

УДК 343.123(477)

## ТЕОРЕТИЧНИЙ ДИСКУРС ПОШУКУ ОСНОВНИХ СКЛАДОВИХ ЧАСТИН СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

**Тарас ТКАЧУК,**

кандидат юридичних наук, доцент, заступник завідувача кафедри організації захисту інформації з обмеженим доступом  
Навчально-наукового інституту інформаційної безпеки  
Національної академії Служби безпеки України

### АНОТАЦІЯ

У статті досліджується зміст категорії «інформаційна система безпеки» та визначаються компоненти цієї системи, а також обґрунтовується необхідність розмежування системи захисту інформації та системи забезпечення інформаційної безпеки.

**Ключові слова:** інформаційна безпека, забезпечення інформаційної безпеки, національна безпека, держава, процес, загроза.

### THEORETICAL DISCUSSION FOR THE SEARCH OF THE MAIN COMPLEXES OF THE SYSTEM OF INFORMATION SECURITY OF THE STATE

**Taras TKACHUK,**

Candidate of Law, Associate Professor, Deputy Head of the Department of Protection of Information Protection with Restricted Access of Educational and Scientific Institute of Information Security of the National Academy of Security Service of Ukraine

### SUMMARY

The article explores the content of the category "information security system" and determines the components of this system, and also substantiates the need to delimit the information security system and the information security ensuring system.

**Key words:** information security, information security ensuring, national security, state, process, threat.

### REZUMAT

Articolul explorează conținutul categoriei "sistem de securitate a informațiilor" și determină componentele acestui sistem și susține, de asemenea, necesitatea de a diferenția sistemul de securitate a informațiilor și sistemul de securitate a informațiilor.

**Cuvinte cheie:** securitatea informațiilor, securitatea informațiilor, securitatea națională, starea, procesul, amenințarea.

**Постановка проблеми.** Сьогодні в Україні закладена основа правового регулювання забезпечення національної безпеки й інформаційної безпеки зокрема, завдяки чому одержали своє законодавче закріплення основні поняття в області національної безпеки, а також правове обґрунтування системи її забезпечення. Водночас основні нормативно-правові акти у сфері інформаційної безпеки вимагають доопрацювання, зокрема в аспекті визначення й законодавчого закріплення поняття й змісту категорії «система інформаційної безпеки», а також розробки теоретичних і правових засад забезпечення інформаційної безпеки України.

**Стан дослідження.** Проблематика інформаційної безпеки та її забезпечення у різних аспектах досліджувалися у наукових працях Х. Андерсена, О. Баранова, Н. Влажика, В. Горбуліна, В. Гурковського, О. Дзьобаня, О. Довганя, Г. Ємельянова, Р. Каложного, Б. Кормича, Дж. Кріка, В. Ліпкана, В. Лопатіна, Р. Максутова, А. Марущака, А. Нашінець-Наумової, М. Нієлса, В. Остроухова, М. Панова, М. Потрубача, Г. Почепцова, С. Расторгуєва, В. Рубана, С. Стрельцова, О. Тихомирова, М.-Дж. Шварца та інших вітчизняних та зарубіжних дослідників. Водночас слід констатувати, що в сучасній науковій літературі та на законодавчому рівні поки не склалося єдиного підходу до розуміння системи інформаційної безпеки держави.

**Метою статті** є дослідити зміст категорії «система інформаційної безпеки» та визначити складові частини відповідної системи.

**Виклад основного матеріалу.** На методологічному рівні предметна сфера інформаційної безпеки є єдиною структурованою за завданнями та предметом дослідження, збалансованою за терміносистемою. Її системотвірним чинником, безумовно, виступають інформація та інформаційні процеси. Втім, для виокремлення складових частин інформаційної безпеки на доктринальному рівні використовується досить широкий спектр критеріїв, що зумовлює диференціацію підходів до розуміння системного змісту поняття «інформаційна безпека».

У зарубіжних наукових джерелах під системою інформаційної безпеки зазвичай розуміють систему безпеки інформації у складі таких структурних елементів, як цілісність, доступність та конфіденційність інформації [1–3]. Під цілісністю інформації розуміють її властивість не бути модифікованою неавторизованим користувачем і (або) процесом, тобто зберігатися у стані, визначеному її створювачем та законним володільцем, у т. ч. і достовірність інформації як її відповідність дійсності в аспекті адекватності відображення. Конфіденційність означає властивість інформації бути недоступною користувачам, які не мають на це права. Ця властивість пов'язана з розмежуванням

інформації за режимом доступу. Доступність інформації полягає в тому, що уповноважений користувач може використовувати її відповідно до правил, встановлених політикою безпеки, не очікуючи більше заданого проміжку часу, тобто це властивість інформації міститися у необхідному користувачеві вигляді та місці, в той час, коли вона йому необхідна [4, с. 190]. Однак відповідні характеристики не можуть надати уявлення про систему інформаційної безпеки як складової частини національної безпеки.

