

КЛАСИФІКАЦІЇ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Тихомиров О.О., ст. викладач

Національна академія Служби безпеки України

Стаття присвячена проблемі класифікації діяльності по забезпеченню інформаційної безпеки. Її вирішення сприятиме усвідомленню комплексного характеру забезпечення інформаційної безпеки та формуванню виваженої державної інформаційної політики.

Ключові слова: інформаційна безпека, забезпечення інформаційної безпеки, захист інформації.

Тихомиров А.А. КЛАССИФИКАЦИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ / Национальная академия Службы безопасности Украины, Украина

Статья посвящена проблеме классификации обеспечения информационной безопасности. Ее решение будет способствовать осознанию комплексного характера обеспечения информационной безопасности и формированию взвешенной государственной информационной политики.

Ключевые слова: информационная безопасность, обеспечение информационной безопасности, защита информации.

Tihomirov A.A. CLASSIFICATIONS OF PROVIDING INFORMATIONAL SECURITY / National academy of Security service of Ukraine, Ukraine

The article is devoted to the problem of classification informational security. Its solving should assist to realize the complex character of providing informational security and form suspended state informational policy.

Key words: informational security, providing informational security, protection of information.

Сьогодні інформаційна сфера складає інтегруючу основу життєдіяльності суспільства, а забезпечення інформаційної безпеки визнається однією з концептуальних засад його подальшого розвитку. За таких умов особливого значення набуває формування виваженої державної інформаційної політики, на основі системних наукових досліджень явищ інформаційної сфери, провідне місце серед яких займає інформаційна безпека.

Одним з важливих етапів системного дослідження інформаційної безпеки є глибокий аналіз загальної структури її забезпечення. Виокремлення та деталізація складових забезпечення інформаційної безпеки за різними ознаками сприятиме усвідомленню особливостей кожної з них, і, відповідно, формуванню комплексу адекватних заходів державного та недержавного характеру, спрямованих на підтримання оптимального інформаційного розвитку України та інтеграції у світовий інформаційний простір.

Інформаційна безпека протягом двох останніх десятиліть є об'єктом актуальних наукових досліджень у різних сферах знань. Аналіз *останніх досліджень і публікацій* свідчить, що загальнотеоретичні та окремі аспекти забезпечення інформаційної безпеки висвітлені на монографічному та дисертаційному рівні. Серед розробників цієї проблеми такі вітчизняні та зарубіжні дослідники, як Я.С. Артамонова, Г.А. Атаманов, М.І. Бусленко, М.Ю. Захаров, О.Ю. Колесов, В. К. Конах, Б.А. Кормич, О.О. Левін, О.В. Логінов, В.М. Лопатін, Ю.Є. Максименко, Т.А. Мартиросян, Н.А. Полянська, Д.В. Сорокін, А.О. Стрельцов та інші.

Водночас слід зазначити, що залишаються недостатньо розкритими питання особливостей загальної структури забезпечення інформаційної безпеки. Оскільки це гальмує процеси усвідомлення системності інформаційної безпеки та негативно позначається на формуванні державної інформаційної політики, то ми поставили за *мету* здійснити спробу декомпозиції такого явища, як забезпечення інформаційної безпеки та встановити підстави його класифікації.

Забезпечення інформаційної безпеки, поряд із захистом суверенітету і територіальної цілісності, визнається однією з найважливіших функцій держави і справою всього Українського народу (ст.17 Конституції України). Ґрунтуючись на цьому, забезпечення інформаційної безпеки доцільно розглядати як цілеспрямовану діяльність, провідним, але не єдиним елементом об'єктно-суб'єктного складу якої є держава. Така інтерпретація враховує синергетичні тенденції розвитку сучасного суспільства і в повній мірі відповідає положенням теорії держави і права, згідно з якою функції держави розуміються як напрями, сторони або види державної діяльності.

