

СУТНІСТЬ ПРАВОВОЇ ПРИРОДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**THE ESSENCE OF THE LEGAL NATURE OF INFORMATION SECURITY**

Гончаров М.В., доктор філософії

У статті розглянуто сутність правової природи інформаційної безпеки з позицій різних дослідників. Проведений аналіз наукових джерел дозволив виявити, що правова природа інформаційної безпеки в цілому, так і на елементарному рівні характеризується науковістю, системністю та має багато аспектів.

Дослідження цілісного поняття «інформаційна безпека» вимагає застосування комплексного підходу до розуміння значення (семасіології) кожного терміну, який його формує («інформація і безпека»). При цьому необхідно зауважити, що термін «інформація» застосовується не як системоутворююча складова, а вживається для означення якісної характеристики базового елемента, тобто категорії «безпека», що розкриває галузеве спрямування і змістовне наповнення заходів, та створює відповідне поле нормативно-правового регулювання.

Для розуміння об'єктивного змісту цілісного поняття «інформаційна безпека» послугуватимемося можливостями окремих методологічних інструментів (в основному, аналізу, синтезу та ін.), які сприятимуть вивченню глибинних діалектичних зв'язків між визначеними категоріями, що його формують.

Акцентовано увагу на основних завданнях державної інформаційної політики та з'ясована мета політики забезпечення інформаційної безпеки України, це формування відкритого інформаційного суспільства, як простору цілісної держави, інтегративного в світовий інформаційний простір з урахуванням національних особливостей і інтересів при забезпеченні інформаційної безпеки на внутрішньодержавному та міжнародному рівнях.

Державна політика забезпечення інформаційної безпеки повинна базуватися на наукових і методологічних розробках, систематизованих і об'єднаних в єдину концепцію. Вона може бути представлена як сукупність національних цілей, інтересів і цінностей; стратегії та тактики управлінських рішень і методів їх реалізації, що розробляються та реалізуються державною владою.

Ключові слова: інформаційна безпека України, забезпечення інформаційної безпеки, національна безпека, система, державна інформаційна політика.

The article examines the essence of the legal nature of information security from the standpoint of various researchers. The analysis of scientific sources made it possible to reveal that the legal nature of information security in general, as well as at the elemental level, is characterized by scientificity, systematization and has many aspects.

The study of the integral concept of «information security» requires the application of a complex approach to understanding the meaning (semasiology) of each term that forms it («information and security»). At the same time, it should be noted that the term «information» is not used as a system-forming component, but is used to denote the qualitative characteristics of the basic element, that is, the category «security», which reveals the industry direction and content of measures, and creates a corresponding field of regulatory and legal regulation.

In order to understand the objective content of the integral concept of «information security», we will use the possibilities of separate methodological tools (mainly, analysis, synthesis, etc.), which will contribute to the study of deep dialectical connections between the defined categories that form it.

Attention is focused on the main tasks of the state information policy and the goal of the policy of ensuring information security of Ukraine is clarified, which is the formation of an open information society as a space of an integral state, integrating into the global information space, taking into account national characteristics and interests while ensuring information security at the domestic and international levels.

The state policy of ensuring information security should be based on scientific and methodological developments, systematized and combined into a single concept. It can be presented as a set of national goals, interests and values; strategies and tactics of management decisions and methods of their implementation, which are developed and implemented by the state authorities.

Key words: information security of Ukraine, provision of information security, national security, system, state information policy.

Постановка проблеми. Актуальність теми дослідження визначається важливим значенням інформаційної сфери для задоволення не тільки потреб суспільства у передаванні і зберіганні відомостей, а й для виконання однієї з найважливіших функцій держави – забезпечення національної безпеки України. На сьогоднішній день забезпечення інформаційної безпеки в Україні полягає у здатності нашої країни захищати національні економічні інтереси від зовнішніх і внутрішніх загроз, також спроможності національної економіки зберігати й поновлювати процес суспільного відтворення.

Необхідною умовою розвитку сучасного суспільства є високий рівень інформаційної безпеки. Саме тому ефективне здійснення правового регулювання інформаційними ресурсами є важливою умовою забезпечення інформаційної безпеки та реалізації виваженої державної політики.

Стан опрацювання цієї проблематики. Вивченню даного питання приділяли увагу багато науковців та дослідників: Біленчук П. Д., Білько С. С., Гнатюк С. Л., Григорчук М. В., Дзьобань О. П., Довгань О. Д., Золотар О. О., Косілова О. І., Кудін С. В., Ліпкан В. А., Логінов О. В., Новицька Н. Б., Ткачук Т. Ю., Тихомиров О. О., Француз А. Й., Цимбалюк В. С., Шевченко А. Є., Ярема О. Г. та інші.

