УДК 351.746.1

Тарас Ткачук,

канд. юрид. наук, доцент, заступник завідувача кафедри організації захисту інформації з обмеженим доступом Навчально-наукового інституту інформаційної безпеки

СУЧАСНІ ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ: ТЕОРЕТИКО-ПРАВОВИЙ АНАЛІЗ

Стаття присвячена огляду підходів до сутності загроз інформаційній безпеці та політико-правовому аналізу загроз інформаційній безпеці України на сучасному етапі. Загрози інформаційній безпеці аналізуються в контексті системи загроз національній безпеці.

Ключові слова: інформаційна безпека, національна безпека, державна безпека, небезпека, загроза.

Постановка проблеми. Інтенсивна інформатизація всіх сфер життєдіяльності суспільства нині є одним із визначальних глобальних чинників подальшого соціально-економічного, інтелектуального та духовного розвитку людства. Водночас людство вступає в нову еру розвитку, котра може бути охарактеризована як період інформаційних воєн. Зокрема, інформаційний складник становить ключовий елемент гібридної війни проти України, що створює реальні загрози національній безпеці. Відтак за умови швидкого формування й розвитку інформаційного суспільства в Україні особливого значення набувають проблеми інформаційної безпеки [1], передусім протидія інформаційним загрозам [2].

Дослідження сучасних загроз інформаційній безпеці держави ґрунтується на наукових здобутках відомих дослідників у сфері безпекознавства, політології, соціології, теорії управління тощо, таких як це О. Бандурка, В. Горбулін, Є. Скулиш, І. Івченко, Р. Калюжний, А. Качинський, В. Ліпкан, А. Марущак, Г. Новицький, В. Пилипчук, М. Стрельбицький та інші науковці, які присвятили свої праці питанням забезпечення національної безпеки. Організація протидії загрозам інформаційній безпеці також стала предметом досліджень таких учених, як В. Бут, В. Домарєв, М. Живко, М. Танцюра, В. Цимбалюк та інші. Водночас, оскільки загрози інформаційній безпеці держави в сучасних умовах є динамічними та постійно змінюються, відповідна проблематика наукових досліджень не втрачає своєї актуальності.

Мета статті – здійснити політико-правовий аналіз сучасних загроз інформаційній безпеці держави в контексті забезпечення національної безпеки України.

Виклад основного матеріалу. Спираючись на положення Закону України «Про основи національної безпеки України» [3], можна стверджувати, що система загроз слугує основою для стратифікації національної безпеки на зовнішньополітичну, внутрішньополітичну, державну, воєнну, економічну, соціальну, гуманітарну, екологічну й інформаційну безпеку, а також безпеку державного кордону. Утім перелік сфер, у яких можуть виявлятися загрози національній безпеці, та форм їх вияву не є вичерпним, адже за сучасних умов зовнішні загрози можуть мати внутрішні джерела й інтегруватися з внутрішніми загрозами [4, с. 13–16].

Саме необхідність протидії загрозам зумовлює можливість дослідження національної безпеки з погляду функціонально-діяльнісного підходу, відповідно до якого національна безпека розглядається як динамічне явище, котре постійно еволюціонує, забезпечуючи реалізацію національних інтересів [5, с. 39] в умовах можливого розгортання загроз, а також дає змогу оцінювати можливості суспільства щодо належного забезпечення «гомеостатичного стану» об'єктів національної безпеки. Відповідно, національна безпека «є системою оптимізації взаємовідносин між усвідомленими загрозами та ресурсами, що має суспільство для протидії цим загрозам» [6, с. 84].

Незважаючи на те що поняття загрози неодноразово наводилося в різних доктринальних і нормативно-правових джерелах, досі немає єдиного підходу до визначення його змісту й ролі в теорії безпекознавства. Зокрема, А. Антонов і В. Балашов визначають загрозу як процес настання таких змін у стані особи, суспільства й держави, що оцінюються ними як здатні створити перешкоди або унеможливити реалізацію їхніх інтересів [7, с. 48]. Разом із тим слово «загроза» в словнику С. Ожегова [8, с. 673] означає можливу небезпеку, тому припускає не лише процес настання змін, а й можливість їх настання. Під загрозою також розуміють «можливість або неминучість виникнення чогось небезпечного, прикрого, тяжкого для кого-, чого-небудь», «те, що може заподіювати яке-небудь зло, якусь неприємність» [9, с. 95].

