УДК 65.012.8:007+32(477)
DOI https://doi.org/10.32841/2307-1745.2023.64.4

Недохлєбов І. І.,
здобувач кафедри конституційного та адміністративного права
Запорізького національного університету

ТЕОРЕТИКО-ПРАВОВИЙ АНАЛІЗ ЗОВНІШНІХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ

Анотація. У статті здійснено комплексний теоретико-правовий аналіз зовнішніх загроз інформаційній безпеці України. Автор обґрунтовує доцільність розгляду загроз інформаційній безпеці держави через призму характеру їхнього виникнення (внутрішні та зовнішні). Запропоновано розглядати зовнішні загрози інформаційній безпеці як сукупність явищ, чинників та подій, які виникають і формуються на міжнародному рівні, а реалізуються – на внутрішньодержавному, пов'язані з негативним зовнішнім впливом на інформаційну систему та загрожують національним інтересам в сфері інформаційної діяльності. Автор доходить висновку, що сфера інформаційної діяльності є достатньо вразливою та постійно стикається з різними зовнішніми загрозами, які негативно, впливають на стан захищеності інтересів держави, суспільства та особистості. Аргументовано, що зовнішні загрози пов'язані з деструктивним впливом, наслідками якого є втрата відомостей, порушення чи обмеження права на інформацію, формування викривленого уявлення про події та процеси, які відбуваються в державі, порушення цілісності інформації у відповідних національних та глобальних інформаційних системах. Доведено, що природа зовнішніх загроз пов'язана з неправомірними діями суб'єктів, які спрямовані на досягнення такого результату, який суперечить національним інтересам в інформаційній сфері. Автор звертає увагу на те, що зовнішні загрози перебувають в площині окремих видів інформаційної діяльності (одержання, використання, поширення та зберігання інформації). Встановлено, що зовнішні загрози пов'язані з процесом задоволення інформаційних потреб, адже негативно впливають на нього шляхом неправомірних обмежень або використання наративів, які формують у суспільстві деструктивні настрої. З'ясовано, що стан інформаційної безпеки залежить, у тому числі, від ефективної системи попередження зовнішніх загроз.

Ключові слова: інформаційна безпека, інформаційна діяльність, інформаційні потреби, зовнішні загрози, національні інтереси, національна безпека, протидія та попередження, правове регулювання.

Постановка проблеми. В умовах тотальної інформатизації суспільства та зовнішньої агресії з боку РФ, актуальним питанням є попередження зовнішніх загроз інформаційній безпеці України. На даний час в державі відсутні комплексні наукові праці з цієї проблематики. Це значно знижує ефективність правового регулювання відповідної сфери. Розуміння природи та змісту зовнішніх загроз дасть змогу розробити систему заходів протидії негативним впливам на національну інформаційну систему. Тому, аналіз зовнішніх загроз інформаційній безпеці України може вважатися актуальним напрямом наукового пошуку.

Аналіз останніх досліджень і публікацій. Проблеми забезпечення інформаційної безпеки в різні часи досліджували: Ю. Я. Андрусишин, В. В. Бараннік, Є. М. Білоусов, В. М. Брижко, О. О. Золотар, І. А. Коваленко, Н. В. Лесько, А. В. Логінов, Б. Д. Леонов, С. Я. Лихова, В. Г. Міхайличенко, В. О. Ніколаєва, Т. С. Перун, І. В. Трубін, В. О. Тімашов, В. В. Шемчук, І. В. Яковюк та інші вчені. Однак, з урахуванням динамічних змін в інформаційній сфері та появи нових викликів, їхні праці частково втратили актуальність.

Метою статті є дослідження правової природи та сутності зовнішніх загроз інформаційній безпеці України.