Слово «забезпечення» має подвійне семантичне значення: 1) надання, створення засобів та умов, гарантування, захист; 2) засоби або система засобів [1, 375]. Названі аспекти, хоча і відповідають загальноприйнятому тлумаченню забезпечення, але, з точки зору теорії діяльності, не є рівнозначними. Засоби діяльності обов'язково знаходять свій прояв у змістовних елементах, що складають незмінну основу самої діяльності [2, 89]. Залежно від широти розгляду конкретного виду діяльності, засоби можуть виступати як самостійним елементом її змісту, так і знаходити свій вираз в інших елементах – меті, завданнях та результатах діяльності. Організаційну діяльність держави узагальнено можна представити у двох стадіях: перша – створення необхідних засобів та забезпечення ними відповідних суб'єктів, друга – використання засобів суб'єктами для досягнення вищої мети. У такому аспекті розгляду засоби як такі, є завданнями та результатом на шляху досягнення загальної мети.

Системний характер інформаційної безпеки дозволяє визначити її забезпечення як складний, комплексний вид діяльності, що висуває особливі вимоги до його структурної характеристики. Наукові дослідження не виробили загальноприйнятого механізму структуризації забезпечення інформаційної безпеки. Для виокремлення складових його загальної структури найчастіше використовуються такі конструкції, як «напрями», «механізми» та «шляхи» забезпечення. Однак саме розуміння забезпечення інформаційної безпеки як комплексного виду діяльності дозволяє гармонізувати термінологію і здійснювати не лише структурний, а й глибокий змістовний аналіз, повною мірою застосовуючи потенціал діяльнісного підходу.

Результати аналізу різноманітних джерел свідчать про недостатню розробленість та систематизованість структурних складових забезпечення інформаційної безпеки. На нормативно-правовому рівні практично безальтернативним залишається підхід, у межах якого, залежно від пріоритетних загроз, визначаються напрями забезпечення інформаційної безпеки, об'єднані за традиційними сферами життєдіяльності. Доктрина інформаційної безпеки України, Доктрина інформаційної безпеки Російської Федерації, а також фундаментальні нормативно-правові акти у сфері забезпечення національної безпеки використовують саме такий підхід. У наукових дослідженнях пріоритет надається класифікації загроз як чинників, що зумовлюють основні напрями або шляхи забезпечення інформаційної безпеки. Між тим, не менш важливим є класифікаційна характеристика самого забезпечення інформаційної безпеки не лише на підставі предмету діяльності (загрози), а й інших критеріїв, що дозволить отримати більш повну уяву щодо його особливостей.

У контексті сприйняття забезпечення інформаційної безпеки як цілісного явища кожен обраний критерій класифікації пропонується інтерпретувати не як підставу диференціації, а як ознаку, що задає окрему площину розгляду. Застосування такого прийому дозволяє створити багаторівневу модель забезпечення інформаційної безпеки, не порушуючи системних взаємозв'язків його складових.

Загальну частину класифікації складають видові групи, які виокремлено на основі сукупності самостійних критеріїв, що стали вже традиційними і можуть бути проаналізовані на прикладі інформаційного законодавства України та Російської Федерації.

За сферами суспільного життя:

- забезпечення інформаційної безпеки в економічній;
- забезпечення інформаційної безпеки в політичній;
- забезпечення інформаційної безпеки в оборонній;
- забезпечення інформаційної безпеки в екологічній;
- забезпечення інформаційної безпеки в соціальній сфері тощо [3; 4].

Підтвердженням важливості такого розподілу є зосередження на ньому уваги в численних наукових дослідженнях і багатьох нормативно-правових актах концептуального та доктринального рівня, що стосуються інформаційної та національної безпеки. Національним законодавством інформаційна безпека визначається як невід'ємна складова кожної зі сфер

національної безпеки, що закріплено Законом України «Про Концепцію Національної програми інформатизації» та Доктриною інформаційної безпеки України.

За аспектами розуміння інформаційної безпеки:

- забезпечення інформаційно-психологічної безпеки;
- забезпечення інформаційно-технічної (технологічної) безпеки;
- забезпечення інформаційної безпеки у сфері прав і свобод людини.

