РОЗДІЛ 8. КРИМІНАЛЬНЕ ПРАВО ТА КРИМІНОЛОГІЯ; КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО

УДК 343.2/.7(477)
DOI https://doi.org/10.24144/2307-3322.2023.77.2.23

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ОБ'ЄКТ ПОСЯГАННЯ ЗЛОЧИНІВ ПРОТИ ОСНОВ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Аніщук В.В.,
кандидат юридичних наук, доцент кафедри права,
факультету бізнесу та права
Луцького національного технічного університету
https://orcid.org/0000-0002-9854-4932
viktoriya.anishchuk@ukr.net

Аніщук В.В. Інформаційна безпека як об'єкт посягання злочинів проти основ національної безпеки України.

Стаття присвячена дослідженню інформаційної безпеки як складової національної безпеки України. Стрімкий розвиток цифровізації в Україні, який ми спостерігаємо в останні роки, спровокував створення новітнього інформаційного суспільства і, як наслідок – виникнення таких явищ як «кіберзагрози» та «кібератаки» у банківській, воєнній, критичній інфраструктурі тощо. У зв'язку з цим до національної безпеки держави цілком виправдано відносять інформаційну безпеку як самостійний елемент національної безпеки. Нове звучання інформаційна безпека набула через повномасштабне вторгнення Російської Федерації в Україну. Держава-агресор проводить жорстокі підступні військові дії не лише на території нашої держави, але й в інформаційному просторі. Спеціальні інформаційні операції Російської Федерації спрямовуються на ключові демократичні інституції (зокрема, виборчі), а спеціальні служби держави-агресора намагаються посилити внутрішні протиріччя в Україні та інших демократичних державах. Застосовані Російською Федерацією технології гібридної війни проти України, у тому числі моделі і механізми інформаційного втручання, поширюються на інші держави, швидко адаптуючись до локальних контекстів та регуляторних політик. Необхідність гарантування інформаційної безпеки зумовлюється, по-перше, потребою забезпечення національної безпеки України в цілому, по-друге, існуванням таких загроз інформаційній сфері країни, які можуть завдавати значної шкоди загальним національним інтересам, по-третє, врахуванням того, що за допомогою інформації можна впливати на зміну свідомості і поведінку людей. Завдання інформаційної безпеки – створення системи протидії інформаційним загрозам та захист власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави. Державна політика щодо забезпечення інформаційної безпеки є важливою складовою національної безпеки. В її основі повинна бути системна превентивна діяльність органів державного управління щодо надання гарантій інформаційної безпеки особистості, соціальним групам, суспільству і державі в цілому. Дослідження інформаційної безпеки як об'єкта злочинів проти основ національної безпеки України в умовах війни є важливим та вкрай актуальним.

Ключові слова: інформаційна безпека, національна безпека, цифровізація, об'єкт злочину, інформаційний простір, кібербезпека.

Anishchuk V. **Information security as an object of crimes against the foundations of national security of Ukraine.**

The article is devoted to the study of information security as a component of the national security of Ukraine. The rapid development of digitalization in Ukraine, which we have observed in recent years, has provoked the creation of the newest information society and, as a result, the emergence of such phenomena

as «cyber threats» and «cyber attacks» in banking, military, critical infrastructure, etc. In this regard, the state quite justifiably refers to information security as an independent element of national security. Information security acquired a new sound due to the full-scale invasion of the Russian Federation into Ukraine. The aggressor state carries out brutal insidious military actions not only on the territory of our state, but also in the information space. Special information operations of the Russian Federation are aimed at key democratic institutions (in particular, electoral ones), and special services of the aggressor state are trying to intensify internal contradictions in Ukraine and other democratic states. The technologies of the hybrid war against Ukraine, including the models and mechanisms of information intervention, applied by the Russian Federation are spreading to other states, quickly adapting to local contexts and regulatory policies. The need to guarantee information security is determined, firstly, by the need to ensure the national security of Ukraine as a whole, secondly, by the existence of such threats to the information sphere of the country that can cause significant damage to general national interests, and thirdly, by taking into account the fact that with the help of information it is possible influence a change in people's consciousness and behavior. The task of information security is the creation of a system for countering information threats and the protection of one's own information space, information infrastructure, and information resources of the state. State policy on ensuring information security is an important component of national security. It should be based on the systematic preventive activity of state administration bodies regarding the provision of information security guarantees to individuals, social groups, society and the state as a whole. The study of information security as an object of crimes against the foundations of the national security of Ukraine in the conditions of war is important and extremely relevant.