Виклад основного матеріалу. У своїх працях науковці досліджують загрози інформаційної безпеки переважно через особливості самої інформації. Зокрема, О. О. Золотар та І. О. Трубін пропонують усі загрози об'єднати в рамках наступних груп: 1) загрози впливу неякісної інформації (недостовірної, дезінформації) на особистість, суспільство, державу; 2) загрози несанкціонованого й неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (їх виробництво, системи формування й використання); 3) загрози інформаційним правам і свободам особистості [1, с. 109]. В свою чергу А. В. Логінов пропонує поділяти загрози інформаційній безпеці на наступні три групи: розкриття інформаційних ресурсів; порушення цілісності інформаційних ресурсів; збій або втручання в роботу інформаційних систем та обладнання [2, с. 61].

В. В. Шемчук зазначає, що загрози інформаційній безпеці України розглядаються як детермінуючі фактори, що зумовлюють і породжують негативні явища, які посягають на національні інтереси в інформаційній сфері, організацію та функціонування національного інформаційного простору загалом. Вони мають або можуть мати широкомасштабне значення, пов'язані із ризиками і небезпеками в інших сферах [3, с. 293]. Тобто, науковець також виходить з особливостей інформації, але пропонує враховувати характер впливу на неї, зокрема масштабність загроз. На нашу думку, подібний підхід дещо звужує перелік загроз та не дозволяє більш детально розкрити їхню природу та алгоритми негативного впливу. Саме тому, ми пропонуємо виходити з поділу загроз на внутрішні та зовнішні, з урахуваннях інших їхніх ознак.

Аналіз наукових джерел доводить, що поняття «зовнішні» загрози не уніфіковано навіть на рівні системи національної безпеки. Тобто, окремі науковці формують власні дефініції, які корелюються зі сферою їхнього наукового пошуку. У зв'язку з цим, пропонуємо під зовнішніми загрозами інформаційній безпеці розглядати сукупність явищ, чинників та подій, які виникають і формуються на міжнародному рівні, а реалізуються – на внутрішньодержавному, пов'язані з негативним зовнішнім впливом на інформаційну систему та загрожують національним інтересам в сфері інформаційної діяльності.

Надалі пропонуємо окремо проаналізувати найбільш актуальні зовнішні загрози інформаційній безпеці держави.

1. Інформаційний тероризм з боку держави-агресора.

І. В. Яковюк, Є. М. Білоусов зазначають, що агресія РФ стосовно України – це не просто регіональна війна з глобальними наслідками, вона також передбачає оформлення нових ліній протистояння. Так, наступною «мішенню» російської агресії можуть стати Молдова, Грузія, країни Центральної Азії і навіть країни Балтії, хоча вони і є членами НАТО. У цьому випадку російська агресія, ймовірно, почнеться повільно, у неконвенційній манері, тобто з кібератак, політичного втручання за допомогою інформаційних операцій, розпалення невпевненості і страху – ідеального живильного середовище для популізму, який, за задумом держави-агресора, зруйнує ліберальну демократію зсередини, і спроб розпалити громадянські війни в цих країнах [4, с. 11].

Ця теза доволі комплексно розкриває природу інформаційного тероризму з боку РФ, яка має політико-правове підгрунтя та втілена у зовнішній політиці держави-агресора. Означена загроза має високий рівень суспільної небезпеки та негативно впливає на стан захищеності національних інтересів в інформаційній сфері. З приводу цієї загрози Б. Д. Леонов та С. Я. Лихова зазначають, що інформаційний тероризм є формою деструктивного впливу, спрямованого на маніпуляцію чи залякування населення або заподіяння з використанням інформаційних технологій шкоди суспільству, державі чи окремим особам з метою примусити органи державної влади, міжнародну організацію, юридичну чи фізичну особу вчинити якусь дію. Традиційно, залежно від спрямованості, можна виділити два види інформаційного тероризму: 1) психологічний (пропаганда тероризму, створення атмосфери страху і паніки в суспільстві); 2) технічний (контролювання або блокування каналів передачі інформації, порушення функціонування об'єктів інформаційної інфраструктури) [5, с. 174].