Даний контекст розгляду достатньо поширений у роботах російських та українських дослідників, причому особливої популярності останнім часом набуває виокремлення забезпечення інформаційної безпеки у сфері прав і свобод людини та дослідження його особливостей [5, 57].

За видами інформаційної діяльності:

- забезпечення одержання інформації у встановленому порядку;
- забезпечення можливостей використання інформації;
- забезпечення законного поширення інформації;
- забезпечення належного зберігання інформації;
- захист інформації [6].

Види інформаційної діяльності безпосередньо визначені та розкриті ст.14 Закону України «Про інформацію», а державна діяльність, що відповідає цим видам, згідно зі ст.6 цього ж закону, складає основу державної інформаційної політики.

За напрямками пізнавального процесу в інформаційній сфері:

- професійна інформаційна освіта;
- наукові дослідження інформаційної сфери;
- просвітницько-інформаційне виховання [6].

Комплексність підходів до інформаційної безпеки та пов'язаних з нею проблем зумовлює обов'язкове виділення особливої діяльності, що закладає інтелектуальні підвалини успішного розвитку національних інформаційних систем. Такою діяльністю є професійна освіта та організація наукових досліджень у галузі інформаційної діяльності, визначена ст.15 та ст.16 Закону України «Про інформацію».

За основними стадіями діяльності з протидії загрозам в інформаційній сфері:

- моніторинг інформаційної сфери (аналіз факторів впливу на інформаційну сферу, виявлення серед них загроз);
- ранжування загроз (встановлення пріоритетності загроз);
- профілактика і попередження негативного впливу загроз;
- безпосередня протидія загрозам.

Загроза як фактор негативного впливу, що зумовлює напрями державної діяльності по забезпеченню безпеки, є традиційною підставою її «горизонтальної» структуризації. Видова група, сформована залежно від стадій діяльності по протидії загрозам в інформаційній сфері є детермінантою «вертикальної» структури та відображає процес здійснення протидії загрозам.

За загальним змістом державного забезпечення інформаційної безпеки:

- інформування (надання суб'єктам необхідної для функціонування та життєдіяльності якісної інформації);
- інформатизація як цілеспрямована діяльність держави (створення політичних, економічних, технічних та інших умов для інформаційного розвитку суб'єктів, розвитку державного інформаційного ресурсу та оптимізації обміну інформацією);

- унормування поведінки суб'єктів в інформаційній сфері (правова регламентація сфери інформаційних відносин);
- боротьба з правопорушеннями в інформаційній сфері.

В означеному контексті розгляду узагальнений зміст державного забезпечення інформаційної безпеки може інтерпретуватися як система державних гарантій в інформаційній сфері, прямо чи опосередковано визначених фундаментальними нормативно-правовими актами, що регламентують інформаційну сферу суспільних відносин. Зміст цих гарантій міститься зокрема в положеннях Закону України «Про Концепцію Національної програми інформатизації», Доктрини інформаційної безпеки України, Доктрини інформаційної безпеки Російської Федерації та ін. [3; 4; 7].

Окреме важливе місце в класифікації займає блок, що визначається змістовними елементами забезпечення інформаційної безпеки та їх характеристиками:

- *за об'єктами інформаційної безпеки:*
 - забезпечення інформаційної безпеки особи;
 - забезпечення інформаційної безпеки суспільства;
 - забезпечення інформаційної безпеки держави [3];
- *за суб'єктами забезпечення інформаційної безпеки:*
 - міжнародне забезпечення (сприяння міжнародному співробітництву в галузі інформації, гарантування інформаційного суверенітету держави; сприяння задоволенню інформаційних потреб громадян за кордоном);
 - державне забезпечення (діяльність державних організацій спрямована на забезпечення інформаційної безпеки);
 - недержавне забезпечення (діяльність громадських організацій та індивідів спрямована на забезпечення інформаційної безпеки) [3];
- *за характером предмета діяльності по забезпеченню інформаційної безпеки:*
 - протидія негативним процесам та явищам (загрозам, небезпекам);
 - сприяння посиленню позитивних процесів;
 - сприяння трансформації нейтральних процесів у позитивні;
- *за характером здійснення впливу:*
 - безпосереднє створення необхідних умов для життєдіяльності суб'єктів в інформаційній сфері;
 - опосередкований вплив шляхом підняття інформаційного потенціалу суб'єктів та сприяння їх самоорганізації;
- *за засобами забезпечення інформаційної безпеки:*
 - правова регламентація відносин в інформаційній сфері;
 - контрольно-наглядова діяльність;
 - інженерно-технічне забезпечення;
 - матеріально-технічне забезпечення.

Посиленої уваги привертають особливості діяльності по розмежуванню доступу до інформації, захисту інформації з обмеженим доступом та розповсюдження відкритої інформації. На основі положень Закону України «Про державну таємницю» та проекту Закону України «Про доступ до публічної інформації» можна здійснити наступний розподіл:

- *залежно від правового режиму інформації:*
 - забезпечення режиму доступу до інформації з обмеженим доступом;

- забезпечення оптимального обміну відкритою інформацією;
- забезпечення належного розповсюдження публічної інформації [8; 9];
- *за заходами по захисту інформації (секретної):*
 - інженерно-технічне забезпечення;
 - організаційно-правове забезпечення;
 - оперативно-розшукове забезпечення;
 - криптографічне забезпечення [8].

Підводячи *підсумки вищезазначеного*, слід констатувати, що міждисциплінарний характер інформаційної безпеки, який охоплює технічні (технологічні), правові, психологічні аспекти, зумовлює надзвичайну складність та багаторівневість системних зв'язків складових забезпечення інформаційної безпеки. Застосування прийомів класифікації, використаних у даній статті, є спробою здійснення структурного аналізу забезпечення інформаційної безпеки в різних площинах розгляду, не порушуючи взаємозв'язків його складових. Усвідомлення особливостей кожної з них на основі системного аналізу сприятиме в подальшому процесам осягнення комплексності забезпечення інформаційної безпеки, формування комплексу тактичних та стратегічних напрямків діяльності у сфері забезпечення інформаційної безпеки, гармонізації національного інформаційного законодавства, що в сукупності створює важливі засади ефективної державної інформаційної політики.

ЛІТЕРАТУРА

1. Великий тлумачний словник сучасної української мови (з дод., допов. та CD) / [уклад. і голов. ред. В.Т. Бусел]. – К.; Ірпінь: ВТФ «Перун», 2009. – 1736 с.: іл.
2. Гусарев С.Д. Юридична діяльність: методологічні та теоретичні аспекти / С.Д. Гусарев. – К.: Знання, 2005. – 357 с.
3. Про Доктрину інформаційної безпеки України: Указ Президента України від 08.07.2009 № 514/2009 / [Електронний ресурс]. – Режим доступу: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=514%2F2009>.
4. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 № 75/98-ВР / [Електронний ресурс]. – Режим доступу: <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=75%2F98-%E2%F0>.
5. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України: дис. ... кандидата юрид. наук: 12.00.01 / Максименко Ю.Є. – К., 2007. – 186 с.
6. Про інформацію: Закон України від 02.10.1992 № 2657-ХІІ / [Електронний ресурс]. – Режим доступу: <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12>.
7. Доктрина информационной безопасности Российской Федерации / [Электронный ресурс]. – Режим доступа: <http://www.gtk.lissi.ru/doc.phtml?DocumentID=39>.
8. Про державну таємницю: Закон України від 21.01.1994 № 3855-ХІІ / [Електронний ресурс]. – Режим доступу: <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?page=1&nreg=3855-12>.
9. Про доступ до публічної інформації: проект Закону України від 13.01.2011 № 2939-VI / [Електронний ресурс]. – Режим доступу: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi>.