Key words: information security, national security, digitalization, object of crime, information space, cyber security.

Постановка проблеми. Суспільний розвиток неминуче супроводжується розвитком політичної, економічної, соціальної і культурної сфер життя держави. Стрімкий розвиток торкнувся також і такої передової сфери, як цифрова, зокрема глобалізація інформаційного та комунікаційного простору, тотальна комп'ютеризація, сукупність результатів семантичної діяльності людства, які сформували принципово нові явища – інформаційне суспільство та кіберпростір. Правомірне та доцільне застосування інформації особливо сьогодні відіграє надзвичайно важливе місце у рамках забезпечення глобальної безпеки людства.

Після створення у вересні 2019 року Міністерства цифрової трансформації України у нашій державі розпочався новий етап у сфері глобальної цифровізації. Сьогодні ми можемо констатувати реальне запровадження і швидкий розвиток цифровізації у всіх сферах життя суспільства України. Безперечно, саме такий швидкий розвиток стимулював створення новітнього інформаційного суспільства і, як наслідок, це спонукало до виникнення таких явищ як «кіберзагрози» та «кібератаки» у банківській, воєнній, критичній інфраструктурі тощо. Виходячи з наведеного, сучасні дослідники до національної безпеки держави цілком виправдано відносять інформаційну безпеку як самостійний елемент національної безпеки [2].

Стан опрацювання цієї проблематики. Цій проблемі були присвячені роботи таких вчених, як М. Барнетте, Р. Башроушу, О. Когут, Д. Пушман, І. Сопілко, А. Сулайман, В. Фурашева Д. Шац та інших.

Метою статті є критичний аналіз особливостей інформаційної безпеки як об'єкта посягання злочинів проти основ національної безпеки України.

Виклад основного матеріалу. Закон України «Про основи національної безпеки» стосовно загроз національній безпеці визначає, що на сучасному етапі найбільш важливими потенційними та реальними ризиками стабільності в суспільстві та національній безпеці України в інформаційній сфері є:

1) розголошення конфіденційної інформації, що є власністю держави та спрямована на забезпечення національних інтересів та потреб держави та суспільства;

2) прояви обмеження доступу громадян до інформації та свободи слова;

3) поширення через засоби масової інформації культу та ідеології насильства, жорстокості тощо;

4) комп'ютерна злочинність та комп'ютерний тероризм;

5) розголошення інформації, що становить як державну, так і іншу таємницю, що передбачена Законом;

6) намагання маніпулювання суспільною свідомістю, зокрема, шляхом поширення упередженої, неповної чи недостовірної інформації [4].

Інформаційний суверенітет та інформаційна безпека України гарантується і забезпечується безпосередньо на законодавчому рівні.

Нове звучання інформаційна безпека набула через повномасштабне вторгнення Російської Федерації в Україну. Держава-агресор проводить жорстокі підступні військові дії не лише на території нашої держави, але й в інформаційному просторі. Відповідно до Указу Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»» було встановлено, що «інформаційна політика Російської Федерації – загроза не лише для України, але й для інших демократичних держав. Спеціальні інформаційні операції Російської Федерації спрямовуються на ключові демократичні інституції (зокрема, виборчі), а спеціальні служби держави-агресора намагаються посилити внутрішні протиріччя в Україні та інших демократичних державах. Застосовані Російською Федерацією технології гібридної війни проти України, у тому числі моделі і механізми інформаційного втручання, поширюються на інші держави, швидко адаптуючись до локальних контекстів та регуляторних політик. Обмежувальні заходи (санкції) та ефективний механізм моніторингу і відповідальності за їх порушення є одним із дієвих механізмів відповіді на дезінформаційну активність Російської Федерації як держави-агресора [5].

