

СУСПІЛЬНО ЗНАЧУЩІ ФАКТОРИ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ SOCIALLY SIGNIFICANT FACTORS OF STATE INFORMATION SECURITY

Внутрішніми і зовнішніми аспектами національної безпеки є інформаційна безпека, що покликана надійно захищати культурне надбання країни, інтелектуальну власність господарюючих суб'єктів і громадян, а також спеціальні відомості, що становлять державну і професійну таємницю. Тому розвиток будь-якої держави як суверенної, демократичної, правової та економічно стабільної можливий лише за умови забезпечення інформаційної безпеки всіх суб'єктів інформаційних відносин.

Сформульовано таке визначення: інформаційна безпека – стан інформаційного середовища, що забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин, безпеку інформації і захист суб'єктів від негативної інформаційної дії. Інформаційна (інформаційно-психологічна) безпека особистості у сучасному суспільстві постає як нагальна проблема, що потребує комплексного та системного вирішення. Відзначено, що основними принципами інформаційної безпеки є: забезпечення конфіденційності, доступності, цілісності й автентичності інформаційних ресурсів та інфраструктури, що її підтримує.

Ми визначили та проаналізували об'єктивні та суб'єктивні фактори в контексті інформаційного розвитку суспільства та забезпечення інформаційної безпеки, такі як: динамічність інформаційної сфери, підвищення соціального значення інформаційних процесів, правове забезпечення, економічний, інтелектуальний (психологічний), технічний, політико-ідеологічний та людський фактори.

Суспільно значущі фактори державної інформаційної безпеки зумовлюють особливу важливість та пріоритетність різноманітної високопрофесійної державної діяльності в інформаційній сфері, юридичного її забезпечення, а також виваженого вибору методів правового регулювання. Одним із головних завдань держави на етапі розвитку є визначення напрямів правового регулювання та створення правових гарантій, необхідних для самореалізації суб'єктів в інформаційній сфері.

Ключові слова: інформація, безпека, інформаційна безпека, державна безпека, фактори інформаційної безпеки.

Internal and external aspects of national security is information security, which is designed to reliably protect the cultural heritage of the country, the intellectual property of business entities and citizens, as well as special information constituting state and professional secrets. Therefore, the development of any state as a sovereign, democratic, legal and economically stable is possible only if the information security of all subjects of information relations is ensured.

The following definition is formulated: information security – the state of the information environment that ensures the satisfaction of the information needs of the subjects of information relations, information security and the protection of subjects from negative information impact. Information (information-psychological) security of the individual in modern society acts as an urgent problem that requires a comprehensive and systematic solution. It is noted that the main principles of information security are: ensuring the confidentiality, accessibility, integrity and authenticity of information resources and infrastructure, it supports.

Objective and subjective factors were identified and analyzed in the context of the information development of society and ensuring information security, such as the dynamism of the information sphere, increasing the social significance of information processes, legal support, economic, intellectual (psychological), technical, political and ideological and human factors.

Socially significant factors of state information security determine the particular importance and priority of a diverse highly professional state activity in the information sphere, its legal support, as well as a balanced choice of methods of legal regulation.

One of the main tasks of the state at the development stage is to determine the areas of legal regulation and create legal guarantees necessary for the self-realization of entities in the information sphere.

Key words: information, security, information security, state security, information security factors.

УДК 347.92:316:004

DOI <https://doi.org/10.32843/2663-5240-2020-16-20>

Панченко О.А.

д. мед. наук, професор,
заслужений лікар України,
президент
Громадська організація
«Всеукраїнська професійна
психіатрична ліга»

Постановка проблеми у загальному вигляді. Внутрішніми і зовнішніми аспектами національної безпеки є інформаційна безпека, що покликана надійно захищати культурне надбання країни, інтелектуальну власність господарюючих суб'єктів і громадян, а також спеціальні відомості, що становлять державну і професійну таємницю. Тому розвиток будь-якої держави як суверенної, демократичної, правової та економічно стабільної можливий лише за умови забезпечення інформаційної безпеки всіх суб'єктів інформаційних відносин.

У сучасних умовах рівень розвитку та безпеки інформаційного простору країни є системоутворюючими факторами у забезпе-

ченні безпеки, що активно впливають на стан політичної, економічної, соціальної, воєнної, інформаційної та інших складових частин національної безпеки держави.