Слід припустити, що ця загроза актуальна для різних рівнів інформаційної безпеки (держава, суспільство, особистість). При чому є певна особливість, яку визначають Ю. Я. Андрусишин та В. В. Бараннік. Науковці стверджують, що небезпека інформаційного тероризму полягає насамперед у відсутності географічних і національних меж, адже терористичні дії можуть вчинятися з будь-якої точки світу, а також у складності ідентифікації особи терориста в інформаційному просторі та встановлення місця його перебування, адже кібер- і медіаатаки хакери здійснюють опосередковано через використання комп'ютерної техніки [6, с. 12].

2. Неконтрольованість контенту в глобальних інформаційних мережах.

Означена загроза безпосередньо пов'язана з проблемою захисту інформації в мережі Інтернет. На думку Н. В. Лесько та М. Р. Малець, характерною ознакою мережі Інтернет є те, що географічні кордони не відіграють ніякої ролі. Саме тому, забезпечити ефективне правове регулювання мережі Інтернет досить складно, адже відсутнє систематизоване законодавство, що регулює відповідні види відносин у всесвітній мережі, окрім того, існують об'єктивні особливості функціонування Інтернету. Тому, з проблемою забезпечення законності в мережі Інтернет тісно пов'язана проблема державного контролю за процесами, що відбуваються в цій мережі [7, с. 189].

Отже, існування досліджуваної загрози є об'єктивним та обумовлене технічними особливостями побудови глобальних інформаційних мереж. Це дозволяє майже безперешкодно поширювати будь-яку інформацію, у тому числі ті відомості, які негативно впливають на суспільство та особистість. І. А. Коваленко зазначає, що проблема захисту авторського та суміжних прав в Інтернеті у наш час стає дедалі актуальною, оскільки досі не вироблено однозначної та єдиної для всіх держав позиції. Інтернет як глобальна комп'ютерна мережа складається з менших мереж, і є відносно новим засобом комунікації. Законодавство просто не встигає за стрімким рухом нових технологій, тому окремі задачі так і залишаються не вирішеними [8, с. 54]. Ця теза вказує на інституційні зв'язки між різними рівнями інформаційної безпеки, оскільки негативний вплив на особистість, неминуче призведе до більш глобальних наслідків на рівні суспільства і держави.

Ще одним аспектом прояву цієї загрози, є небезпека соціальних мереж. З цього приводу В. М. Брижко зазначає, що існує три основні групи ризиків у соціальних мережах при використання персональних даних: повна інформація про особу; повідомлення персональних даних злочинцям; відсутність у користувача реального контролю над персональними даними. Тому, глобальні соціальні мережі та Інтернет є потенційною загрозою для багатьох користувачів, які наражають свої персональні дані на небезпеку [9, с. 31].

3. Міжнародна кіберзлочинність.

З приводу цієї загрози О. Буров наголошує, що негативний вплив кіберзлочинності на національну безпеку та її інформаційну складову проявляється у наступному: 1) організованість та наявність джерел фінансування кіберзлочинів, спрямованих на політичну та економічну дестабілізацію країн; 2) високий ступінь вразливості онлайн-сервісів, користувачам яких складно захистити персональну інформацію; 3) розвиток ринку «програмних вразливостей», який є додатковою загрозою безпеці інформації в телекомунікаційних мережах [10, с. 42]. В умовах тотальної інформатизації та цифровізації суспільства, ця загроза стає дедалі актуальнішою та змушує державу постійно удосконалювати системи захисту інформації.

На сьогодні у Стратегії кібербезпеки України від 2021 року закріплені наступні загрози, які негативно позначаються на інформаційній безпеці: гібридна агресія РФ проти України у кіберпросторі (використання кіберзброї наступального призначення); кіберзлочинність, яка завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам; організовані та спонсоровані урядами інших держав кібератаки, що пов'язані з викраденням у політичних, економічних або військових цілях чутливої інформації (кібершпигунство); використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності [11].

