УДК 338.2:351.863
DOI https://doi.org/10.32837/yuv.v0i4.1980

Т. Перун,
кандидат юридичних наук,
асистент кафедри адміністративного та інформаційного права
Навчально-наукового інституту права, психології та інноваційної освіти
Національного університету «Львівська політехніка»

СТРУКТУРНІ ЧИННИКИ МЕХАНІЗМУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Постановка проблеми. Трансформація економічної системи в Україні відповідно до змін світового господарства в умовах глобалізації супроводжується значним посиленням ролі інформаційної безпеки як фундаментальної основи економічної ефективності держави в цілому.

Система інформаційної безпеки держави перманентно перебуває під впливом кризових явищ, її складові елементи можуть негативно відбитися на стані об'єктів інформаційної безпеки національної економіки. Важливим завданням економічної науки є змістовне наповнення категорії «інформаційна безпека держави» з урахуванням розвитку сучасного економічного середовища, яке динамічно розвивається в умовах економічної кризи й підвищених ризиків. Нині встановлюються нові відносини між суб'єктами господарювання в напрямку вдосконалення інформаційної безпеки їхньої діяльності. Тому проблема визначення перспективних напрямків інформаційної безпеки держави на сучасному етапі розвитку економіки актуальна, а дослідження теоретичних основ інформаційної безпеки й побудова на їхній основі сучасних методів її оцінки мають важливе прикладне значення.

Аналіз останніх досліджень і публікацій. Інформаційна система держави через її виключно важливу роль у ринковій економіці знаходиться у фокусі досліджень вчених-економістів. Теоретичні проблеми, пов'язані з різними елементами системи інформаційної безпеки та їхньої взаємодії, досліджуються в роботах таких зарубіжних авторів: М. Вебера, A.Z. Vieane, G.J. Funke, R.S. Gutzwiller, V.F. Mancuso, B.D. Sawyer, C.D. Wickens та інші.

У національній економічній науці досі залишається дискусійним питання про сутність інформаційної безпеки. Дотепер існує не менше двох десятків визначень, різних за своїм смисловим навантаженням. Серед вітчизняних авторів, які приділяли у своїх роботах значну увагу аспектам інформаційної безпеки, можна виділити М.А. Бендікова, Я.Д. Вишнякова, Л.П. Гончаренко, В.П. Шеломенцева, Г.Б. Клейнера, Л.Г. Окорокова, Е.А. Олейникова, В.Л. Тамбовцева, О.О. Барабаш, В. Мунтіян, С.А. Харченко, В.П. Бочарникова й ряд інших.

Формулювання цілей статті (постановка завдання). Метою статті є дослідження генезису поняття «інформаційна безпека держави», аналіз та обґрунтування основних підходів до трактування сутності механізму інформаційної безпеки держави та його структурних чинників, визначення структури й особливостей взаємодії її складових елементів на кожному рівні забезпечення безпеки держави.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Слід зазначити, що у вісімдесятих роках минулого

століття американський футуролог Alvin Toffler у своїй праці “Previews & Premises: An Interview with the Author of Future Shock and The Third Wave” розглядав інформацію як «один із головних видів сировини, причому невичерпної» [1]. Виник новий тип громадських відносин, в якому основним економічним ресурсом виступає інформація – інформаційне суспільство.

Що ж таке інформація? C. Murdoch, K. Knorr, F. Trager, проаналізувавши різні концепції поняття інформації у своїй роботі “Economics interests & national security” [3], виділили ряд її особливостей (рис. 1).

У наш час термін «інформація» розглядається як правова, економічна, соціальна й політична категорія, тому пропонуємо визначення, яке об’єднує всі її галузеві аспекти: *це універсальна категорія, що пронизує всі сфери суспільної діяльності, опосередковує знання та думки, є засобом спілкування, взаємодії та співробітництва, формування стереотипів мислення та поведінки* (рис. 2).

Впровадження інформаційно-комунікаційних технологій відкрило нові можливості для подальшого розвитку інформаційних процесів і для ефективнішого розвитку державних політико-правових інститутів, суб’єктів економічної діяльності, інститутів громадянського суспільства, а також для найповнішої реалізації прав і свобод громадян. Від ефективного використання можливостей сучасних інформаційних технологій залежить безпека держави й перспективи формування правового інформаційного суспільства, яке може реалізовувати конституційні права й свободи громадян.

