

РОЗДІЛ II

Конституційне, адміністративне, інформаційне та міжнародне право

УДК 340:659.2(477)

Р. Банк

Сучасна правова парадигма інформаційної безпеки України

Стаття присвячена проблемі правового забезпечення інформаційної безпеки як складової національної безпеки України. Визначено нормативно-правове закріплення інформаційної безпеки України та окреслено суттєві прогалини в законодавстві України в регулюванні цього явища. Проведено аналіз та класифікацію видів інформаційних загроз. Запропоновані деякі шляхи вирішення проблеми правового забезпечення інформаційної безпеки у контексті збереження інформаційного суверенітету України.

Ключові слова: безпека, інформаційна безпека, національні інтереси, інформаційний суверенітет, безпекознавство

Актуальність теми. В умовах сучасних глобалізаційних потрясінь та макроекономічних негараздів у світовій економіці, інформація стає дедалі вагомішим ресурсом, за допомогою якого громадяни, суспільства та держави отримують певний матеріальний зиск. Інформація з нематеріального блага перетворилась у фінансовий дивіденд, який можна акумулювати заради досягнення власних амбіцій. За таких обставин захист інформації та інформаційних ресурсів стає першочерговим завданням владних інституцій, яким необхідно розробити механізм захисту від інформаційних загроз. Для нейтралізації інформаційним загрозам існує система комплексного забезпечення інформаційної безпеки, яка покликана протидіяти дестабілізуючим факторам, що негативно впливають на інформаційне середовище. Проблема забезпечення інформаційної безпеки, у зв'язку з швидким зростанням інформаційних технологій набула нових тенденцій, зокрема у питаннях широкого застосування автоматизованих інформаційних систем, заснованих на використанні комп'ютерних і телекомунікаційних засобів.

За роки незалежності в Україні були намагання розробити правові, економічні, техніко-технологічні, медійні комплексні заходи із забезпечення інформаційної безпеки. Однак, як показує практичний досвід, залишається ряд невирішених проблемних питань, які потребують ретельного наукового дослідження, зокрема у правовому полі.

Мета статті полягає у дослідженні правових аспектів забезпечення інформаційної безпеки України та її законодавчого визначення. Для реалізації визначеної мети необхідно вирішити наступні **завдання**: 1) здійснити правовий та соціально-філософський аналіз поглядів щодо розуміння інформаційної безпеки; 2) дослідити застосування поняття «інформаційна безпека» у законодавстві України; 3) визначити інформаційні загрози, що впливають на стан забезпечення інформаційної безпеки України.

Аналіз досліджень та публікацій. Феномену інформаційної безпеки присвячено праці як зарубіжних так і вітчизняних науковців. До теоретиків та практиків, які займалися дослідженням інформаційної безпеки з правових, економічних, технічних, управлінських поглядів слід віднести: І. Арістову, В.Бебика, Д.Белла, Ж.Бодрійара, А. Гальчинського, О. Голобуцького, П. Друкера, Я. Жаліло, О. Зошенко, М. Зубка, І. Коліушко, А. Колодюка, Е. Лемберга, В.Ліпкана, Є. Макаренко,

Н. Марчука, Г. Почепцова, А. Пшеворського, М. Роуза, Е. Тофлера, Ф. Фукуяму С.Хантінгтона, Б. Хофмана, В. Цимбалюка та інших. Необхідно зауважити, що комплексний аналіз цього феномену потребує подальших практичних та теоретичних досліджень в контексті вдосконалення системи інформаційної безпеки України.

Виклад основного матеріалу. У сучасному світі інформація стає стратегічним національним ресурсом – одним з основних багатств економічно розвинутої держави, головним джерелом економічної і військової могутності держави. Національний інформаційний ресурс повинен стати одним із вирішальних ресурсів розвитку країни, привабливою сферою вкладення капіталів суб'єктів господарської діяльності. Жодна сфера життя сучасного суспільства не може функціонувати без розвинутої інформаційної структури. Проникаючи в усі сфери діяльності держави, інформація здобуває конкретне політичне, матеріальне і вартісне вираження. Йде об'єктивний процес становлення інформаційного суспільства, в якому інформаційна діяльність буде основою економічного процвітання і благополуччя.

Динамічний розвиток економічних, політичних, соціальних подій ХХІ століття сформулювали нове уявлення про інформацію, як одного із факторів (ресурсів) виробництва. На макрорівні інформація впевнено займає позиції головного фактора могутності держави, адже здатність держави мати у своєму розпорядженні найсучасніші інформаційні технології дозволяє ефективно управляти інформацією. Володіння державою такою здатністю – шлях до подальшого нарощування своєї економічної та військової міцності [1, с. 2].