В Законі України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 року. № 2163-VIII деталізовані об'єкти кібербезпеки та кіберзахисту, які охороняє держава. Мова йде про: 1) конституційні права і свободи людини і громадянина; 2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; 3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність; 4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; 5) об'єкти критичної інфраструктури; 6) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні

ресурси; 7) об'єкти критичної інформаційної інфраструктури; 8) комунікаційні системи, які використовуються для задоволення суспільних потреб [12].

4. Дезінформаційні кампанії проти України.

Щодо природи цієї загрози Т. С. Перун наголошує, що відсутність міжнародних домовленостей і взаємних зобов'язань держав із питань заборони інформаційної зброї і демілітаризації світової інформаційної сфери відкривають широкі можливості перед спеціальними службами і збройними силами щодо використання потенціалу інформаційних технологій на шкоду інтересам миру, стабільності й міжнародної безпеки. На думку науковця проблема ускладнюється тим, що специфіка інформаційної сфери дозволяє віддалено і приховано впливати на критично важливу інформаційну інфраструктуру, порушити роботу систем управління енергетикою, транспортом, зв'язком, фінансовою сферою, викликати техногенні аварії, завдати серйозної шкоди підприємствам і установам, а також підірвати основи обороноздатності країни [13, с. 135].

Якщо зосередитися за сутності категорії «дезінформація», то слід звернути увагу на тезу В. О. Тімашова та Л. В. Ніколаєвої які стверджують, що дезінформація – це цілеспрямована, умисна діяльність з метою надати завідомо хибну інформацію про певні події чи речі. До дезінформації належить сфабрикована, змішана з фактами та реальними подіями інформація, яка суттєво відрізняється від будь-яких схожих на новини даних, а також це автоматизовані облікові записи, які використовують для функціонування мереж прихильників фейкових новин, зрежисовані відео чи цільова реклама [14, с. 291].

Чинники існування цієї загрози доволі комплексно окреслює О. Самчинська яка переконана, що обов'язковими ознаками дезінформації є: умисел створення, модифікації та/або поширення недостовірної інформації; умисел введення в оману; заздалегідь визначена мета та порушення або можливість порушення прав та законних інтересів особи чи держави як наслідок такої діяльності. Тобто, уся дезінформація за своєю природою є недостовірною інформацією, але не уся недостовірна інформація може вважатися дезінформацією [15, с. 41].

Висновки з дослідження і перспективи подальших розвідок у даному науковому напрямку. Таким чином, сфера інформаційної діяльності є достатньо вразливою та постійно стикається з різними зовнішніми загрозами. Вони по-різному, але негативно, впливають на стан захищеності інтересів держави, суспільства та особистості в інформаційній сфері. Переважно, мова йде про деструктивний вплив, наслідками якого є втрата відомостей, порушення чи обмеження права на інформацію, формування викривленого уявлення про події та процеси, які відбуваються в державі, порушення цілісності інформації у відповідних національних та глобальних інформаційних системах. Характер проаналізованих загроз розкриває їхню природу, яка пов'язана з неправомірними діями суб'єктів, які спрямовані на досягнення такого результату, який суперечить національним інтересам в інформаційній сфері. Проведене дослідження показало, що усі загрози перебувають в площині інформаційної діяльності, точніше її окремих видів (одержання, використання, поширення та зберігання інформації). Також означені загрози слід пов'язати із процесом задоволення інформаційних потреб, адже вони негативно впливають на нього. Це стосується неправомірних обмежень або використання наративів, які формують у суспільстві деструктивні настрої. Проаналізовані загрози свідчать про достатню умовність належного стану інформаційної безпеки, який залежить від багатьох чинників. З огляду на це, перспективним напрямком подальших наукових пошуків є систематизація засобів попередження зовнішніх загроз інформаційній безпеці.