Гуманітарна складова частина інформаційної безпеки містить у собі величезну сукупність проблем, пов'язаних із дотриманням конституційних прав і свобод громадян у сфері духовного розвитку й інформаційної діяльності. Тож безпеку інформаційної сфери не можна сприймати суто як захист телекомунікаційних мереж або мереж зв'язку, засобів масової інформації від проникнення небажаної або шкідливої інформації. Необхідність дослідження загроз інформаційній безпеці людини з погляду її інформаційних прав та свобод підкреслює О. Золотар, наголошуючи на тому, що інформаційна безпека людини передбачає в т. ч. реалізацію життєво важливих інтересів людини та гармонійний розвиток в умовах інформаційного суспільства незалежно від наявності інформаційних загроз [5, с. 77].

Отже, оскільки метою забезпечення інформаційної безпеки є передусім попередження шкідливих інформаційних впливів та неправомірних дій щодо інформаційних ресурсів та інформаційних систем (біологічних, соціальних та технічних), захист прав та забезпечення реалізації інтересів суб'єктів інформаційної сфери, а також забезпечення захищеності істотних властивостей інформації, нами вже обґрунтовувалася думка, що система інформаційної безпеки складається з безпеки інформації, безпеки від інформаційних впливів, а також захисту інформаційних прав та належного порядку реалізації інтересів суб'єктів інформаційної сфери [6, с. 155].

Безпека інформації як захищеність її основних властивостей має забезпечуватися не лише щодо інформації з обмеженим доступом, але й щодо іншої інформації, оскільки має бути відвернена загроза не лише порушення конфіденційності інформації, але й порушення її цілісності та достовірності, а також доступності. Під безпекою від інформаційних впливів слід розуміти безпеку інформаційних систем та зв'язків між ними від інформаційних впливів, що здатні спричинити шкоду, в т. ч. й інформаційно-психологічну безпеку людини та суспільства. Забезпечення інформаційно-психологічної безпеки полягає в мінімізації негативних впливів на свідомість людини та суспільства, пов'язаних передусім із маніпулюванням свідомістю з різною метою і поширенням суспільно небезпечної інформації, в т. ч. деструктивної ідеології (культу насильства та жорстокості, расизму, радикального націоналізму, порнографії тощо) [7, с. 70–71]. Захист інформаційних прав та забезпечення реалізації інтересів суб'єктів інформаційної сфери як підсистема інформаційної безпеки пов'язаний із двома іншими її складовими частинами, оскільки йдеться передусім про потребу у безпечному інформаційному середовищі та цивільні права на інформацію.

Якщо мовиться про інформаційну безпеку як про інформаційний вимір національної безпеки, мається на увазі стан не окремих структур, сторін або відносин нації, а її здатність ефективно функціонувати, всупереч негативним факторам, не поступатися своїми інтересами під тиском зовнішніх, внутрішніх або комплексних загроз. Таким чином, категорія «інформаційна безпека» на національному рівні повинна стосуватися країни, держави, що розуміється як органічна єдність території, населення й влади, і тлумачиться на холистичних засадах, виходячи з якісної своєрідності цілого стосовно до його частин. Ця своєрід-

ність полягає в тому, що інформаційна безпека країни припускає й означає інформаційну безпеку всіх її структур і утворень, але допускає можливе ослаблення її для деяких з них. Зміцнення інформаційної безпеки окремих об'єктів, сегментів або сфер, узятих окремо, важливе для інформаційної безпеки як складової частини національної безпеки (її інформаційного виміру), але не створює її.

Отже, інформаційна безпека виступає як стан і умови життєдіяльності соціуму, які забезпечують сприятливі умови для розвитку особистості, суспільства й держави, а так само й інших об'єктів, тоді як інформаційна безпека кожного з цих об'єктів окремо виступає не як її частини, а як її мета та результат. У широкому сенсі інформаційна безпека повинна включати такі проблеми, як протистояння культурній експансії з боку країн із розвиненою аудіовізуальною промисловістю, збереження національної і мовної самобутності, нейтралізацію впливу недоброякісної, недостовірної, хибної інформації (дезінформації) на реалізацію національних інтересів. Слід звернути увагу й на те, що «безпека взагалі» не існує, адже атрибутом існування об'єкта будь-якої природи є наявність загроз, відтак модель системи інформаційної безпеки припускає визначення того, кому, що, чим загрожує, а також можливі механізми й способи протидії загрозовим факторам.