Економічна та військова могутність держави певною мірою залежить від здатності забезпечити інформаційну безпеку як складову національної безпеки України. Згідно розд. VI п. 3 Закону України «Про Концепцію Національної програми інформатизації», інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки [2].

Нині інформаційна безпека відіграє одну з ключових ролей у забезпеченні життєво важливих інтересів країни. Це, в першу чергу, обумовлено швидким розвитком сучасних інформаційно-телекомунікаційних технологій, засобів зв'язку й інформатизації і, як наслідок, істотним зростанням впливу інформаційної сфери на життя нашого суспільства.

Закріплення в Конституції України (ст. 17) пріоритетності інформаційної безпеки, як основної функції держави демонструє рівень значущості інформаційних процесів та важливості протидії інформаційним загрозам [3].

У зв'язку з російською інформаційною окупацією України, захист інформаційного суверенітету України та налагодження механізму протидії інформаційному впливу на українське суспільство вимагає інноваційних підходів.

В ст. 8 Закону України «Про основи національної безпеки України», визначено основні напрями державної політики з питань національної безпеки в інформаційній сфері, зокрема про забезпечення інформаційного суверенітету України, про вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України та ін. [4]. Однак, необхідно відмітити, що положення означеного Закону мають здебільшого декларативний зміст, що нівелює його практичне застосування.

Більш практичну цінність мають підзаконні нормативні акти, які конкретизують суб'єкт інформаційних загроз, що впливає на рівень забезпечення інформаційної безпеки України. Так, в розд. III «Стратегії національної безпеки України», затвердженої Указом Президента України від 26 травня 2015 року зазначено про агресивні дії Росії, що здійснюються для виснаження української економіки і підризу суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території, що супроводжуються інформаційно-психологічно війною, приниженням української мови і культури, фальшуванням української історії, формуванням російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу [5].

У п. 7 «Воєнної доктрини України» затвердженої Указом Президента України від 24 вересня 2015 року зазначено, що однією з головних тенденцій, що впливає на воєнно-політичну обстановку в регіоні довкола України, є інформаційна війна Російської Федерації проти України. У п. 7 «Воєнної доктрини України» визначено, що одним з воєнно-політичних викликів, які можуть перерости в загрозу застосування воєнної сили проти України є цілеспрямований інформаційний (інформаційно-психологічний) вплив з використанням сучасних інформаційних технологій, спрямований на формування негативного міжнародного іміджу України [6].

Безумовно, вищезазначені нормативні акти деталізують інформаційні загрози та суб'єкта, що здатний їх використати заради досягнення власних цілей. В той же час, для протидії означеним

загрозам в Україні створений орган виконавчої гілки влади – Міністерство інформаційної політики України, основним завданням якого є забезпечення інформаційного суверенітету України.

На Міністерство інформаційної політики України відповідно до Положення «Про Міністерство інформаційної політики України», затвердженого постановою Кабінету Міністрів України від 14 січня 2015 року покладено ряд важливих завдань, а саме здійснення нормативно-правового регулювання у сфері забезпечення інформаційного суверенітету України, зокрема з питань поширення суспільно важливої інформації в Україні та за її межами, а також забезпечення функціонування державних інформаційних ресурсів та безпосередня участь у формуванні державної інформаційної політики [7].

Аналіз означеної вище нормативно-правової бази свідчить про суттєвий прогрес у питаннях збереження інформаційного суверенітету України, але в той же залишаються проблемні питання системного підходу щодо забезпечення інформаційної безпеки держави, зокрема прийняття спеціального законодавства, в якому б чітко визначались суб'єкти інформаційної діяльності та розподіл повноважень між ними у сфері протидії інформаційній агресії щодо України.

Вбачається доцільним відмітити, що таким спеціальним законодавством могла б стати розроблена Експертною радою при Міністерстві інформаційної політики України «Доктрина інформаційної безпеки України» (далі – Доктрина), прийнята 29 грудня 2016 року Радою національної безпеки і оборони України та затверджена Указом Президента України 25 лютого 2017 року.

Доктрина визначає засади формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни. Також Доктриною передбачено захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку Російської Федерації, захист українського суспільства від агресивного інформаційного впливу Російської Федерації, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України, всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірної та об'єктивної інформації і т.д. [8].