Однак інформація – це не тільки творча сила. Вона має потенціал, який може дестабілізувати суспільство, якщо її практично необмежені можливості впливу на людину й суспільство використовуються в інтересах

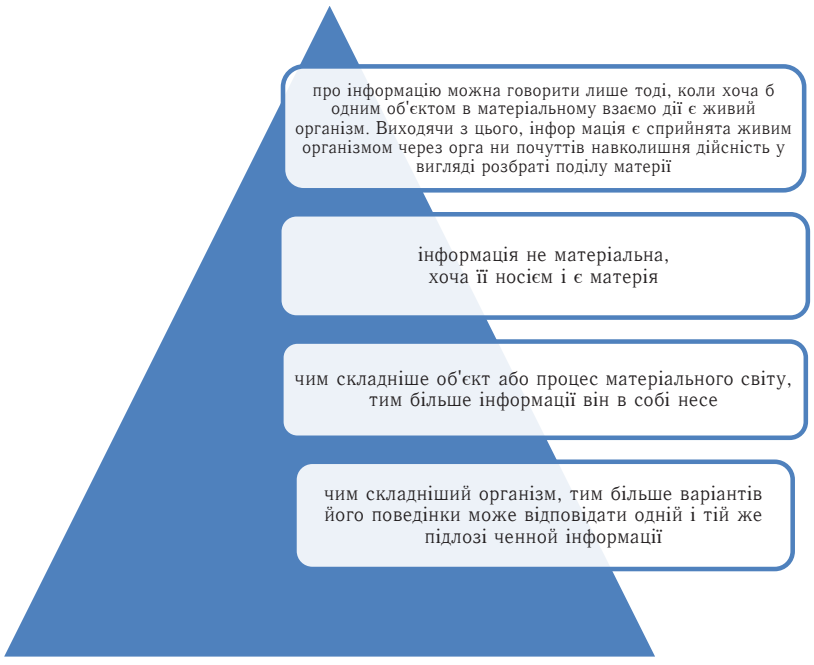

Рис. 1. Визначальні риси інформації як наукової категорії

коаліційних угруповань, окремих держав, політичних угруповань чи окремих осіб. Досвід новітньої історії світу розкрив очевидність: інформація може стати джерелом політичної та соціальної загроз. Цим викликана необхідність державно-правового й суспільного регулювання інформаційних потоків, зокрема діяльності засобів масової інформації (далі – ЗМІ). Виникла сфера політико-правових відносин, що забезпечують інформаційну безпеку особистості, суспільства й держави. Електронні ЗМІ й Інтернет відіграють все більшу роль у політичному житті.

Державні структури, політичні партії, громадські об'єднання відкривають свої сайти й портали, зростають можливості громадянина брати участь у політичному творчому процесі: обговоренні законопроєктів, висуненні ініціатив, участі в інноваційних проєктах і так далі. У зв'язку з інтенсивним розвитком зазначених політичних процесів вельми актуальною стає проблема забезпечення інформаційної безпеки в цій сфері.

Інформаційна безпека у сфері політичних відносин, у політичному процесі може розглядатися як сукупність пов'язаних між собою компонентів, що перманентно взаємодіють.

З процесуального боку інформаційна безпека держави може бути представлена такими основними напрямками:

– інформаційна безпека у сфері політичних інтересів;

– інформаційна безпека у сфері політичних відносин;

– інформаційна безпека у виборчому процесі;

– інформаційна безпека в партійно-політичному процесі;

– інформаційна безпека зовнішньополітичного процесу й тому подібне.

За основними сферами прояву системне вираження інформацій-

Рис. 2. Аспекти інформації

ної безпеки держави локалізується в трьох напрямках:

1) інформаційна безпека у сфері функціонування державних органів влади (державна інформаційна безпека);

2) інформаційна безпека, яка здійснюється у сфері громадянського суспільства (громадська інформаційна безпека);

3) інформаційна безпека особистості, а також особиста інформаційна безпека [7, с. 1179].

Всесвітній день захисту інформаційної безпеки було встановлено 30 листопада 1988 року, коли відбулася перша масова комп'ютерна епідемія, яку спровокував Хробак Моріса (англ. *Morris worm*) [11, с. 20].