Щодо загроз безпеці, то їх у загальному вигляді визначають як сукупність чинників та умов, що створюють небезпеку певному об'єкту. В. Горбулін та А. Качинський розглядають загрозу як родову ознаку безпеки (можливість чи неминучість виникнення соціальних, природних або техногенних явищ із прогнозованими, але неконтрольованими небажаними подіями, що можуть статись у певний момент часу в межах певної території, спричинити смерть людей

чи завдати шкоди їхньому здоров'ю, призвести до матеріальних і фінансових збитків тощо) [4, с. 14, 27–28]. Небезпеку ж науковці вважають якісним станом – безпекою на її нульовому рівні [4, с. 13].

Загрози національній безпеці можуть бути класифіковані за різними підставами, що висвітлює їх складну та багатошарову систему. Зокрема, у науковій політологічній думці загрози національній безпеці класифікуються за місцем знаходження джерела – зовнішні та внутрішні; за масштабами можливих наслідків – загальнонаціональні, регіональні, локальні, поодинокі; за ступенем сформованості – потенційні, реальні; за ступенем суб'єктивного сприйняття – завищені, занижені, мінімальні, умовні, адекватні; за характером виникнення – загрози природного, техногенного й соціального характеру; за сферами життєдіяльності – загрози в економічній, політичній, оборонній, міжнародній, соціальній, інформаційній, науково-технічній, екологічній, культурній і духовній сферах [4, с. 203–205] тощо.

М. Литвин і В. Кохан, досліджуючи питання внутрішньої безпеки, пропонують вирізняти загрози національній безпеці України у сферах політики, економіки, у соціальній і військовій сферах, у сферах екології, культури, освіти і просвітництва, боротьби зі злочинністю, а також загрози, що викликають аварії й катастрофи техногенного, природного та іншого характеру [10]. В. Ліпкан уважає, що поділу на внутрішні й зовнішні підлягають передусім джерела загроз [11, с. 54].

Як зазначає М. Хусаінов, принципова відмінність постконфронтаційного періоду полягає в тому, що на заміну домінуючій загрозі світу й інтересам наддержав приходить велика кількість потенційних загроз меншого масштабу, однак досить серйозних за своїми наслідками, що зачіпають інтереси багатьох країн [12, с. 68]. Паралельно з розширенням діапазону традиційних загроз процеси глобалізації є також причиною появи їх нової генерації. В основі специфічної якості цих загроз лежить характерне для глобалізації «відтериторіювання» явищ і процесів, які функціонують у транскордонному суспільному просторі, відірвані від територіальної локалізації.

Дійсно, аналіз найбільш актуальних в умовах сьогодення загроз національній безпеці дає змогу дійти висновку щодо взаємозв'язку джерел виникнення і способів вияву більшості внутрішніх і зовнішніх загроз. Відповідно, на доктринальному рівні з'являються пропозиції щодо розширення типології зовнішніх і внутрішніх загроз національній безпеці шляхом уведення нового типу загроз – транскордонних, що мають глобальний характер та об'єднують одночасно ознаки внутрішніх і зовнішніх загроз: за формою вияву є переважно внутрішніми, а за своєю сутністю (за джерелами виникнення та стимуляції, складом можливих учасників тощо) – можуть бути й зовнішніми. До цього типу загроз варто зарахувати загрози інформаційній безпеці держави, що зумовлюється специфікою інформаційної сфери життєдіяльності суспільства і стимулює розвиток нефізичної концепції безпеки.