Прийняття означеного документу вирішує деякі прогалини у законодавстві щодо державної політики забезпечення інформаційної безпеки України, однак не усуває їх повністю. По-перше, доктрина не має такої правової сили по відношенню до інших нормативних документів, наприклад як закон і залишається суцільно системою офіційних поглядів, концептуальних ідей і положень, по-друге, особлива структура доктрини не може чітко регламентувати і вирішити широкий спектр проблемних питань, що визначені у законі та надати їм особливого юридичного статусу загальнообов'язковості.

У зв'язку з вищезазначеним не погоджуємось з позицією Є. Євграфової, яка вважає, що усі приписи (положення), що викладені в актах/доктринах, закріплюють основні цілі, принципи, завдання, етапи реалізації, строки проведення намічених заходів, очікувані результати), є правовими імперативами, обов'язковими до виконання, а не рекомендаціями чи пропозиціями [9, с. 57].

Однак визначені у Доктрині завдання для конкретних органів державної влади мають суцільно формальний зміст і за саботаж виконання цих завдань для означених органів державної влади можливе настання тільки політичної відповідальності, що нівелює значення і юридичну силу Доктрини.

На підтвердження хибності прийняття доктрини замість спеціалізованого закону як базового юридичного документу у сфері забезпечення інформаційної безпеки України було прийняття Доктрини інформаційної безпеки України ще у 2009 році, затвердженої Указом Президента України. В цьому документі, який вже втратив чинність, напрями державної політики у сфері інформаційної безпеки України були визначені обтічно та викладені без функціонального наповнення, що в подальшому призвело до можливості безперешкодного втручання в інформаційний простір України та порушення інформаційного суверенітету України державою-агресором.

Очевидно, що інформаційна безпека є складним, системним, багаторівневим явищем, на стан і перспективи розвитку якого мають безпосередній вплив зовнішні і внутрішні чинники.

Одним з таких чинників, крім недосконалої чинного інформаційного законодавства є фінансова слабкість більшості українських ЗМІ, яку для задоволення власних планів використовують закордонні неурядові організації, фінансово-політичні клани, радикальні та екстремістські налаштовані політичні сили для проникнення в інформаційний простір держави. Зокрема, використовуючи можливості українського медіапростору, іноземні держави здійснюють інформаційну політику у вигідному для них руслі (проведення широкомасштабних PR-акцій,

стажування українських журналістів, поширення друкованої продукції тощо).

Також за останні роки зафіксовано спроби використати окремих радикально настроєних осіб з метою дестабілізації суспільно-політичної обстановки, розпалювання сепаратистських настроїв, національної та релігійної ворожнечі.

На сьогоднішній день загрози інформаційній безпеці України мають руйнівний вплив для її державності. На нашу думку, серед найбільш небезпечних видів можна виділити наступні:

- інформаційний тероризм (маніпулювання свідомістю, пропаганда, зомбіювання певних соціальних груп, інформаційний шантаж та ін.);
- кібертероризм (хакерські атаки на суб'єктів публічної адміністрації, проникнення в інформаційно-телекомунікаційну систему, перехоплення управління, поширення небезпечних вірусів, розсилка спам-реклами та ін.);
- інформаційна експансія та інформаційне домінування (захоплення медіа-простору, теле- і радіо частот, витіснення альтернативних ЗМІ, інформаційний вакуум).
- поширення неякісної інформації (дискредитація, дезінформація, чутки, фальшива інформація та ін.);
- несанкціонований і неправомірний вплив сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання);
- слабка інформаційна інфраструктура (обмеженість щодо протидії інформаційній агресії);
- промисловий шпіонаж (порушення прав інтелектуальної власності, проведення конкурентної розвідки, розкрадання патентованої інформації);
- неефективність державної інформаційної політики (недосконалість законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства).

У межах нашого дослідження важливо відзначити, що транскордонний характер загроз інформаційній безпеці обумовлює необхідність вироблення і реалізації комплексних зусиль для ефективної протидії їм у взаємодії з міжнародними організаціями. Так, найбільш активне співробітництво України в галузі інформаційної безпеки спостерігається з НАТО в рамках програми «Безпека через науку». Ця програма використовує такі механізми підтримки в галузі інформаційної безпеки: гранти на налагодження та укріплення зв'язків, які існують; візити експертів та трансфер технологій; створення дослідницьких центрів; підтримку проектів досліджень [10, с.18].