Тому практичне значення має аналіз суспільно значущих факторів державної інформаційної безпеки як позитивного, так і негативного характеру, які є реальними умовами здійснення правового регулювання, становлення громадянського й інформаційного суспільства, розбудови правової держави, забезпечення національної та інформаційної безпеки з метою вироблення ефективних моделей державного управління та адекватних форм і методів здійснення державної влади.

Аналіз останніх досліджень і публікацій.

Інформаційну безпеку, проблеми захисту національного інформаційного простору досліджували багато науковців. Варто зазначити, що питання, пов'язані з темою дослідження, розглядаються в працях А. Нашинець-Наумової, О. Тихомирова, Г. Почепцова, О. Кустовської, С. Ковтуна, В. Шульги, Н. Довнар, К. Захаренко, Д. Маркової та інших.

Таким чином, дослідження суспільно значущих факторів інформаційної безпеки, пошук механізмів захисту громадян від негативних інформаційних впливів є актуальним питанням для науки і практики державного управління, а саме інформаційної безпеки як невід'ємної складової частини національної безпеки України.

Виділення не вирішених раніше частин загальної проблеми. Питання важливості виявлення суспільно значущих факторів, що впливають на інформаційну безпеку, залишається досить актуальним. Вибрана тема дослідження покликана сприяти вирішенню проблеми інформаційної безпеки суспільства, держави та особистості в умовах турбулентності.

Мета статті – визначити суспільно значущі фактори державної інформаційної безпеки.

Виклад основного матеріалу дослідження. Чіткого науково обґрунтованого підходу як до змісту, так і до поняття «інформаційна безпека» на тепер не вироблено. У нормативних правових актах України і печатній продукції використовуються різні терміни: «безпека», «безпека особистості», «політична безпека», «міжнародна безпека», «національна безпека», «державна безпека», «безпека країни» та ін.

У загальному значенні безпека – це стан захищеності від чого завгодно та може застосовуватися як щодо особистості зокрема, так і суспільства та держави загалом. Водночас це поняття відрізняється залежно від сфери застосування: політології, економіки, соціології і т.д. З позиції суспільних відносин безпекою можна назвати стан, у якому людина має відчуття впевненості та захищеності, почуття довіри до іншої особи або правової системи [6].

Поняття «інформаційна безпека» широко використовується в наукових публікаціях, навчальній літературі та законодавчих документах різного рівня, але воно досі не має однозначного розуміння, а його зміст у різних джерелах має кардинальні розбіжності [2; 5]. Безпека є державним завданням та, на нашу думку, полягає не тільки у відсутності загроз, які суб'єктивно сприймаються окремими особами і групами, а й в оцінці і підготовці особи-

стості та державних структур до інформаційних загроз.

У дослідженні ми виходили із взаємозв'язку базових понять «інформація», «інформаційна безпека» та «інформаційна культура». Інформація має властивість амбівалентності, тобто виступає одночасно у вигляді двох реальностей: об'єктивної та суб'єктивної. Згідно з першою інформація носить або атрибутивний, або функціональний характер. Згідно з другою інформація – компонент нашого буття, реальність, але не об'єктивна, а суб'єктивна, така, що належить до сфери ідеального. Вона нематеріальна, це спалах свідомості, що породжує образ реального світу.

В іншій термінології, що вживається деякими дослідниками, інформація має дві сторони: змістову і показну [6]. Суть змістової сторони інформації – віддзеркалення в свідомості людини навколишньої дійсності, включаючи повідомлення у формі психічних відчуттів. Ця сторона інформації залежить від фізіологічних особливостей рецепторів людини, її нервової системи, наявного досвіду осмислення тих або інших відчуттів, а також досвіду фіксації пізнавальних образів у мові, що веде до виникнення понятійного мислення. Суть показної сторони інформації визначають самі повідомлення, що передають психічні емоційні відчуття іншим людям. Показна сторона інформації залежить від здатності людини описувати свої відчуття деякою мовою, перетворювати описи на повідомлення і передавати їх іншим людям. Перетворення показної сторони інформації на змістову і навпаки становить суть загального закону поширення інформації.

