілісності та доступності інформації. Вони охоплюють як технологічні аспекти (захист мереж, криптографію, контроль доступу), так і соціально-політичні (протидія дезінформації, інформаційним війнам та маніпуляціям).

На основі аналізу стратегічних цілей інформаційної безпеки вважаємо за потрібне виокремити стратегічну ціль 1 «Протидія дезінформації та інформаційним операціям,

насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини» [2].

Досягнення зазначеної цілі здійснюватиметься шляхом виконання таких завдань: «1) створення системи раннього виявлення, прогнозування та запобігання гібридним загрозам, зокрема, створення системи протидії дезінформації та інформаційним операціям, спрямованої на запобігання, максимально швидке виявлення та реагування держави і суспільства на інформаційні загрози; 2) ужиття заходів щодо запобігання та протидії поширенню дезінформації та деструктивної пропаганди стосовно європейської та євроатлантичної інтеграції України; 3) розвиток спроможностей складових сил оборони щодо протидії загрозам в інформаційному просторі; 4) підготовка та проведення складовими сил оборони інформаційно-психологічних операцій та інших заходів, спрямованих на запобігання, стримування та відсіч збройної агресії Російської Федерації проти України; 4) посилення відповідальності за поширення недостовірної інформації (дезінформації); 5) запровадження дієвих механізмів виявлення, фіксації, обмеження доступу та/або видалення з українського сегмента мережі Інтернет інформації, розміщення якої обмежено або заборонено законом; 6) ефективна взаємодія державних органів, органів місцевого самоврядування та інститутів громадянського суспільства при формуванні та реалізації державної політики в інформаційній сфері; 7) унеможливлення розповсюдження та демонстрації інформаційних та аудіовізуальних продуктів (продукції), проведення гастрольних заходів, що популяризують або пропагують державу-агресора та її органи влади, представників органів влади держави-агресора та їхні дії, що створюють позитивний образ держави-агресора, виправдовують чи визнають правомірною окупацію території України, містять заклики до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, екстремізму, сепаратизму, комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів та їхньої символіки, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі і ненависті, вчинення терористичних актів, посягання на права та свободи людини і громадянина тощо; 8) протидія інформаційним кампаніям, спрямованим на залучення та/або втягування громадян України, у тому числі дітей, до не передбачених законами України воєнізованих чи збройних формувань» [2].

Отже, можна підсумувати, що ефективна реалізація як стратегічної цілі 1, так і інших цілей, визначених у Стратегії інформаційної безпеки, дозволяє не лише запобігати загрозам, але й створювати сприятливі умови для розвитку суспільства, економіки та державного управління, забезпечуючи довіру до інформаційних систем і комунікацій.

У цьому питанні також варто зазначити, що протидія чуткам є важливою складовою діяльності Президента України, органів державної влади, органів місцевого самоврядування, правоохоронних органів. Але, окрім вищезазначених суб'єктів, ключову роль відіграють журналісти. Адже саме вони доносять до суспільства важливу інформацію про події, що відбуваються в країні та світі. Одним із головних принципів журналістики є об'єктивність і достовірність, оскільки громадяни покладаються на медіа для отримання правдивої інформації. Завдяки професійному аналізу, незалежності та дотриманню етичних норм вони забезпечують суспільству доступ до правди. Важливо, щоб журналістика залишалася поза впливом політичних чи комерційних інтересів, оскільки це може призвести до викривлення реальності.

Окрім цього, журналісти виконують роль своєрідної «четвертої гілки влади», викриваючи корупцію, зловживання владою та порушення прав людини. Вони можуть

впливати на громадську думку, привертаючи увагу до соціально важливих проблем. Наприклад, розслідувальна журналістика нерідко стає рушійною силою суспільних змін.

Особливу увагу до ЗМІ та діяльності журналістів в умовах воєнного стану привернули такі науковці, як Залєвська І. І., Удренас Г. І. На їх думку, «правда є головним інструментом боротьби з ворожими фейками. Цю правду добувають і несуть у маси журналісти. Мужність українських журналістів, які висвітлюють хід війни, ризикуючи своїм життям, зазначив керівник відділу ЮНЕСКО зі свободи вираження поглядів та безпеки журналістів Гільєрмо Канела на зустрічі у Центрі журналістської солідарності НСЖУ у Львові: «Вражає, наскільки українські журналісти віддані своїй справі, незважаючи на те, що їх спіткало. Ми підтримуємо вас у цій солідарності і хочемо зрозуміти, що можемо зробити для вас, щоб ви продовжували роботу» [8, с. 23].