Різні компоненти системи інформаційної безпеки держави детально проаналізовано в роботі Nyre-Yu, Megan & Gutzwiller, Robert & Caldwell, Barrett "Observing Cyber Security Incident Response: Qualitative Themes From Field Research. Proceedings of the Human Factors and Ergonomics Society Annual Meetingi" [6].

На думку автора, державно-правовий механізм забезпечення інформаційної безпеки особистості – це система взаємопов'язаних нормативних гарантій та організаційно-діяльнісних елементів, що визначають стан захищеності держави в інформаційній сфері й надають фактичну можливість її громадянам реалізувати свої інформаційні права й свободи.

Структуру механізму забезпечення інформаційної безпеки держави утворюють три елементи: інформаційно-правова, інформаційно-технічна й інформаційно-психологічна безпека.

Інформаційно-правова безпека – це стан захищеності прав громадян на пошук, одержання, зберігання, використання та поширення інформації, а також права на недоторканність інформації про приватне життя. Об'єктами інформаційно-правової безпеки особистості виступають: право людини на інформацію, право на захист від небезпечної інформації, право на недоторканність інформації про приватне життя людини. Право на інформацію – це суб'єктивне право людини, що полягає в можливості вільно здійснювати будь-які операції, пов'язані з пошуком, отриманням, розповсюдженням інформації, як правило, без урахування її призначення та змісту. Право на захист від небезпечної інформації – це суб'єктивне право людини, що полягає в можливості перебувати в стані безпеки від негативних інформаційно-психологічних впливів, у результаті чого здійснювати різні дії, що відповідають її інтересам. Право на недоторканність приватного життя виражається у свободі спілкування між людьми на неформальній основі у сферах сімейного життя, родинних, дружніх зв'язків, інтимних та інших особистих контактів, уподобань, симпатій та антипатій.

Недоліками сучасного стану нормативно-правового забезпечення інформаційної безпеки є: відсутність ратифікації міжнародних документів, термінологічні неточності в нормативних актах, що регулюють питання інформаційної безпеки, розмиті формулювання об'єктів інформаційної безпеки особистості, невизначеність у повноваженнях суб'єктів забезпечення інформаційної безпеки особистості, неврегульованість питань забезпечення інформаційно-психологічної безпеки, на стадії розробки знаходиться законодавство, що регулює питання забезпечення інформаційної безпеки органів державної влади й місцевого самоврядування в глобальній інформаційній мережі Інтернет.

Інформаційно-технічна безпека. Система інформаційно-технічної безпеки ґрунтується на використанні різних комунікаційних засобів, серед яких нині на першому місці – інформаційні технології. Ідентифікація та авторизація застосовуються для обмеження доступу випадкових і незаконних

суб'єктів інформаційних систем до її об'єктів. Ідентифікація – присвоєння суб'єктам та об'єктам доступу особистого ідентифікатора й порівняння його із заданим. Авторизація – перевірка приналежності особі наданого їй ідентифікатора й підтвердження його автентичності. Іншими словами, авторизація полягає в перевірці того, чи є суб'єкт, що підключається, тим, за кого він себе видає.

Загальний алгоритм роботи таких систем полягає в тому, щоб отримати від суб'єкта (наприклад, користувача) інформацію, що засвідчує його особу, перевірити її справжність і потім надати (або не надати) цьому користувачеві доступ до роботи із системою.

Наявність процедур авторизації або ідентифікації користувачів є обов'язковою умовою будь-якої захищеної системи, оскільки всі механізми захисту інформації розраховані на роботу з ідентифікованими суб'єктами й об'єктами інформаційних систем.

Інформаційно-психологічна безпека – це стан захищеності від негативних інформаційних впливів і впровадження деструктивної інформації у свідомість або підсвідомість особи, що дозволяють спеціальними засобами й методами впливати на психіку і, як наслідок, визначати її поведінку. Проблема відкритості інформації та контролю над нею в процесі розширення використання в державній практиці інформаційної техніки поряд із загрозою для розвитку демократії в цілому несе в собі загрозу порушення прав і свобод особи. Річ у тому, що держава, звичайно, володіє великим, у порівнянні з окремою особистістю, економічним і технічним потенціалом для придбання та використання інформаційних засобів, за допомогою яких цілком можливо контролювати окремих людей або групи. Можна сказати, що ступінь демократичності суспільства в цілому пов'язаний зі ступенем інформованості його громадян.