Важливим складником показної сторони інформації є інформаційне середовище, що має, своєю чергою, дві складові частини: організаційну і технологічну. Організаційний складник включає виробництво засобів інформатизації та інформаційних послуг, інформаційний ринок, підготовку і перепідготовку кадрів, проведення наукових досліджень. Технологічний складник інформаційної інфраструктури утворюється інформаційно-телекомунікаційними системами.

Поняття «інформаційна безпека» визначається такими складниками, як: задоволення інформаційних потреб суб'єктів в інформаційному середовищі; безпека інформації; захист суб'єктів інформаційних відносин від негативного інформаційного впливу.

За такого підходу можна сформулювати таке визначення: *інформаційна безпека – стан інформаційного середовища, який забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин, безпеку інформації*

та захист суб'єктів від негативного інформаційного впливу. У цьому визначенні суб'єктами інформаційних відносин можуть бути держава, суспільство, організації, людина [8].

Основними принципами інформаційної безпеки є: забезпечення конфіденційності, доступності, цілісності й автентичності інформаційних ресурсів та інфраструктури, що її підтримує (рис. 1).

Доступність інформаційних ресурсів – це можливість за прийнятний час одержати необхідну інформаційну послугу, яка перебуває у вільному доступі. Інформація має надава-

тися повноправним користувачам ресурсів своєчасно і безперешкодно. Тому, не протиставляючи доступність решті аспектів, її можна виділити як найважливіший елемент інформаційної безпеки.

Цілісність інформаційних даних означає здатність інформації зберігати початковий вигляд і структуру як у процесі зберігання, так і після неодноразової передачі. Вносити зміни, видаляти або доповнювати інформацію вправі тільки власник або користувач з легальним доступом до даних. Цілісність виявляється найважливішим аспектом ІБ у тих випадках, коли інформація служить «керівництвом додії».

Конфіденційність – це захист від несанкціонованого доступу до інформації. У процесі дій і операцій інформація стає доступною тільки користувачам, які включені в інформаційні системи та успішно пройшли ідентифікацію.

Достовірність вказує на приналежність інформації довіреній особі або власнику, який одночасно виступає в ролі джерела інформації, це гарантія того, що джерелом інформації є саме та особа, яка заявлена як її автор. Достовірність інформації безпосередньо впливає на суспільну та індивідуальну свідомість, такою ж мірою на громадську думку і через це стає одним з основних принципів забезпечення інформаційної безпеки [1].

