

ОРГАНІЗАЦІЙНО-ПРАВОВІ ФОРМИ ТА МЕТОДИ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

§ 1 Основні форми політики інформаційної безпеки

Закон України «Про основи національної безпеки України» (ч. 2 ст. 5) визначає, що «національна безпека України досягається шляхом проведення виваженої державної політики»¹. Таким чином, саме політика називається головним інструментом досягнення необхідних безпечних умов суспільного і державного життя. До того ж акцент робиться саме на державній політиці, тобто такій, яка проводиться від імені держави її владними органами. Взагалі, на питаннях розстановки акцентів ми зупинялися у підрозділі, присвяченому структурі інституціонального механізму, і наголошували на важливості недержавного сегмента політики інформаційної безпеки. Але разом з тим і підкреслювали, що цей недержавний елемент повинен реалізовуватися насамперед через механізми держави. І це не дивно, адже саме в арсеналі державних засобів проведення політики є всім відомий інструмент державного примусу, який найчастіше й асоціюється з такими термінами, як «захист», «безпека» тощо.

Таким чином ми підходимо до розгляду тих форм і методів, у вигляді та за допомогою яких політика інформаційної безпеки повинна досягати своєї конкретної мети.

Знову ж таки вже згаданий Закон України «Про основи національної безпеки» дає на це запитання досить широку відповідь, вказуючи, що «вибір конкретних засобів і шляхів забезпечення національної

¹ Закон України «Про основи національної безпеки України» від 19 червня 2003 р. //Голос України. – 22 липня 2003 р. – № 134.

безпеки України обумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам загроз національним інтересам»¹.

Крім того, політика інформаційної безпеки повинна проводитися лише у тих формах і тими методами та засобами, які є притаманними і прийнятними у демократичній правовій державі. Тобто ґрунтуватися на принципах демократії і верховенства права.

Це підтверджується нормами ст. 5 згаданого закону, яка виділяє основоположні принципи державної діяльності в цій сфері:

- пріоритет прав і свобод людини і громадянина;
- верховенство права;
- пріоритет договірних (мирних) засобів у розв'язанні конфліктів;
- своєчасність і адекватність заходів захисту національних інтересів реальним і потенційним загрозам;
- чітке розмежування повноважень та взаємодія органів державної влади у забезпеченні національної безпеки;
- демократичний цивільний контроль над військовою організацією держави та іншими структурами в системі національної безпеки;
- використання в інтересах України міждержавних систем та механізмів міжнародної колективної безпеки.

Ведучи мову про реалізацію політики, потрібно зазначити, що через свій функціональний характер політика, будучи особливою формою існування, виступає як певного роду діяльність. У сучасній науці прийнято вирізняти дві форми існування політики: теоретичну (ідеальну) та практичну (матеріальну).

В теоретичній формі свого існування, яка відповідає філософській категорії ідеального, політика пов'язана з людською свідомістю як носієм цієї ідеальної форми політики і виражається у формі розумової діяльності. Теоретична політична діяльність включає формування політичної свідомості, менталітету, певних політичних установок, концепцій, програм тощо. Головними функціями в даному разі є пізнавальна, прогностична і ціннісно-орієнтовна.

Практична (матеріальна) форма політики, по суті, може бути охарактеризована як матеріалізація ідеальної форми, її зовнішній вияв у матеріальному світі, вона є тим, за допомогою чого зміст політики може бути донесений до конкретних її об'єктів. Матеріальну форму політики становить політична практика, організаційно-контрольна діяльність, управління та регулювання. Головними функціями цієї фор-

¹ Закон України «Про основи національної безпеки України» від 19 червня 2003 р. //Голос України. – 22 липня 2003 р. – № 134.

ми політичної діяльності є вироблення і реалізація внутрішньої і зовнішньої політики держави. На рівні державної політики це виражається в діяльності всієї системи інститутів публічної влади і конкретних продуктах цієї діяльності (наприклад, ухвалення конкретних політичних рішень, вибори, міжнародні переговори тощо).