З появою цифрових технологій та соціальних мереж відповідальність журналістів тільки зросла. Фейки та маніпуляції поширюються дуже швидко, тому професіонали медіасфери мають особливо уважно перевіряти джерела інформації. Звідси можна зробити висновок про те, що важливим фактором у боротьбі з чутками є відповідальна діяльність засобів масової інформації. Відповідно медіа, які поширюють недостовірну інформацію, лише можуть посилювати загрозу інформаційній безпеці.

Не менш важливу роль у забезпеченні інформаційної безпеки відіграє громадянське суспільство. Громадські організації, ініціативи та освітні проєкти сприяють підвищенню рівня медіаграмотності населення. Чим більше людей здатні критично оцінювати отриману інформацію, тим менше шансів у дезінформаційних кампаній досягти своєї мети.

Сучасні технології також відіграють значну роль у забезпеченні інформаційної безпеки. Використання штучного інтелекту та алгоритмів аналізу великих даних допомагає ідентифікувати джерела чуток, прогнозувати їхній вплив і розробляти ефективні стратегії протидії.

Висновки

Інформаційна безпека є ключовим елементом національної безпеки кожної держави. У сучасному світі, де інформація стала стратегічним ресурсом, важливе значення має її захист від несанкціонованого доступу, маніпуляцій, кіберзагроз та інших небезпек. Для цього Україна розробила нормативно-правову базу, яка регулює питання інформаційної безпеки та забезпечує правовий механізм її підтримки.

Нормативно-правове забезпечення інформаційної безпеки охоплює законодавчі акти, міжнародні угоди, концепції, стратегії та рекомендації щодо захисту інформації. Основними завданнями такої правової системи є гарантування конфіденційності, цілісності та доступності даних, регулювання діяльності суб'єктів інформаційної сфери, а також встановлення відповідальності за порушення інформаційних прав і кіберзлочини.

Таким чином, інформаційна безпека є важливим елементом захисту суспільства від чуток та маніпуляцій. Її забезпечення потребує безпосередньої взаємодії держави, медіа, громадськості та ефективних рішень. Комплексний підхід до цієї проблеми сприяє формуванню стійкого до дезінформації суспільства, що є необхідною умовою стабільності та розвитку держави.

Література

1. Котерлін І. Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. *Актуальні проблеми вітчизняної юриспруденції*. 2022. № 1. С. 150-155.

2. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України; Стратегія від 28.12.2021 р. № 685/2021. URL: https:// zakon.rada.gov. ua/laws/ show/ 685/2021#n14.

3. Лук'янова В. В., Лаутар А. Ю. Інформаційна безпека в умовах розвитку інформаційної системи. *Вісник Хмельницького національного університету*. 2017. № 2. Т. 3. С. 97-101.

4. Конституція України від 28.06.1996 р. № 254к/96-ВР. URL: https:// zakon. rada.gov. ua.

5. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

6. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

7. Про медіа: Закон України від 13.12.2022 р. № 2849-IX. URL: https:// zakon.rada.gov.ua/laws/show/2849-20#Text.

8. Залєвська І. І., Удренас Г. І. Інформаційна безпека України в умовах російської військової агресії. *Південноукраїнський правничий часопис*. 2022. № 1-2. С. 20-26.

Kravchuk V.

INFORMATION SECURITY IN THE CONTEXT OF COUNTERING RUMOURS

The study found that information security is an important component of national security and stability of the state. It is aimed at protecting information from destructive influences, in particular, the spread of rumours and disinformation, which can lead to social tension, economic crises and political instability. It is stated that rumours are unconfirmed or distorted information that is spread in society and is often used to manipulate public opinion. They can be political, economic, social or crisis-related. For example, during political elections, rumours can influence electoral sentiment, and in times of economic instability, they can provoke panic in financial markets. Particular attention is drawn to the fact that countering rumours is an important component of information security and requires a comprehensive approach. The state plays a key role in this process by implementing legislative mechanisms aimed at combating disinformation, monitoring the information space and responding promptly to threats. At the same time, it is noted that an important factor in the fight against rumours is the responsible activity of the media. Journalists should verify the accuracy of information, promptly refute fakes and adhere to professional ethics standards. At the same time, media outlets that disseminate false information may increase the threat to information security. It is emphasised that modern technologies also play a significant role in ensuring information security. The use of artificial intelligence and big data analysis algorithms helps to identify sources of rumours, predict their impact and develop effective countermeasures. The author concludes that ensuring information security requires interaction between the State, the media, the public and technological solutions. An integrated approach to this problem contributes to the formation of a society resistant to disinformation, which is a prerequisite for the stability and development of the state.

Key words: *information security, rumours, counteraction, public authorities, society, journalists, administrative law.*