Чинна Стратегія національної безпеки України серед основних загроз національній безпеці, які мають безпосередній стосунок до інформаційної сфери, визначає агресивні дії Росії, що підривають суспільно-політичну стабільність з метою знищення держави Україна й захоплення її території, в тому числі інформаційно-психологічну війну, приниження української мови й культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу, а також ведення інформаційної війни проти України, відсутність цілісної комунікативної політики держави, недостатній рівень медіакультури суспільства, уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, фізична й моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом [13]. Необхідно зауважити, що у Стратегії відмежовуються вияви інформаційно-психологічної війни (п. 3.1), загрози кібербезпеці й безпеці інформаційних ресурсів (п. 3.7) від суто загроз інформаційній безпеці (п. 3.6), що, на нашу думку, не є виправданим.

Інформаційна безпека посідає особливе місце в системі національної безпеки. Хоча всі складники в структурі національної безпеки пов'язані між собою, варто зазначити, що окремі види безпеки є не лише самостійними, а й такими, що мають відповідні виміри в інших сферах життєдіяльності суспільства, закладаючи фундамент забезпечення їх безпеки. Серед таких «інтегративних» [14] видів доцільно передусім назвати інформаційну безпеку. То ж загрози інформаційного характеру можуть спрямовуватись до будь-яких складників державної безпеки, однак їх негативний вплив завжди опосередковуватиметься завданням шкоди інформаційній безпеці держави. Зокрема, економічна безпека в сучасних умовах інформаційно-мережевої економіки безпосередньо залежить від безпеки інформаційної, адже головним ресурсом розвитку виробництва стає інформаційний продукт [15, с. 162]. Невипадково виняткову небезпечність загроз інформаційній безпеці підкреслює Г. Сащук: «Ураховуючи той факт, що під впливом інформаційних атак може цілеспрямовано змінюватися світогляд і мораль як окремих осіб, так і суспільства загалом, нав'язуються чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності й форм виявів сучасних методів прихованого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які суперечать інтересам національної безпеки» [16].

Відтак система загроз інформаційній безпеці має комплексний характер і в загальному вигляді включає в себе загрози безпеці інформації та інформаційної інфраструктури; загрози безпеці суб'єктів інформаційної сфери й соціальних зв'язків між ними від інформаційних впливів; загрози належному порядку реалізації прав та інтересів суб'єктів інформаційної сфе-

ри. Відповідно, доцільно погодитись із визначенням загроз інформаційній безпеці держави як сукупності умов і факторів, які становлять небезпеку життєво важливим інтересам держави суспільства й особи у зв'язку з можливістю негативного інформаційного впливу на свідомість і поведінку громадян, а також інформаційні ресурси та інформаційно-технічну інфраструктуру [17, с. 89]. До істотних властивостей загроз інформаційній безпеці держави при цьому належать вибірковість, передбачуваність і шкідливість [18, с. 17].

Зважаючи на динамічність суспільно-політичної обстановки та появу якісно нових небезпечних для нашої держави факторів, закріплення фіксованого переліку загроз інформаційній безпеці України, який до того ж не має вичерпного характеру, навряд чи є доцільним. Тому пропоновані науковцями переліки зазвичай є розширеними та більш актуальними порівняно з наведеним вище [17, с. 90–91], однак і такі розгорнуті переліки загроз не можуть уважатися вичерпними та незмінними. Джерелами загроз при цьому можуть бути людина, технічні пристрої, моделі, алгоритми, програми; технологічні схеми обробки; зовнішнє середовище тощо [19, с. 67].