Мета статті – розглянути тенденції наукових поглядів сутності інформаційної безпеки України.

Виклад основного матеріалу. З метою забезпечення комплексного підходу до виконання завдань нашого наукового дослідження звертаємося до джерельної науково-практичної бази у сфері інформаційної безпеки України. Це означає, що емпіричною базою для такого аналізу слугуватимуть опрацьовані нами джерела без градації на галузеву приналежність.

О. Д. Довгань, Т. Ю. Ткачук, досліджуючи історичні аспекти та джерела оприлюднення перших згадувань про інформаційну безпеку, зазначають: «Проблематика інформаційної безпеки та її забезпечення у різних аспектах висвітлювались у наукових працях Плутарха, Сенеки, Платона, Макиавеллі, Гроція, а також інших вітчизняних та зарубіжних дослідників» [1, с. 80].

Як вбачається з наведеної вище цитати, логічним висновком є те, що сфера інформаційної безпеки ще в ранні часи набула дуалістичного характеру. Причиною цього, на наш погляд, є те, що вказані вчені мали визначні досягнення не тільки в юриспруденції, а й у філософії. Тому виведені ними узагальнення поєднують у собі юридичну і філософську компоненту.

О. О. Золотар, досліджуючи першоджерела інформаційної безпеки, зазначає, що «початок історії захисту

інформації вчені пов'язують з появою можливості фіксації інформаційних повідомлень на твердих носіях, тобто з винаходом писемності, а першим видом інформації, що підлягала захисту, вважають державну таємницю» [2, с. 140].

На думку науковця, майже одночасно з винайденням писемності були відкриті методи і способи захисту інформації, а саме шифрування і приховування. Як приклад О. О. Золотар наводить історичний факт, що засвідчує спосіб захисту інформації від стороннього доступу і поширення. Такий випадок відомий як перший шифрований текст, прихований під рецептом глазурі при нанесенні її на вироби гончарства (Месопотамія, 2000 років до н. е.).

Відомі наукові погляди щодо розуміння та формування парадигми інформаційної безпеки мають в основі широку палітру філософського знання, що сягає своїм корінням глибокої давнини. Філософи минувшини завжди досліджували причини і джерела загроз, намагалися домогтися стабільного миру та процвітання. За таких умов трансформувалися підходи до розуміння інформації. Питання безпеки особи, суспільства, держави та отримання достовірної інформації цікавили мислителів Стародавнього світу. Щоправда, вказана проблема розглядалася переважно в контексті війни й миру [3, с. 40].

О. Курбан, досліджуючи генезу інформаційного впливу в XVIII столітті на прикладі боротьби за незалежність мешканців північноамериканських колоній, зазначає: «У своїй боротьбі колоністи використовували соціальні мережі (товариства «Сини свободи», «Кореспондентські комітети»), застосовували образні символи («дерево свободи», стереотипи та лозунги «Воля або смерть»). Вони дуже активно застосовували дієві акції, тогочасні медіа, чутки, маніпуляцію» [4, с. 30].

О. П. Дзьобань, досліджуючи наукову спадщину Томаса Гоббса та Еммануїла Канта, зазначає, що «наукове обґрунтування проблеми національної безпеки взагалі, й інформаційних її аспектів зокрема, в сучасному розумінні й певні напрямки її вирішення містяться у працях вказаних науковців» [5, с. 41].

О. Павленко, вивчаючи генезу інформаційної безпеки, здійснила аналіз історичних джерел виникнення і розвитку цієї галузі права, і запропонувала його поділ на етапи:

I етап – до 1816 року – характеризується використанням природно виникаючих засобів інформаційних комунікацій. Для цього періоду основним завданням збереження відомостей полягало в недопущенні сторонніх осіб до володіння інформацією про факти, майно, події тощо, які мали для людини чи колективу людей важливе, а в окремих випадках – життєве значення.

II етап – починаючи з 1816 року – пов'язаний з початком використання штучно створених технічних засобів електро- і радіозв'язку. Поряд з використанням досвіду попереднього періоду застосовувалися такі інструменти захисту інформації, як «перешкодостійке кодування повідомлення (сигналу) з подальшим декодуванням прийнятого повідомлення (сигналу)».

III етап – починаючи з 1935 року – пов'язаний з появою засобів радіолокації і гідроакустики. У цей період головним напрямком у сфері захисту інформації було забезпечити приймальні пристрої радіолокаційних систем «активними маскуючими і пасивними імітуючими радіоелектронними перешкодами».