Однак водночас слід враховувати, що повна свобода інформації може призвести й до прямо протилежного результату – комп'ютерного контролю над особистістю, що рівносильно позбавленню особистої свободи. Вже нині з достатньою підставою можна говорити про те, що інформаційні технології досить широко використовують для контролю над особистістю, що суперечить принципам демократії. Не без підстав багато політологів відзначають, що нині стає все очевиднішою загроза поліцейського й політичного спостереження за індивідами за допомогою інформаційної техніки.

Висновки дослідження та перспективи подальших досліджень у цьому напрямі. Однією з істотних причин інформаційної вразливості держави є нерозвиненість політико-правового механізму, що гарантує її інформаційну безпеку. Ефективне функціонування механізму забезпечення інформаційної безпеки забезпечують політичні інституції держави, що встановлюють і реалізують інтереси, цінності й потреби особистості у сфері безпеки.

Перспективним напрямком для подальших наукових досліджень може стати запропонована автором модель та інші схеми, спільно об'єднані в єдиний механізм забезпечення інформаційної безпеки держави.

З метою вдосконалення нормативно-правового забезпечення механізму інформаційної безпеки держави доцільно:

1) на законодавчому рівні виробити єдину термінологію, характерну для цієї сфери, у формі глосарію як обов'язкового нормативного варіанта для інших правових актів, що стосуються інформаційної безпеки;

2) внести категорію «Законодавство у сфері захисту інформаційної безпеки держави» в Єдиний державний реєстр нормативно-правових актів;

3) уточнити положення Доктрини інформаційної безпеки України,

визначивши, що об'єктами інформаційної безпеки є забезпечення права на інформацію, права на захист від небезпечної інформації, права на недоторканність приватного життя громадян;

4) закріпити перелік видів інформації, яку державні, громадські й комерційні організації зобов'язані надати громадянам у межах реалізації ними механізму інформаційної безпеки, а також встановити, які види інформації та в яких випадках повинні надаватися безкоштовно;

5) прийняти Закон України «Про доступ до глобальної мережі Інтернет», в якому поряд з іншими розв'язувалося б питання забезпечення інформаційної безпеки держави в Інтернеті.

У науковій статті викладається ступінь та еволюція механізму інформаційної безпеки. З'ясовано, що термін «механізм інформаційної безпеки держави» базується на основі детермінантів і принципів безпеки.

Інформаційна безпека країни може розглядатися з позиції забезпечення захисту життєво важливих інтересів усіх громадян, суспільства й держави від внутрішніх і зовнішніх загроз.

Автор зазначає, що інформаційна безпека – це динамічний елемент економіки, який адаптується до вимог свого часу. Таким чином, розглядаючи поняття інформаційної безпеки, слід виходити з визначення рівноваги економічної системи та її подальшого сталого розвитку.

Також розглядається взаємодія засобів масової інформації та державних органів влади. Аналізується впровадження інформаційно-комунікаційних технологій як фактору подальшого розвитку інформаційних процесів та ефективнішого розвитку державних політико-правових інститутів. Розглянуто можливі варіанти підвищення ефективності інформаційного забезпечення державної політики. Показано, що інформаційне забезпечення державної політики з доступом громадян до відкритих державних ресурсів є одним зі складників національних інтересів України в інформаційній сфері.

Автор доходить висновку, що з метою вдосконалення нормативно-правового забезпечення механізму інформаційної безпеки держави доцільно: на законодавчому рівні виробити єдину термінологію, характерну для цієї сфери, у формі глосарію як обов'язкового нормативного варіанта для інших правових актів, що належать до інформаційної безпеки; внести категорію інформаційної безпеки держави в Єдиний державний реєстр нормативно-правових актів; уточнити положення Доктрини інформаційної безпеки України, визначивши, що об'єктом інформаційної безпеки є забезпечення права на інформацію, права на захист від небезпечної інформації, права на недоторканність приватного життя громадян.

Ключові слова: інформаційна безпека, форми інформаційної безпеки, інформаційна безпека держави, напрями формування інформаційної безпеки, механізми державного управління.

Perun T. Structural factors of the state information security mechanism

The paper reseach highlights the degree and evolution of the information security mechanism. It was found that the term "state information security mechanism" is based on determinants and security principles.