Також ефективним засобом протидії інформаційним загрозам стало налагодження співробітництва між НАТО і країнами-партнерами, одним з яких є Україна, в рамках Ради євроатлантичного партнерства (РСАП) та програми «Партнерство заради миру» (ПЗМ). Приєднання України до програми ПЗМ передбачало підписання і ратифікацію у 2002 році Угоди про безпеку між Урядом України і Організацією Північноатлантичного Договору [11]. Пізніше, у 2015 р. Україною була підписана і ратифікована Угода про співробітництво у сфері підтримки між Кабінетом Міністрів України та Організацією НАТО з підтримки та постачання (ОНПП) [12]. Згідно з цими угодами сторони погоджуються консультуватися в політичних питаннях і питаннях безпеки, розширювати й інтенсифікувати політичне і військове співробітництво в Європі, усвідомлюючи, що ефективність співробітництва в цих сферах має на увазі обмін таємною інформацією та/або інформацією обмеженого доступу.

Висновки. Враховуючи все вищезазначене, необхідно відмітити, що стан забезпечення інформаційної безпеки в Україні є незадовільним, адже існує низка таких проблем як порушення інформаційного суверенітету та інформаційного простору України, інформаційно-психологічна агресія, інформаційна маніпуляція та зомбіювання населення, низька інформаційна культура суспільства та інші дестабілізуючі інформаційні проблеми, що безумовно, негативно впливають на рівень забезпечення інформаційної безпеки України.

В умовах військово-інформаційних викликів Україна має бути готова до забезпечення своєї інформаційної безпеки, при цьому нашій державі необхідно розробити всеосяжну і чітку стратегію інформаційного захисту, що має сприяти досягненню поставлених цілей, а не перешкоджати їх досягненню. В майбутньому цю систему необхідно розвивати, враховуючи правові, технологічні, матеріально-фінансові та інші аспекти.

Реалізація стратегічних завдань, основних принципів державної інформаційної політики та відновлення інформаційного суверенітету України, потребує вдосконалення організаційно-правових механізмів забезпечення інформаційною безпекою держави, відповідного інтелектуального та інноваційно-ресурсного потенціалу, зокрема вдосконалення законодавства з інформаційної безпеки,

зокрема шляхом:

– розробки і прийняття Закону України «Про забезпечення інформаційної безпеки України», Національної стратегії формування інформаційного суспільства та Концепції інформаційної безпеки України;

– внесення змін до Кримінального кодексу України, а саме доповнення ст. 258⁶ «Інформаційний терористичний акт»;

– кодифікації та уніфікації інформаційного законодавства;

– оптимізації державної політики інформатизації, регулювання інформаційного співробітництва, контролю за встановленим порядком і правилами формування і використання інформаційних ресурсів;

– закріплення на законодавчому рівні інтернет-відносин у ланцюгу держава-інтернет-споживач.

Отже, формування нових суспільних відносин в інформаційному суспільстві передбачає створення відповідного комплексу правового забезпечення. Усі елементи суспільного життя, пов'язані із забезпеченням інформаційної безпеки України, мають бути достатньо врегульовані чітко встановленими правилами поведінки (законодавством).

Джерела та література

1. Гуцалюк М. Інформаційна безпека України: нові загрози / М. Гуцалюк // *Бизнес и безопасность*. – 2003. – № 5. – С. 2-3.
2. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 р. № 75/98-ВР // *Відомості Верховної Ради України*. – 1998. – № 27-28. – Ст. 182.
3. Конституція України: Закон України від 28 черв. 1996 р. № 254к/96-ВР // *Відомості Верховної Ради України*. – 1996. – № 30. – ст. 141.
4. Про основи національної безпеки України: Закон України від 19 черв. 2003 р. № 964-IV// *Офіційний вісник України*. – 2003. – № 29. – Ст.1433.
5. Стратегія національної безпеки України: Указ Президента України від 26 травня 2015 року № 287 [Електронний ресурс]. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/287/2015>.
6. Воєнна доктрина України: Указ Президента України від 24 вересня 2015 року № 555 [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/555/2015/paran8#n8>.
7. Про Міністерство інформаційної політики України: Постанова Кабінету Міністрів України від 14 січня 2015 р. № 2 [Електронний ресурс]. – Режим доступу: <http://zakon0.rada.gov.ua/laws/show/2-2015-%D0%BF>.
8. Доктрина інформаційної безпеки України: Указ Президента України від 25 лютого 2017 року № 47 [Електронний ресурс]. – Режим доступу: <http://www.president.gov.ua/documents/472017-21374>.
9. Євграфові Є. Доктрина у правовій науці і юридичній практиці / Є. Євграфова // *Вісник Національної академії правових наук України*. – 2013. – № 2 (73). – С. 52-62.
10. Войціховський А.В. Питання інформаційної безпеки України на сучасному етапі / А.В. Войціховський // *Право і безпека*. – 2015. – № 3 (58). – С. 15-20.
11. Угода про безпеку між Урядом України і Організацією Північноатлантичного Договору від 13.03.1995 р. (ратиф. Україною 12.09.2002 р.) [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/950_002.
12. Угода про співробітництво у сфері підтримки між Кабінетом Міністрів України та Організацією НАТО з підтримки та постачання (ОНПП) від 27.04.2015 р. (ратиф. Україною 01.07.2015 р.) [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/950_029.
13. Банк Р.О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект / Р.О. Банк // *Інформація і право*. – 2016. – № 1 (16). – С. 110-116.