Література:

1. Золотар О. О., Трубін І. В. Класифікація загроз інформаційній безпеці. *Інформаційне право*. 2013. № 3 (9). С. 105–112.
2. Логінов А. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади: дис. … канд юрид. наук: 12.00.07. Київ. 2005. 186 с.
3. Шемчук В. В. Загрози інформаційній безпеці: проблеми визначення та подолання. *Експерт: парадигми юридичних наук і державного управління*. 2020. № 1. С. 285–296.
4. Яковюк І. В., Білоусов Є. М. Національна безпека України в умовах нових викликів європейській та євроатлантичній солідарності: монографія. Харків: «ФО-П Рубан В. В.». 2022. 148 с.
5. Леонов Б. Д., Лихова С. Я. Інформаційний тероризм як загроза національній безпеці України. *Юридичний вісник*. 2021. № 2 (59). С. 170–176.
6. Андрусишин Ю. Я., Бараннік В. В. Інформаційний тероризм як сучасна загроза інформаційній безпеці людини, суспільства, держави. *Інформаційна безпека людини, суспільства, держави*. 2021. № 1. С. 6–15.
7. Лесько Н. В. та Малець М. Р. Правова характеристика глобальної мережі Інтернет. *Юридичний науковий електронний журнал*. 2021. № 1. С. 186–189.
8. Коваленко І. А. Актуальні проблеми захисту й охорони прав інтелектуальної власності в мережі Інтернет в умовах глобалізації суспільства та сучасних технологій. *Вчені записки ТНУ імені В. І. Вернадського*. 2018. № 3. С. 52–55.
9. Брижко В. М. Захист персональних даних: реалії та практика сучасності. *Інформація і право*. 2013. № 3 (9). С. 25–34.
10. Буров О. Кіберзлочинність як загроза інформаційному суспільству. *Теорія і практика інтелектуальної власності*. 2008. № 3. С. 39–44.
11. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серпня 2021 р. № 447/2021. *Урядовий кур'єр*. 2021. № 65.
12. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 р. № 2163-VIII. *Голос України*. 2017. № 208.
13. Перун Т. С. Забезпечення інформаційної безпеки в зоні бойового конфлікту. *Актуальні проблеми держави і права*. 2020. № 5. С. 131–138.
14. Тімашов В. О., Ніколаєва Л. В., Міхайличенко В. Г. Правовий захист суспільства від дезінформації. *Юридичний науковий електронний журнал*. 2022. № 6. С. 288–293.
15. Самчинська О. А. Дезінформація: поняття та сутність. *Адміністративне право і процес*. 2022. № 3 (38). С. 32–45.

Nedokhliebov I. Theoretical and legal analysis of external threats to information security of Ukraine

Summary. The article provides a comprehensive theoretical and legal analysis of external threats to Ukraine's information security. The author substantiates the expediency of considering threats to the information security of the state through the prism of the nature of their occurrence (internal and external). It is proposed to consider external threats to information security as a set of phenomena, factors and events that arise and are formed at the international level, and are implemented at the domestic level, are associated

with a negative external influence on the information system and threaten national interests in the field of information activities. The author comes to the conclusion that the field of information activity is quite vulnerable and constantly faces various external threats that negatively affect the state of protection of the interests of the state, society and the individual. It is argued that external threats are associated with destructive influence, the consequences of which are loss of information, violation or limitation of the right to information, formation of a distorted view of events and processes taking place in the state, violation of the integrity of information in the relevant national and global information systems. It has been proven that the nature of external threats is related to the illegal actions of subjects, which are aimed at achieving such a result that contradicts national interests in the information sphere. The author draws attention to the fact that external threats are in the plane of certain types of information activities (receiving, using, distributing and storing information). It has been established that external threats are related to the process of satisfying information needs, because they negatively affect it through illegal restrictions or the use of narratives that create destructive attitudes in society. It was found that the state of information security depends, among other things, on an effective system for preventing external threats.

Key words: information security, information activity, information needs, external threats, national interests, national security, countermeasures and prevention, legal regulation.