Крім того, тривалий час спеціальні служби Російської Федерації проводять свої спеціальні інформаційні операції, більшість із яких спрямовані на підрив національної безпеки України, її національних інтересів, ліквідацію української державності та знищення української ідентичності, провокування проявів екстремізму, панічних настроїв у суспільстві, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації в Україні. Російською Федерацією використовуються нові активні заходи, у тому числі міжнародного характеру, щодо легітимізації спроби анексії Автономної Республіки Крим та міста Севастополя, заперечення своєї участі у війні на території Донецької та Луганської областей та посилення адвокаційної кампанії за зняття санкцій, запроваджених у зв'язку з порушенням Російською Федерацією суверенітету і територіальної цілісності України. Задіяння у цьому процесі Російською Федерацією всіх її спроможностей (політичних, інформаційних, економічних, розвідувальних та інших) залишається особливо небезпечним викликом для України.

У результаті тимчасової окупації у 2014 році державою-агресором частини території України були захоплені розташовані на цій території об'єкти інформаційної інфраструктури, зокрема й об'єкти Концерну радіомовлення, радіозв'язку та телебачення.

Державою-агресором застосовуються методи тотального придушення свободи слова, контролю над редакційною політикою засобів масової інформації та інших інформаційних ресурсів, що функціонують на цих територіях.

На тимчасово окупованих територіях, у районах здійснення заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації у Донецькій та Луганській областях розгорнуто безпрецедентну інформаційну кампанію. Використовуючи також регулярне постачання на тимчасово окуповані території потужного передавального обладнання та блокування українських інформаційних ресурсів, Російська Федерація намагається створити альтернативну викривлену інформаційну реальність, побудовану на наративах держави-агресора.

Придушення будь-яких спроб інакомислення посилюється регулярними репресіями стосовно незалежних журналістів на тимчасово окупованій території Автономної Республіки Крим та міста Севастополя, а також переслідуванням за перегляд українського контенту, що є характерним для тимчасово окупованих територій Донецької та Луганської областей.

Інформаційний тиск, що здійснюється державою-агресором, негативно відображається й на дітях, які проживають на тимчасово окупованих територіях, адже через свій вік вони є особливо вразливими для впливу інформаційних кампаній.

В Україні триває процес становлення системи стратегічних комунікацій. Органами державної влади України здійснено низку організаційних та практичних заходів зі зміцнення власної інституційної спроможності у сфері стратегічних комунікацій, однак не створено дієвого механізму координації і взаємодії між усіма органами державної влади, залученими до здійснення заходів із протидії загрозам в інформаційній сфері. Зазначене послаблює можливості до розбудови комплексного стратегічного планування інформаційного потоку, здійснення системної комунікативної діяльності Кабінету Міністрів України, об'єднання всіх ключових суб'єктів у сфері інформаційних відносин, суб'єктів формування і реалізації державної політики щодо ефективного захисту національного інформаційного простору, утвердження позитивного іміджу України, реалізації цілей захисту національної безпеки України в інформаційній сфері.

Регулювання відносин у сфері інформаційної діяльності не відповідає сучасним викликам та загрозам. Це перешкоджає розвитку українського медіаринку, ускладнює ведення бізнесу у цій сфері, зберігає залежність засобів масової інформації від їх власників, не забезпечує додержання професійних стандартів діяльності журналістів.

Актуальною проблемою є непоодинокі випадки втручання в професійну організаційно-творчу діяльність засобів масової інформації та в індивідуальну професійну творчу діяльність журналістів, інші посягання на свободу інформаційної діяльності, зокрема перешкоджання їх професійній діяльності, погрози, насильство щодо них, посягання на їх життя та власність. Зазначене позбавляє журналістів можливості належним чином інформувати суспільство про суспільно важливі події та явища.

У нашій державі склалася унікальна та неоднозначна ситуація, коли проплачені російські ЗМІ проштовхують абсолютно недемократичні принципи розвитку нашої держави, формуючи, таким чином відповідну думку лояльних до держави-агресора громадян України, що завдає значної шкоди інтересам нашої держави у продовженні її демократичного розвитку. З огляду на зазначені обставини, можна зауважити, що вище згаданий указ є необхідним для захисту національних інтересів України і спрямований саме на зупинення розповсюдження російської пропаганди у нашій державі. Тому усі закиди щодо обмеження свободи діяльності ЗМІ на території України є недоцільними та такими, що не відповідають дійсності.