Банк Р. Современная правовая парадигма информационной безопасности Украины.

Данная статья посвящена проблеме правового обеспечения информационной безопасности как составляющей национальной безопасности Украины. Информация из нематериального блага превратилась в финансовый дивиденд. При таких обстоятельствах защита информации и информационных ресурсов становится первоочередной задачей властных институтов, которым необходимо разработать механизм защиты от информационных угроз. Для нейтрализации

информационных угроза существует система комплексного обеспечения информационной безопасности, которая призвана противодействовать дестабилизирующим факторам, негативно влияющим на информационную среду. Сейчас информационная безопасность играет одну из ключевых ролей в обеспечении жизненно важных интересов страны. Это обусловлено существенным ростом влияния информационной сферы на жизнь общества. Закрепление в Конституции Украины приоритетности информационной безопасности, как основной функции государства демонстрирует уровень значимости информационных процессов и важности противодействия информационным угрозам. Реализация стратегических задач, основных принципов государственной информационной политики и восстановление информационного суверенитета Украины, нуждается в совершенствовании организационно-правовых механизмов обеспечения информационной безопасности государства, соответствующего интеллектуального и инновационно-ресурсного потенциала, в частности совершенствование законодательства о информационной безопасности.

Ключевые слова: безопасность, информационная безопасность, национальные интересы, информационный суверенитет.

Bank R. Modern Legal Paradigm of Information Security in Ukraine. The article deals with the problem of legal support of the information security as an integral part of the national security of Ukraine. The concept of information has evolved from the intangible benefits matter into a financial dividend. Under such circumstances the protection of information and information resources is the primary task of the governmental institutions which are obliged to develop a mechanism of protecting information security. To neutralize the threat to the information resources there exists an integrated system of measures ensuring information security, which aims at counteracting the destabilizing factors that negatively influence the information environment. Now the information security plays a principal role in providing vital interests of the society, which is due to a significant increase in the influence of the information sphere on the life of society. The fact that priority of information security as the function of the state is fixed in the Constitution of Ukraine shows the level of importance of information processes and the importance of counteraction to the threats concerning it. Implementation of strategic objectives, basic principles of state information policy and restoring information sovereignty of Ukraine require improvements in the institutional and legal mechanisms to ensure information security, appropriate intellectual and innovative resources, including improvement of legislation in this field.

Key words: security, information security, national interests, information sovereignty.

УДК [340.126:347.4](477+438)

А. Гороть

Характеристика джерел регіонального співробітництва України в рамках Єврорегіону «Буг»

У статті здійснено аналіз основоположних актів, які започаткували розвиток регіонального співробітництва України в рамках Єврорегіону «Буг». Визначається що нормативно-правова база регіонального співробітництва двох держав, особливо з другої половини 90-х років, значно наблизилась до кращих європейських зразків, що дало змогу ефективно налагодити регіональну співпрацю в межах єврорегіонів. Підсумки роботи Єврорегіону «Буг» переконливо свідчать про значний потенціал такої моделі транскордонного співробітництва, але його подальший розвиток потребує адекватних інструментів і ресурсів, у першу чергу людських та фінансових. Для того, щоб забезпечити неухильне просування Єврорегіону «Буг» вперед, необхідно вміло й ефективно задіяти усі наявні механізми та фінансові джерела.

Ключові слова: єврорегіони, Єврорегіон «Буг», інтеграція, регіональне співробітництво, транскордонне співробітництво, Україна.