Найбільш небезпечні загрози інформаційній безпеці держави, передусім транскордонні й такі, що мають політичне забарвлення, вже тривалий час вивчаються в рамках проблеми інформаційної війни, під поняттям якої об'єднуються. Інформаційна війна з урахуванням наявних точок зору на її природу може бути визначена як сукупність цілеспрямованих інформаційних впливів, що здійснюються з використанням інформаційної зброї, а також дій, не опосередкованих її використанням, спрямованих на заволодіння інформацією, що не є загальнодоступною, її несанкціоноване поширення, модифікацію або знищення, здійснювані задля досягнення запланованої мети. Інформаційна війна становить найвищий ступінь інформаційного протиборства, спрямований на розв'язання суспільно-політичних, ідеологічних, національних, територіальних конфліктів між державами, народами, націями та соціальними групами шляхом широкомасштабної реалізації засобів і методів інформаційної зброї [20, с. 365]. На думку В. Горбуліна, О. Додонова, Д. Ланде [21, с. 7], інформаційні війни, котрі є лише елементами багатоаспектних військово-політичних протистоянь, прийнято називати інформаційними операціями. Їх основними методами інформаційної війни слугують блокування або перекручування інформаційних потоків і процесів прийняття рішень супротивником [22, с. 77].

Так, з метою виправдання свого втручання у внутрішні справи України Росія вже тривалий час спрямовує свою пропаганду проти української влади, намагається дискредитувати європейський вибір нашої держави, виставляє АТО «карательною акцією» з «хаотичними бойовими діями», які призводять до невиправданих жертв серед мирного населення, поширює чутки про непрофесійність і деморалізованість української армії [23, с. 181]. Крім того, в інформаційний простір України запускаються проекти тотального соціального зомбування, які начебто не пов'язані з політичними питаннями та подіями в АТО, але насправді спрямовані на просування ідеології «Русского міра» та використовують маніпулятивні технології, маскуючись під пропаганду добра, людяності, взаємодопомоги з метою здійснення масштабного впливу на свідомість українців [24, с. 207].

До виявів інформаційної війни може бути зарахована й так звана інформаційна злочинність [25], левова частка якої припадає на кіберзлочини. З урахуванням сучасних тенденцій до розширення мережевої архітектури організованої злочинності в цей час відбувається формування неформальних груп хакерів у навчальних закладах і безпосередньо у віртуальному просторі. Також наявні відомості про залучення організованими злочинними групами хакерів до підготовки злочинів у кредитно-банківській сфері, на фондовому ринку, до протиправного заволодіння службовою інформацією. Не виключена й розробка організованими злочинними співтовариствами планів інформаційних операцій, у т. ч. інформаційних диверсій.

Якщо станом на 2015 рік Україна посідала 5 місце у світовому рейтингу з ризику зіткнення з веб-загрозами [26, с. 87], після атаки вірусу «Petya» в поточному році, від якої постраждали енергетичні компанії, банки, урядові сайти тощо, антирейтинг нашої країни в питаннях кібербезпеки відчутно зріс. За оцінками фахівців, 2017 рік загалом характеризують такі тенденції у сфері загроз інформаційній безпеці: неконтрольовані ризики, пов'язані з так званим «інтернетом речей» і поширенням мережевих з'єднань; стрімке зростання «кіберзлочинів як сервісу» – надання цифрових послуг кримінальними синдикатами; зростання правових ризиків у сфері регулювання мережевих комунікацій; хакерські атаки, спрямовані на підрив репутації брендів і політичних сил [27].

Особливою групою загроз інформаційній безпеці, що актуальні для України, є загрози, зумовлені віртуалізацією – соціальним відчуженням людини, зміненими станами свідомості, переходом до особистісного віртуального світу. За прискорених темпів інформаційного прогресу, особливо з розвитком «інтернету речей», людина взагалі ризикує перетворитися на даток до інформаційних технологій та інформаційних ресурсів. Тому необхідно забезпечити не лише безпеку інформації, а й інформаційну безпеку суспільства, котре, у свою чергу, є носієм такої глобальної загрози інформаційній безпеці людини, як інформаційна дискримінація, яка виявляється в поділі людей на тих, які мають доступ до інформації, і тих, які його не мають, адже від цього залежить можливість формування неспотвореної «картини світу». Як правильно зазначає З. Живко, закрити національний інформаційний простір від такого інформаційного впливу, передусім зовнішнього, за допомогою адміністративних заходів неможливо, то ж варто оберігати його від загроз безпеці так само, як наземний, повітряний і морський [28, с. 117–118].