IV етап – починаючи з 1946 року – пов'язаний з винаходом і впровадженням у практичну діяльність електронно-обчислювальних машин (комп'ютерів). Для даного етапу характерним виступало фізичне обмеження доступу сторонніх осіб до устаткування, на якому зберігалася інформація.

V етап – починаючи з 1965 року – обумовлений створенням і розвитком локальних інформаційно-комунікаційних мереж. Завданнями інформаційної безпеки зазна-

ченого періоду були забезпечити ефективне збереження інформації шляхом фізичного захисту джерел (носіїв) інформації.

VI етап – починаючи з 1973 року – пов'язаний з використанням надмобільних комунікаційних пристроїв з широким спектром завдань. З урахуванням технологічних проривів загрози інформаційній безпеці ставали дедалі серйознішими, що вимагало розроблення відповідних систем захисту від несанкціонованого втручання (хакерства) у порядок використання інформаційних ресурсів. У цей час починає формалізуватися інформаційне право як нова галузь міждержавної правової сфери.

VII етап – починаючи з 1985 року – пов'язаний зі створенням і розвитком глобальних інформаційно-комунікаційних мереж з використанням космічних засобів забезпечення [6].

Колектив науковців, серед яких А. Б. Тоцький, О. І. Тимошенко, А. М. Гуз, вважають, що історія охорони і захисту інформації на території сучасної України також сягає ще додержавних часів. Першим видом інформації, яку потрібно було охороняти, була військова інформація. Спочатку охорону такої інформації забезпечував князь, потім особа, яку він призначав особисто. Війна була на той час головним і загально визначним способом ведення зовнішньої політики будь-якої держави, тому захист військової інформації був головним у політиці князів Олега, Ігоря, Святослава, Ярослава та княгині Ольги. Князі, йдучи в похід, намагалися приховати інформацію про кількість війська і напрям головного удару. Ворог не міг адекватно реагувати на небезпеку, а заздалегідь розпущені чутки, перебільшення і неправдива інформація ще більше призводили до паніки [7, с. 11].

У контексті сказаного вище доцільно навести озвучений результат наукової розвідки колективу у складі В. М. Петрик, А. М. Кузьменко, В. В. Остроухов, які віднайшли одне з первинних документальних свідчень про застосування інформації з метою обману ворогів при провадженні воєнних дій. Науковці зазначають, що до XIII ст. належить один з перших історичних прикладів масштабного застосування дезінформації у воєнних цілях. Пов'язаний цей приклад із вторгненням монголів до Угорщини у 1241 р. [8, с. 56]. Монголи розбили військо угорців та їх союзників на річці Шайо і при цьому серед трофеїв виявили королівську печатку. Хан Батий наказав підготувати наказ угорською мовою від імені короля Бели про припинення опору, скріпивши його захопленою королівською печаткою. Цей документ розіслали в різні частини ще не завойованої країни, що сприяло введенню в оману угорської армії.

Окремо слід вирізнити напрацювання у цій галузі права закордонних науковців, так, Роберт Оуен уважав, що «тільки звільнення народів від приватновласницького ярма й об'єднання їх в один союз покладе край насильству й уможливить забезпечення безпеки [9, с. 375]. На думку відомого філософа й економіста, справжній безпековий стан як вселюдська гармонія можливий лише за умови організованого виховання населення при застосуванні інформаційних інструментів виховного характеру.

Ю. М. Канигін та В. І. Кушерець вважають, що «суспільство з великим запізненням починає осмислювати політичні, економічні, соціальні, військові, психологічні та інші наслідки глобальної інформатизації» [10, с. 35].

Вважається, що одними з перших проблеми комп'ютерної інформаційної безпеки усвідомили і зробили впевнений крок до їх вирішення державні відомства США в кінці 60-х років XX століття, коли комп'ютери коштували великих грошей, а інтернет зароджувалася з нечисленних, виключно військових і наукових інформаційних мереж.

Українська історія також зберегла свідчення про факти використання інформації як для доведення до відома

ворога неправдивих відомостей, та і для організації протидії внутрішнім загрозам щодо недопущення витоку секретної інформації.

Так, у матеріалах раніше згадуваного доробку авторського колективу за участі А. Б. Тоцького, О. І. Тимошенко, А. М. Гуз, знаходимо відомості про те, що у Запорізькій Січі та державі Богдана Хмельницького вироблені були своєрідні форми захисту військово-політичної інформації. Хмельницький широко використовував дезінформацію. В спогадах польських урядовців та військових часто зустрічається рядки на кшталт «одне думає, про інше пише», «наміри його жодним чином не можна зрозуміти». Хмельницький зазначав у жовтні 1648 р.: «А військова справа така: коли мисль буде йти на війну, щоб тої мислі ніхто не видав і недруг би остерігався» [7, с. 14].