Необхідно також враховувати, що зміст інформаційної безпеки не можна зводити тільки до захищеності – він значний ширший. Забезпечення безпеки передбачає не тільки збереження певного наявного стану, але й створення можливостей для виходу на новий, якісно вищий рівень розвитку. Відповідно, безпека – не стільки незмінний стан об'єкта, скільки його здатність відтворюватися, розбудовуватися, стало і прогресивно розвиватися в умовах конфліктів, невизначеності та ризику. Так само неприйнятним є визначення інформаційної безпеки як «захищеності інтересів», адже інтереси – це потреби, без задоволення яких нормальне існування соціуму неможливе, тож їх потрібно не захищати, а реалізовувати. Захисту потребують цінності, необхідні для нормальної життєдіяльності людини, суспільства, держави, і умови, що забезпечують їхній доступ до цих цінностей і можливість користуватися ними. Безпека припускає, насамперед, наявність необхідних цінностей і доступу до них. Відсутність цінностей вимагає пошуку їх нових джерел або їх заміників, а ускладнений доступ до них – усунення перешкод або вжиття заходів для їхнього подолання, що, у свою чергу, визначає зміст категорії «національні цілі».

Таким чином, інформаційну безпеку України слід визначити як стан, за якого в умовах дії різнопланових загроз забезпечується самозбереження, сталий і прогресивний розвиток інформаційної сфери, в т. ч. захищеність національних цінностей, необхідних для існування суверенної Української держави та виконання нею своїх функцій, а також досягнення відповідних національних цілей та реалізація національних інтересів. Інформаційна сфера утворюється сукупністю:

- суб'єктів інформаційних процесів;
- інформаційної інфраструктури;
- інформаційного простору;
- інформаційних ресурсів;
- суспільних відносин, що складаються у зв'язку з формуванням, зберіганням, передачею та розповсюдженням інформації.

За такого визначення система інформаційної безпеки з погляду її об'єктів відповідає класичній формулі для об'єктів національної безпеки «територія – народонаселення – система державного управління», однак замість території для інформаційної безпеки вважаємо за доцільне використовувати поняття «інформаційний простір», яке в

т. ч. охоплюватиме інформаційну модель території та її інформаційне обслуговування.

На нашу думку, розмежування інформаційної безпеки як стану динамічної системи та забезпечення інформаційної безпеки як процесу підтримання цього стану (включаючи самовідтворення, збереження та розвиток) дозволяє певним чином зняти протиріччя між організаційно-структурним і функціонально-діяльним підходами до визначення сутності феномену інформаційної безпеки та її системи. Тож система інформаційної безпеки як певне утворення, що характеризується подільністю, відкритістю, адаптивністю та наявністю структури, мети й пріоритетів оптимальної взаємодії елементів [8, с. 86], виступає об'єктом для системи забезпечення інформаційної безпеки, до якої також входять сили й засоби забезпечення інформаційної безпеки.

**Висновки.** Відповідно до ст. 17 Конституції України, захист інформаційної безпеки, нарівні із захистом суверенітету та територіальної цілісності України, є найважливішою функцією держави та справою всього українського народу [9], тож інформаційна безпека, безперечно, є однією з найважливіших складових частин національної безпеки України. Оскільки інформаційна сфера має своїм змістом знання про інші сфери життєдіяльності суспільства, вона одночасно існує як самостійно, так і у взаємозв'язку з іншими сферами життєдіяльності суспільства, адже здійснює їх «інформаційне обслуговування» за допомогою інформації. Це зумовлює виняткове значення інформаційної сфери та загроз, що на неї спрямовані.

Складна воєнно-політична, оперативно-стратегічна та економічна ситуація, яка склалася внаслідок збройної агресії Росії проти України, окупації і анексії частини суверенної території України, проведенням антитерористичної операції в окремих регіонах Донецької та Луганської областей, де триває інспірований та підтриманий Російською Федерацією збройний конфлікт, набуває загрозливих проявів також у інформаційному просторі. У сукупності зі стратегічним значенням інформаційної сфери для сталого розвитку сучасного суспільства це зумовлює пріоритетний характер інформаційної безпеки у системі національної безпеки України. Відповідно, надзвичайно важливим є правильне усвідомлення змісту категорії «система інформаційна безпека».