Вважаємо також за доцільне визначити та проаналізувати об'єктивні та суб'єктивні



Рис. 1. Основні принципи інформаційної безпеки

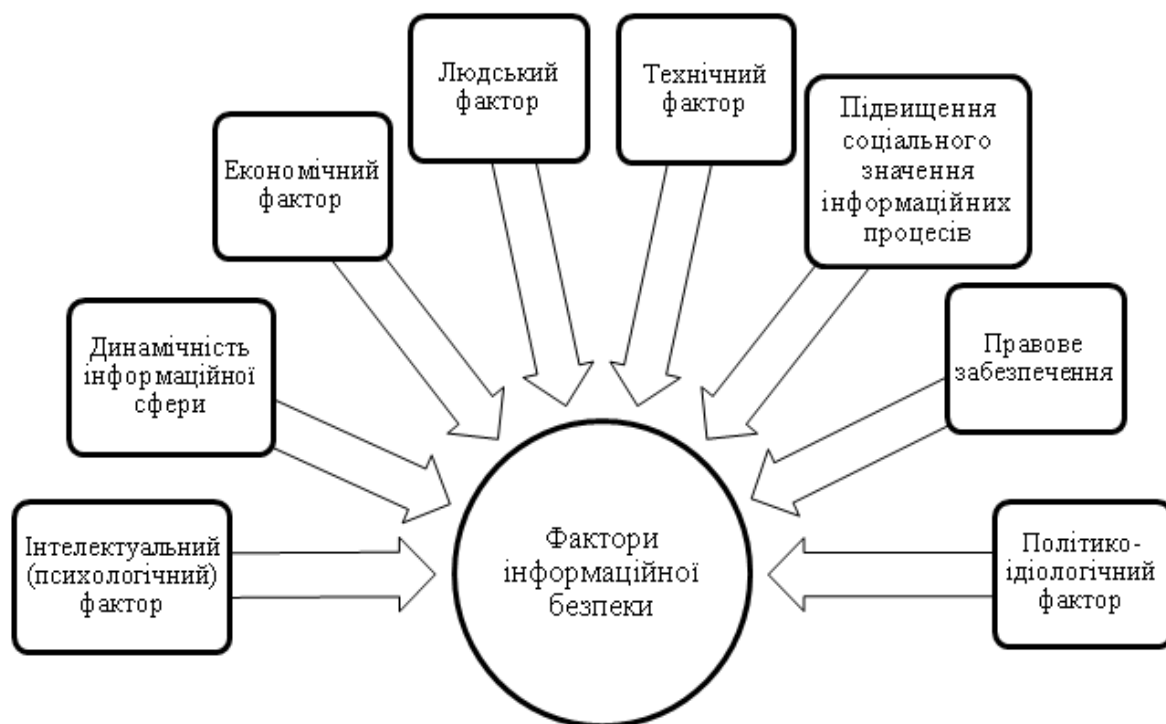


Рис. 2. Фактори інформаційної безпеки

фактори в контексті інформаційного розвитку суспільства та забезпечення інформаційної безпеки (рис. 2) [3; 4].

До інтелектуального (психологічного) фактору можна віднести такі характеристики української суспільної свідомості та явища негативного характеру, що у сукупності гальмують процеси інформаційного розвитку суспільства та забезпечення інформаційної безпеки, як: ірраціональність, консерватизм та апатичність суспільної свідомості; відсутність сформованості в загальносуспільній свідомості інформаційних потреб; відсутність усвідомленості інформаційних загроз; низький рівень правової свідомості громадян; падіння рівня загальної освіти і культури громадян; загальна поширеність правового нігілізму.

Ускладнює процеси утворення інформаційного права на всіх його етапах формування, формулювання та на етапі реалізації права. Стрімка динамічність інформаційної сфери потребує своєчасного розвитку законодавчої бази держави. Основними чинниками динамічності перетворень в інформаційній сфері є: стрімкий розвиток інформаційної сфери та інформаційно-комунікаційних технологій; підвищена складність і різноманітність суспільних відносин в інформаційній сфері; новизна інформаційних відносин та відсутність досвіду їх правового регулювання; відсутність загальноприйнятих варіантів поведінки в інформаційній сфері, вироблених суспільством [7].

Підвищення соціального значення інформаційних процесів В. Шульга [10] визначає як пріоритетність організаційно-забезпечувальної діяльності держави в інформаційній сфері, як основу подальшого розвитку суспільства, що підтверджується такими чинниками, як: всепроникливість інформаційних процесів; створення широких інформаційно-комунікативних можливостей; виникнення додаткових можливостей саморозвитку суб'єктів; виникнення нових особливо небезпечних загроз суспільній безпеці; безпрецедентне підвищення загальносоціального значення всіх складників інформаційної безпеки. Економічний фактор створює економічне підґрунтя інформаційного розвитку суспільства і держави та матеріально-технічні можливості впровадження інформаційно-комунікаційних технологій. Узагальненими чинниками економічного характеру, що визначають результативність процесу забезпечення інформаційної безпеки, є: відсутність стабільного зростання економіки; низький рівень забезпеченості широких верств населення всіма необхідними для розвитку матеріально-технічними засо-

бами; низький рівень забезпеченості апарату держави сучасними інформаційно-комунікаційними засобами; недостатність фінансування сфери освіти та науки.

Складники технічного фактору характеризують технічну досконалість і сучасність засобів обробки інформації, що визначає рівень технічної готовності до розгортання інформаційних процесів. Основними з них є: нерозвиненість мережі швидкісного Інтернету; недосконалість інформаційних ресурсів; застарілість автоматизованих систем обробки інформації.

Політико-ідеологічний фактор визначає рівень усвідомленості соціально сильними групами індивідів необхідності вирішення соціальних проблем та проблем інформаційної сфери. Як вважає С. Ковтун [3], до нього можна віднести: відсутність сталої, незалежної від політичних персон, стратегії становлення України на світовій арені; відсутність реальної, послідовної та виваженої державної програми соціального розвитку; неправовий характер діяльності державної влади; пріоритетність політичної доцільності над правовою; бюрократичність апарату держави; нерозвиненість громадянського суспільства; нерозвиненість інформаційних зв'язків між державою і суспільством тощо.