Обидві форми існування політики об'єктивізуються в процесі реалізації конкретних політичних рішень і вже в такій формі сприймаються суспільством. «Матеріалізація політики, приведення її в дію в предметній формі досягається шляхом створення відповідних інструментів або засобів: політичних інститутів (виборності, призначень, представництва ...), інститутів (органів, установ) влади – уряду, його апаратів та ін.; в документах, політичних текстах програм, статутів, доповідей, промов, розпоряджень, інструкцій, наказів, декретів; у видовищній, аудіовізуальній формі – пропаганді, лозунгах, засобах масової інформації, ... в наукових дослідженнях».¹

Виходячи з уже визначеного нами місця інформаційної безпеки серед функцій сучасної держави, ми можемо стверджувати, що реалізація цієї політики щодо забезпечення цього виду безпеки об'єктивізується в конкретних діях суб'єктів публічної влади. Політика інформаційної безпеки, будучи складовою державної політики, реалізується у відповідних формах діяльності органів публічної влади.

Взагалі поняття форми є філософською категорією і може використовуватися в кількох значеннях. У діалектичному матеріалізмі категорія форми невід'ємно пов'язана з категорією змісту. Ці дві філософські категорії відображають взаємозв'язок двох сторін природної та соціальної реальності: певним чином впорядкованої сукупності елементів і процесів, що утворюють предмет або явище, тобто змісту і способу існування та виразу цього замісту, його різноманітних модифікацій, тобто форми. Поняття форми вживається також у значенні внутрішньої організації структури, і в цьому значенні проблематика форми отримує подальший розвиток у категорії структури.²

В процесі суспільного розвитку відбувається процес взаємодії форми та змісту політики, який реалізується як у впливі різних компонентів змісту, в тому числі і структури на форму, так і у впливі структурних компонентів форми на зміст політики. Подібна взаємодія має

¹ Политология: энциклопедический словарь. / Общ. ред. и сост. Ю. И. Аверьянов. – Москва: Изд-во Моск. коммерч. ун-та, 1993. – С. 254

² Философский словарь. / Под ред. М. М. Розенталя. – Москва: Политиздат, 1972. – С. 372.

певну ієрархічну структуру, в якій зміст посідає привілейоване становище стосовно форми. У відносинах змісту та форми зміст є основною, а форма – похідною від змісту, в ідеальному варіанті зміст визначає форму, необхідну для своєї актуалізації. Але форма має певну самостійність щодо змісту і може тією чи іншою мірою впливати як на сам зміст політики, так і на процес реалізації цього змісту. Цей вплив може носити як позитивний, так і негативний характер. Негативний характер взаємодії форми та змісту найчастіше виражається в конфлікті змісту та форми, окремих їх компонентів, що обумовлюється їх невідповідністю.

Конфлікти змісту та форми політики можуть носити функціональний, юридичний або моральний характер. Функціональний характер виражається у невідповідності змісту політики конкретним формам та засобам її реалізації, недосконалості відповідних суспільних або державних інститутів, на які покладено проведення цієї політики. Конкретним прикладом такого конфлікту може слугувати необхідність проведення адміністративної реформи в Україні через недосконалість існуючої системи і її невідповідність тим завданням, які стоять в цій сфері перед нашою державою.

Конфлікт юридичного характеру обумовлюється недосконалістю нормативно-правового регулювання суспільних відносин, що є об'єктом політики, наявністю колізій правових норм та прогалин у законодавстві, невідповідності правових норм сучасному стану суспільних відносин. Як приклад можна навести значні прогалини в правовому регулюванні питань інформаційної безпеки.

Конфлікт морального характеру обумовлюється різним відношенням суб'єктів та об'єктів політики до конкретних засобів її втілення. Це проблема так званих «непопулярних засобів», до яких найчастіше змушені вдаватися правителі в період певних економічних або політичних труднощів і які (засоби) можуть бути неадекватно або негативно сприйняті суспільством.

Уникнення та розв'язання подібних конфліктів форми і змісту є однією з умов ефективності політики, а вміння суб'єктів політики знаходити виходи з подібних ситуацій є частиною так званого мистецтва або науки управління.

Діяльність державних органів щодо реалізації державної політики відбувається в особливих формах і за допомогою специфічних методів. «Форми реалізації функцій держави показують, як її оформлено. Ме-

тоди ж здійснення функцій держави являють собою способи та засоби, що використовуються при функціонуванні держави».¹

І в цьому аспекті форми реалізації державної політики інформаційної безпеки, на нашу думку, цілком охоплюються класичною класифікацією на правові та організаційні форми реалізації функцій держави.