Отже, з урахуванням викладеного, інформаційну безпеку держави слід визначати як постійний процес діяльності компетентних органів, направлений на попередження, протидію загрозам в інформаційній сфері, а також застосування активних заходів інформаційного впливу та сукупність умов такої діяльності, які реалізуються й здатні контролюватися тривалий час. Оскільки під дією інформаційних впливів може цілеспрямовано змінюватися світогляд та мораль як окремих осіб, так і суспільства в цілому, нав'язуватися чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності та форм проявів сучасних методів прихованого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які суперечать інтересам національної безпеки, вироблення механізмів протидії їм у всіх напрямках, інформаційна безпека держави включає в себе не тільки захист, а й уміння та здатність створювати інформаційні загрози противнику. Також слід зазначити, що комплексне функціональне визначення інформаційної безпеки як постійного процесу діяльності компетентних органів, направлено на попередження, протидію загрозам в інформаційній сфері, а також застосування активних заходів інформаційного впливу та сукупності умов такої діяльності, які реалізуються й здатні контролюватися тривалий час, дозволяє виділити пасивну (протидія інформаційним загрозам) та активну складову

частини (створення інформаційних загроз) інформаційної безпеки. У складі визначених вище компонентів – безпеки інформації, безпеки «від інформації» та належного порядку реалізації прав та інтересів суб'єктів інформаційної сфери, щодо яких триває постійний процес протидії інформаційним загрозам та створення інформаційних загроз супротивнику, – поняттям інформаційної безпеки охоплюється не лише захищеність інформаційної сфери, що є передумовою її належного функціонування, але й можливість справляння суб'єктами інформаційної сфери необхідних впливів на інші сфери життєдіяльності суспільства, взаємодії з останніми.

Нормативне закріплення системного характеру та змісту складових частин інформаційної безпеки не лише сприятиме більш коректному усвідомленню її сутності суб'єктами інформаційної сфери, але й забезпечить гармонійний розвиток законодавства у відповідній сфері та підвищить ефективність правового забезпечення інформаційної безпеки України. За відсутності такого концептуального визначення не можуть бути адекватно сформульовані визначення безпеки інформації, кібербезпеки тощо.

#### Список використаної літератури:

1. Nieves M., Dempsey K., Yan Pillitteri V. An Introduction to Information Security. URL: <https://doi.org/10.6028/NIST.SP.800-12r1>.
2. National Security Telecommunications and Information Systems Security. National Training Standard for Information Systems Security (Infosec). URL: [www.cnss.gov/Assets/pdf/nstissi\\_4011.pdf](http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf).
3. Federal Financial Institutions Examination Council (FFIEC). Information Technology Examination Handbook (IT Handbook): Information Security URL: [https://www.ffiec.gov/press/pdf/ffiec-it-handbook\\_information\\_security\\_booklet.pdf](https://www.ffiec.gov/press/pdf/ffiec-it-handbook_information_security_booklet.pdf).
4. Мельник С.В. Понятійно-категоріальний апарат у системі професійної підготовки майбутніх фахівців з кібербезпеки. Інформаційні технології і засоби навчання. 2016. Т. 55. № 5. С. 187–197.
5. Золотар О.О. Загрози інформаційній безпеці людини. Правова інформатика. 2014. № 2 (42). С. 70–79.
6. Ткачук Т. Складники інформаційної безпеки: аналіз критеріїв. Visegrad journal on human rights. 2017. № 4. С. 153–158.
7. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави: монографія / заг. ред. Р.А. Калужний. Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.
8. Могилевский В.Д. Системная безопасность: формализованный подход. Материалы конференции «Проблемы внутренней безопасности России в XXI веке». М.: ЭДАС-ПАК, 2001. С. 86–89.
9. Конституція України від 28 червня 1996 р. URL: [zakon5.rada.gov.ua/laws/show/254k/96-vp](http://zakon5.rada.gov.ua/laws/show/254k/96-vp).

#### ДОВІДКА ПРО АВТОРА

**Ткачук Тарас Юрійович** – кандидат юридичних наук, доцент, заступник завідувача кафедри організації захисту інформації з обмеженим доступом Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України

#### INFORMATION ABOUT THE AUTHOR

**Tkachuk Taras Yuriiovich** – Candidate of Law, Associate Professor, Deputy Head at the Department of Protection of Information Protection with Restricted Access of Educational and Scientific Institute of Information Security of the National Academy of Security Service of Ukraine

[tarast25@gmail.com](mailto:tarast25@gmail.com)