Висновки

Інформаційна безпека є складним, системним, багаторівневим явищем, на стан якого впливають зовнішні і внутрішні чинники, зокрема політична обстановка у світі; внутрішньополітична обстановка в державі; стан і рівень інформаційно-комунікаційного розвитку країни тощо. Загрози інформаційній безпеці здебільшого супроводжують виникнення й реалізацію загроз в економічний і політичній сферах, у сфері виконання функцій держави тощо, і заподіяння шкоди в інформаційні сфері є передусім засобом досягнення інших цілей. Поряд із суто корисливою метою в сучасних умовах інформаційні загрози пов'язані з розпалюванням міжнаціональної, міжконфесійної та іншої ворожнечі, дискредитацією правоохоронної системи й органів державної влади загалом, заподіянням шкоди честі, гідності та ділової репутації фізичних осіб, у тому числі публічних, формуванням «образу ворога», «зомбуванням» населення задля створення умов щодо управління масовою свідомістю. При цьому потенціал інформаційної сфери через її інтегрувальний характер і здатність «проникнення» до інших сфер життєдіяльності суспільства внаслідок їх інформаційного обслуговування поки що недостатньо усвідомлюється політиками та правоохоронцями (за винятком виявів кіберзлочинності), однак успішно використовується представниками організованих злочинних співтовариств і політичними супротивниками нашої держави. Стратегічне інформаційне протистояння нині становить небезпечний компонент гібридної війни, розгорнутої Росією проти України, причому головною загрозою інформаційній безпеці нашої держави сьогодні залишається загроза впливу ворога на інформаційну інфраструктуру, інформаційні ресурси, на суспільство, свідомість і підсвідомість особистості з метою нав'язати власну систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності.

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 № 47/2017 [Електронний ресурс]. – Режим доступу : www.president.gov.ua/documents/472017-21374.

2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України : Указ Президента України від 15.03.2016 № 96/2016 [Електронний ресурс]. – Режим доступу : www.president.gov.ua/documents/962016-19836.

3. Про основи національної безпеки України : Закон України від 19.06.2003 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/964-15.

4. Горбулін В.П. Засади національної безпеки України / В. Горбулін, А. Качинський. – К. : Інтертехнологія, 2009. – 272 с.

5. Качинський А.Б. Індикатори національної безпеки: визначення та застосування їх граничних значень / А.Б. Качинський. – К. : НІСД, 2013. – 104 с.

6. Горлач М.І. Політологія: наука про політику / М. Горлач, В. Кремень. – К. : Центр учбової літератури, 2009. – 840 с.

7. Антонов А.Б. Основы обеспечения безопасности личности, общества и государства : [учебное пособие] / А. Антонов, В. Балашов. – М. : Институт защиты предпринимателя, 1996. – С. 36–55.

8. Ожегов С.И. Словарь русского языка / С.И. Ожегов. – М., 1988. – 748 с.

9. Словник української мови : в 11 т. / АН УРСР, Ін-т мовознавства ім. О.О. Потебні ; редкол.: І.К. Білодід (голова) та ін. – К. : Наукова думка, 1972. – Т. 3 / ред.: Г.М. Гнатюк, Т.К. Черторизька. – 1972. – 744 с.

10. Литвин М.М. Умови та фактори внутрішньої загрози національній безпеці України / М. Литвин, В. Кохан [Електронний ресурс]. – Режим доступу : plesetsk-info.ru/uchebnoe-posobie/umovi-ta-faktori-vnutrshno-zagrozi-natconalni-bez.

11. Ліпкан В.А. Національна безпека України : [навчальний посібник] / В. Ліпкан. – К. : КНТ, 2009. – 576 с.

12. Хусаинов М.И. Современные подходы к классификации транснациональных угроз безопасности / М. Хусаинов // Вестник Военного университета. – 2010. – № 1 (21). – С. 65–70.

13. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про національну безпеку України» : Указ Президента України від 26.05.2015 № 287/2015 [Електронний ресурс]. – Режим доступу : www.president.gov.ua/documents/2872015-190.

14. Прокоф'єва-Янчиленко Д.М. Кримінологічна безпека як інтегративна складова національної безпеки / Д.М. Прокоф'єва-Янчиленко // Наукові праці Національного університету «Одеська юридична академія». – 2014. – № 14. – [Електронний ресурс]. – Режим доступу : naukovipraci.nuoua.od.ua/tom-xiv.

15. Цивілізаційний вибір України: парадигма осмислення і стратегія дії : [національна доповідь] / ред. кол.: С. Пирожков, О. Майборода, Ю. Шайгородський та ін. ; Інститут політичних і етнонаціональних досліджень ім. І.Ф. Кураса НАН України. – К. : НАН України, 2016. – 284 с.

16. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки / Г. Сащук [Електронний ресурс]. – Режим доступу : http:// journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php.

17. Інформаційна безпека (соціально-правові аспекти) / [В. Остроухов, В. Петрик, М. Присяжнюк та ін.] ; за ред. Є.Д. Скулиша. – К. : КНТ, 2010. – 776 с.

18. Дереко В.Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки / В. Дереко // Інформаційна безпека людини, суспільства, держави. – 2015. – № 2 (18). – С. 16–22.

19. Хмелевський Р.М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності / Р. Хмелевський // Сучасний захист інформації. – 2016. – № 4. – С. 65–70.

20. Світлична В.Ю. Інформаційна безпека: багатогранність сутності, види загроз та шляхи забезпечення / В. Світлична, Т. Світлична // Науково-технічний збірник. – Х. : ХНАМГ, 2013. – № 109. – С. 360–369.

21. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : [монографія] / В. Горбулін, О. Додонов, Д. Ланде. – К. : Інтертехнологія, 2009. – 164 с.

22. Сопілко І.М. Інформаційні загрози та безпека сучасного українського суспільства / І. Сопілко // Юридичний вісник. – 2015. – № 1 (34). – С. 75–80.

23. Куцька О.М. Особливості інформаційно-психологічного впливу Російської Федерації напередодні та початковому етапі антитерористичної операції на сході України / О. Куцька // Інформаційна безпека людини, суспільства, держави. – 2017. – № 1(21). – С. 180–190.

24. Снитко О.С. Проекти тотального зомбування в інформаційному просторі України / О. Снитко // Інформаційна безпека людини, суспільства, держави. – 2017. – № 1 (21). – С. 207–215.

25. Юрченко И.А. Понятие и виды информационных преступлений / И. Юрченко // Российское право в Интернете. – 2003. – № 1. – [Электронный ресурс]. – Режим доступа : http://rli.consultant.ru/ magazine/2003/01.

26. Платоненко А.В. Сучасні загрози інформаційної безпеки для державних та приватних установ України / А. Платоненко // Сучасний захист інформації. – 2015. – № 4. – С. 86–90.

27. Thor Olavsrud. 4 information security threats that will dominate 2017. CIO (December 29, 2016) [Online tool]. – Available at : https:// cio.com/article/3153706/security/4-information-security-threats-that-will-dominate-2017.html.

28. Живко З. Інформаційні загрози: суть і проблеми / З. Живко, М. Живко // Безпека та захист інформації в інформаційних системах : тези доповідей ІІ міжнародної НПК. – К., 2017. – С. 116–118.

Статья посвящена обзору подходов к сущности угроз информационной безопасности и политико-правовому анализу угроз информационной безопасности Украины на современном этапе. Угрозы информационной безопасности анализируются в контексте системы угроз национальной безопасности.

Ключевые слова: информационная безопасность, национальная безопасность, государственная безопасность, опасность, угроза.

The article is devoted to the review of approaches to the essence of threats to information security and politico-juridical analysis of threats to information security of Ukraine at the present stage. The threats of information security are analysed in the context of the system of threats of national security.

Key words: information security, national security, state security, dangers, threat.