The information security of the country can be considered from the standpoint of ensuring the protection of vital interests of all inhabitants of the country, society and the state

in the economic sphere from internal and external threats.

Author notes that information security is a dynamic element of the economy that adapts to the requirements of its time. Thus, considering the concept of information security, we should proceed from the definition of the balance of the economic system and its further sustainable development.

The interaction between the media and state authorities is also considered. The introduction of information and communication technologies as a factor of further development of information processes and more effective development of state political and legal institutions is analyzed. Possible options for improving the efficiency of information support of state policy are considered. It is shown that information support of state policy with access of citizens to open state resources is one of the components of national interests of Ukraine in the information sphere.

The author concludes that in order to improve the regulatory and legal support of the information security mechanism of the state it is advisable: at the legislative level to develop a single terminology specific to this area, in the form of a glossary as a mandatory regulatory option for other legal acts related to information security; to enter the category of information security of the state in the Unified state register of normative legal acts; clarify the provisions of the Doctrine of Information Ukraine Security determining that the objects of information security are ensuring the right to information, the right to protection from dangerous information, the right to privacy of citizens.

Key words: information security, forms of information security, information security of the state, directions of formation of information security, mechanisms of public administration.

Література

1. Toffler A. Previews & Premises: An Interview with the Author of Future Shock and The Third Wave. W. Morrow, 1983. 230 p.

2. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 лютого 2017 року № 47/2017 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 29.07.2020).

3. Economic factors as objects of security : Economics security & vulnerability / C. Murdoch, K. Knorr, F. Trager. Economics interests & national security. Lawrence, 2001. 867 p.

4. National Security Act of 1947. URL: https://history. state.gov/milestones/1945-1952/national-security-act.

5. Bahuguna, Ashutosh and Bisht, Raj and Pande, Jeetendra. Don't Wanna Cry: A Cyber Crisis Table Top Exercise for Assessing the Preparedness against Eminent Threats. International Journal of Engineering and Advanced Technology. Vol. 9. Issue 1. October 2019. P. 3705–3710.

6. Nyre-Yu, Megan and Gutzwiller, Robert and Caldwell, Barrett. Observing Cyber Security Incident Response: Qualitative Themes From Field Research. Proceedings of the Human Factors and Ergonomics Society Annual Meeting. 2019. P. 437–441.

7. Martin J., Dubй C., Coovert M. D. Signal detection theory (SDT) is effective for modeling user behavior toward phishing and spear-phishing attacks. Human Factors. 2018. No. 60 (8). P. 1179–1191.

8. Aggarwal P., Gonzalez C., Dutt V. HackIt: A real-time simulation tool for studying real-world cyber-attacks in the laboratory. CNCS 2019, September. DOI: 10.1007/978-3-030-20488-4_11.

9. VieaneA.Z.,FunkeG.J.,GutzwillerR.S., Mancuso V.F., Sawyer B.D., Wickens C.D. Addressing human factors gaps in cyber defense. Proceedings of the Human Factors and Ergonomics Society. No. 60. P. 770–773 ; Vishwanath A., Harrison B., Ng Y.J. Suspicion, cognition, and automaticity model of phishing susceptibility. Communication Research. 2016. No. 45 (8). P. 1146–1166.

10. Бочарников В.П. Fuzzy Technology: основы моделирования и реше-

ния экспертно-аналитических задач / Б.В. Почарников, С.В. Свешников. Киев : Эльга, НикаЦентр, 2003. 296 с.

11. Steinke J., Bolunmez B., Fletcher L., Wang V., Tomassetti A.J., Repchick K.M., Tetrick L.E. Improving cybersecurity incident response team effectiveness using teams-based research. IEEE Security and Privacy. 2015. No. 13 (4). P. 20–29.

12. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення. URL: http://nbuv.gov.ua/UJRN/boz_2012_2_36.

13. Барабаш О.О. Четверте покоління прав людини: загальнотеоретична характеристика. Вісник Національного університету «Львівська політехніка». Юридичні науки. 2016. № 837. С. 213–217.

14. Сулейманова Ш.С. Эффективность информационного обеспечения государственной политики: проблемы и перспективы. Коммуникология. 2018. Том. 6. № 1. С. 15–33. DOI: 10.21453/2311-3065-2018-6-1-15-33.