Основною метою зловмисників завжди буває порушення складових інформаційної безпеки – доступності, цілісності або конфіденційності.

С. О. Лисенко: Серед останніх новацій із-за кордону варто зазначити, що 15 липня 2016 року німецький уряд затвердив план «Біла книга» з питань оборонної політики та безпеки, в тому числі інформаційної. В ній чітко вказано, що Російська Федерація стала реальною загрозою, що шкодить існуючому міжнародному порядку та європейській безпеці.

Поточним підсумком до вищесказаного є те, що сучасний стан і розуміння значення інформаційної безпеки нерозривно пов'язані з тими наріжними каміннями, на яких виникла і ґрунтується державна політика у сфері забезпечення як національного, так і міжсуб'єктного спілкування з дотримання межових знаків, встановлених як

допустимі норми освідомлення з приватно-державними процесами конкретних національних утворень.

Показовими у цій ситуації є висновки, озвучені С. О. Лисенко за результатами дослідження історичних аспектів інформаційної безпеки як сфери спеціальних правовідносин. Науковець зазначає, що в ситуації, що склалась, правомірно «задекларована необхідність підвищення загальної інформаційної захищеності всього блоку НАТО... [11, с. 23–25]. При цьому науковець відзначає надзвичайну потребу у створенні Європейської ПРО, а також висловлюється про необхідність удосконалення механізмів захисту інформаційного поля. Такий підхід можна пояснити необхідністю створення оновленої системи захисту інформації між країнами НАТО.

Висновки. Як вбачається з вищеведеного, інформація не існує відособлено від людського середовища і має конкретну мету, з якою впливає на суспільство. Здійснене дослідження підтвердило науково-практичну тезу про те, що на різних етапах розвитку суспільства рівень інформаційного впливу на людей напряду залежав від розвитку інструментів інформаційного впливу. Саме для розв'язання окремих завдань нашого дослідження ми торкнулися генезуальних проблем у підходах до розуміння правової природи інформаційної безпеки. На наш погляд, фундаментальними засадами виникнення у зародковому стані понять, які сьогодні визначені як інформаційна безпека, є звичаєве право, елементи якого у процесах розвитку цивілізації набули загальнообов'язкового характеру для їх учасників на підґрунті запровадження нормативно-правового регулювання цієї сфери.

ЛІТЕРАТУРА

1. Довгань О. Д., Ткачук Т. Ю. Наукова рефлексія інформаційної безпеки України: від позитивізму до метафізики права. *Інформація і право*. 2018. № 4 (27). С. 79–89.
2. Золотар О. О. Генеза суспільних відносин щодо інформаційної безпеки людини. *Інформація і право*. 2018. № 1 (24). С. 139–148.
3. Псалтир. Харків: Фоліо, 2013. 574 с.
4. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі. Київ, 2016. 286 с.
5. Дзьобань О. П. Національна безпека України: концептуальні засади та світоглядний сенс: монографія. Харків: Майдан, 2007. 284 с.
6. Павленко О. Історія виникнення інформаційної безпеки. URL : <https://www.sutori.com/en/story/istoriia-vinikniennia-informatsiinoi-biezpieki-94qRpbMUISHMP2JQSCupsNrN>.
7. Організаційно-правові основи захисту інформації з обмеженим доступом : навч. посіб. [А. Б. Тоцький, О. І. Тимошенко, А. М. Гуз та ін.]. Київ : Європейський університет, 2006. 232 с.
8. Соціально-правові основи інформаційної безпеки. [В. М. Петрик, А. М. Кузьменко, В. В. Остроухов та ін.] : навч. посіб. [за ред. В. В. Остроухова]. Київ : Росава, 2007. 496 с.
9. Оуен Р. Організаційна поведінка в освіті: Керівництво учбовими закладами та шкільна реформа. [пер. з англ. О. В. Христенко]. Харків: Каравела, 2003. 488 с.
10. Канигін Ю. М., Кушерець В. І. Біблія та майбутнє науки: орієнтири сучасних знань. Київ: Т-во «Знання України», 2009. 163 с.
11. Гончаров М. В. Теоретико-правові основи регулювання інформаційної безпеки в Україні: дис. ... канд. юрид. наук: 12.00.01. Ірпінь, 2023. 215 с.