До того ж, цілком можна погодитись із твердженням, що в умовах війни на Сході РФ активно розпочала упереджене та викривлене висвітлення фактів та явищ не лише для свого населення, але й безпосередньо для всього світу, що в результаті призвело до антиукраїнського руху. Такі дії сприяли пропаганді ідей сепаратизму, насильства, національної ворожнечі суспільства, яскравим прикладом якого є самопроголошені утворення так званих ДНР та ЛНР на території унітарної України.

Слід зазначити, що засоби масової інформації вже давно на практиці визнаються четвертою гілкою влади, яка має безперечно вагомий вплив на засоби масової комунікації та може здійснювати маніпуляції з суспільною думкою. Сьогодні преса робить те, що століття тому робили священики та церква. Телебачення, газети, радіо, інформаційні агенції грають першу скрипку у ментальній ідеологічній сфері [6]. Громадяни довіряють ЗМІ більше, ніж державі, про що свідчать настрої населення Східної частини України, на яких поширювалася вся пропагандистська інформація Російської Федерації.

Можна цілком погодитися із позицією французького філософа Жана Бодріяр, який зауважував: «Про що мріють засоби масової інформації, як не про те, щоб викликати подію однією лише своєю присутністю?» Якщо йдеться про будь-яке повідомлення, що буде повторюватись достатню кількість разів, воно буде сприйматися як істина. «… Через повторення ідея закріплюється в умах так міцно, що у кінцевому підсумку вона вже сприймається як істина.» Ця технологія покладена, зокрема, в основу формування цілих держав. Тому тепер не обов'язково бути розвиненою країною - достатньо впевнити всіх у тому, що вона такою є [6].

Необхідність гарантування інформаційної безпеки зумовлюється, по-перше, потребою забезпечення національної безпеки України в цілому, по-друге, існуванням таких загроз інформаційній сфері країни, які можуть завдавати значної шкоди загальним національним інтересам, по-третє, врахуванням того, що за допомогою інформації можна впливати на зміну свідомості і поведінку людей. Завдання інформаційної безпеки – створення системи протидії інформаційним загрозам та захист власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави. При виникненні криз, загострені конфліктів інформаційна боротьба може перерости в інформаційну війну, яка здійснюється за допомогою інформаційної зброї. Показниками, виступають цілеспрямованість, масштабність та комплексність дій тощо [1].

Висновки. Отже, державна політика щодо забезпечення інформаційної безпеки є важливою складовою національної безпеки. В її основі повинна бути системна превентивна діяльність органів державного управління щодо надання гарантій інформаційної безпеки особистості, соціальним групам, суспільству і державі в цілому. Аналіз свідчить про існування реальних загроз інформаційній безпеці України [3, с. 158]. Поряд з цим, проблема інформаційної безпеки держави є досить складною і багатогранною і тому її слід розглядати лише у взаємозв'язку з іншими проблемами, які мають більш високий або такий же порядок важливості. Перш за все, до таких проблем відноситься проблема національної безпеки.

Насамкінець необхідно зазначити, що інформаційна безпека, в умовах триваючої війни РФ проти України, є надзвичайно важливим механізмом захищеності всіх сфер життя та інтересів як людини, так і держави. Можна визначити, що інформаційна безпека працює задля запобігання можливого на-

несення шкоди шляхом упередженого інформування населення, яка у наслідку призводить до неправдивого та незаконного висвітлення інформації, її розповсюдження, використання та поширення.

Список використаних джерел:

1. Бондаренко, В.О. Інформаційна безпека сучасної держави: концептуальні роздуми URL: http://www.crime-research.iatp.org.ua/library/strateg.htm (дата звернення: 20.04.2023).
2. Войціховський А.В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Право».* Випуск 29, 2020.
3. Данільян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України: структура та напрямки реалізації: навч. посіб. Х.: Фоліо, 2002. 285 с.
4. Про основи національної безпеки України: Закон України. Офіційний Вісник України. 2003. № 29. Ст. 1433.
5. Про рішення ради національної безпеки і оборони України від 15 жовтня 2021 року «Про стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2022 року № 685/2021 / Президент України. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n33 (дата звернення: 20.04.2023).
6. Торяник В.М. Інформаційна безпека як складова національної безпеки держави. Роль ЗМІ в забезпечення інформаційного суверенітету України. *Право і Суспільство.* 2016. № 2. С. 151–156. URL: http://www.pravoisuspilstvo.org.ua/archive/2016/2_2016/part_1/28.pdf (дата звернення: 20.04.2022).