З точки зору О. Тихомирова [9], інформаційна безпека виступає об'єктом правового захисту. Правові засоби забезпечення інформаційної безпеки є провідним фактором захисту національних інтересів у цій сфері, а їх застосування визначається: оптимізацією балансу відносин між правом суб'єктів інформаційних відносин на отримання інформації та правом на встановлення обмежень таких відносин з боку інших осіб щодо відомостей, володарями яких вони є; розробкою та реалізацією правових заходів захисту інформації, доступ до якої має обмежуватися правовими підставами в процесі захисту інформаційних ресурсів. Правове забезпечення ліквідації загроз і ризиків у сфері інформаційної безпеки є основним фактором структурування, формування, розглядається як законотворча діяльність, що спрямована на запобігання шкоди інтересам особи, суспільства та держави в інформаційній сфері.

На думку багатьох авторів, у тому числі Д. Маркова [11], людський фактор заслуговує особливої уваги, тому що саме люди формують режим інформаційної безпеки, вони ж виявляються і головною загрозою. Слід усвідомити той ступінь залежності від комп'ютерної обробки даних, в який потрапило сучасне суспільство. Оскільки людина є споживачем

інформації та суб'єктом її обробки, завжди існував, існує і буде існувати ризик, пов'язаний з помилкою прийняття рішення.

Одним із пріоритетних завдань держави на етапі розвитку є визначення напрямів правового регулювання та створення правових гарантій, необхідних для самореалізації суб'єктів в інформаційній сфері. Більшість із перелічених факторів є загальними чинниками (джерелами) процесу утворення національного права і тому дають змогу розглядати процеси розвитку інформаційного права України в контексті проблем становлення правової системи України загалом.

Висновки. Підсумовуючи, зазначимо, що сутність інформаційної безпеки держави можна визначити як стан інформаційного середовища, який забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин, безпеку інформації та захист суб'єктів від негативного інформаційного впливу.

Інформаційна (інформаційно-психологічна) безпека особистості у сучасному суспільстві постає як нагальна проблема, яка потребує комплексного та системного вирішення. Суспільно значущі фактори державної інформаційної безпеки зумовлюють особливу важливість та пріоритетність різнопланової високопрофесійної державної діяльності в інформаційній сфері, юридичного її забезпечення, а також виваженого вибору методів правового регулювання.

ЛІТЕРАТУРА:

1. Довнар Н.Н. Достоверность информации как фактор обеспечения информационной безопасности. *Вестник ЮУрГУ. Серия «Право»*. 2015. Т. 15, № 1. С. 57–62.
2. Захаренко К. Основні суб'єкти та інститути інформаційної безпеки. *Науковий вісник. Серія «Філософія»*. Харків : ХНПУ. 2017. Вип. 48 (частина I). С. 212–219.
3. Ковтун С.В. Інформаційна безпека : підручник. Харків : Вид. ХНЕУ, 2009. 368 с.
4. Кустовська О.В. Методологія системного підходу та наукових досліджень : курс лекцій. Тернопіль : Економічна думка, 2005. 124 с.
5. Марущак А.І. Дослідження проблем інформаційної безпеки у юридичній науці. *Правова інформатика*. 2010 № 3(27). С. 17–21.
6. Муравська (Якубівська) Ю.Є. Інформаційна безпека суспільства: концептуальний аналіз. *Економіка і суспільство*. 2017. Вип. № 9. С. 289–294.
7. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : Видавничий дім «Гельветика», 2017. 168 с.
8. Панченко О.А. Информационная безопасность личности : монография / О.А. Панченко, Н.В. Банчук. Киев : КИТ, 2011. 672 с.
9. Тихомиров О. Забезпечення інформаційної безпеки: теоретико-правовий аспект. *Право України*. 2011. № 4. С. 252–259.
10. Шульга В.І. Сучасні підходи до трактування поняття «інформаційна безпека». *Ефективна економіка*. 2015. № 4. URL: <http://www.economy.nayka.com.ua/?op=1&z=5514>.
11. Маркова Д.Г. Человеческий фактор в информационной безопасности. *Известия ТулГУ. Технические науки*. 2018. Вып. 10. С. 149–152.