Правові форми державної діяльності щодо проведення політики інформаційної безпеки, найзначніший обсяг якої здійснюється в державно-управлінській сфері, на яку покладено здійснення політики інформаційної безпеки відповідно до законів України, безпосередньо пов'язані з існуючим в державі механізмом правового регулювання.

З огляду на структуру механізму інформаційної безпеки України, ми можемо виділити головні правові форми реалізації відповідної політики, а саме: правотворча діяльність (суб'єктами якої є Верховна Рада, Президент України, Кабінет Міністрів, міністерства та відомства), застосування правових норм правоохоронними та контрольними органами.

Слід також відзначити високе значення організаційних форм державної діяльності. Форми цієї групи, як і правові, «пов'язані з компетенцією органу, державно-владним повноваженням його представників, проте це повноваження виявляє себе не як пряме юридичне веління, а опосередковано через позаюридичні засоби, і лише їхні передумови та результати можуть бути юридично зафіксовані»². Організаційні форми набувають виключного значення в деяких аспектах інформаційної безпеки, які стосуються розбудови та захисту інформаційної інфраструктури, організаційних заходів щодо додержання режимів таємності і конфіденційності інформації, застосування заходів технічного і криптографічного захисту інформації тощо.

§ 2 Особливості застосування методів державного управління в сфері інформаційної безпеки

Діяльність державних органів щодо реалізації конкретних завдань у рамках захисту інформаційної безпеки держави відбувається за допо-

¹ Теория государства и права. /Под ред. В. К. Бабаева. – Москва, Юристъ, 1999. – С. 85

² Коваль Л. В. Адміністративне право. – Київ, 1996. – С. 81.

могою специфічних методів. Причому ці методи обумовлюються конкретними загрозами і повинні бути адекватними. В загальнофілософському розумінні метод (від грецького *methodos* — буквально «шлях до чого-небудь») — спосіб досягнення мети, певним чином впорядкована діяльність.¹ Але в нашому випадку, згідно з Концепцією національної безпеки, існують чіткі обмеження цих способів. Причому такі обмеження побудовано за двома основними напрямками.

По-перше, це обмеження, які ставляться вимогами демократичних принципів діяльності державних органів.

По-друге, це обмеження, які ставляться умовою адекватності і відповідності характеру загрози.

Грунтуючись на запропонованій нами концепції побудови системи інформаційної безпеки за схемою з двома керівними центрами, які представлені відповідно законодавчим органом і вищими органами виконавчої влади ми можемо провести певну диверсифікацію методів, що використовуються у функціонуванні цього механізму.

Законодавчому органу, Верховній Раді, у цій схемі відводиться роль постановки завдань — визначення основних параметрів інформаційної безпеки, а також виконання певних контрольних функцій.

Але безпосередньо реалізація цієї політики інформаційної безпеки відбувається через систему органів виконавчої влади. Таким чином, саме методи соціального регулювання і управління, які є в арсеналі виконавчої влади, набувають виключного значення для проведення політики інформаційної безпеки з метою досягнення необхідних безпечних параметрів функціонування інформаційної сфери держави. А ті «методи, що їх використовують суб'єкти управління (передусім державні органи), є адекватними змісту первісної правової матерії, якою є регулятивні або правоохоронні, імперативні чи дозвольні норми права.»²

У контексті забезпечення інформаційної безпеки (необхідних умов і параметрів інформаційних процесів) ці методи діяльності органів публічної влади виступають як «способи організації, впорядкування процесів, що відбуваються в системі, прийоми здійснення загальних функцій, що виникають в процесі спільної діяльності».³

¹ Философский словарь. / Под ред. М. М. Розенталя. — Москва: Политиздат, 1972. — С. 241

² Коваль Л. В. Адміністративне право. — Київ, 1996. — С. — 108.

³ Бахрах Д. Н. Административное право. — Москва: БЕК, 1999. — С. 186

Знову ж таки в галузі методології і наука, і практика управління ґрунтуються на класичних методах переконання, заохочення та примусу. Наразі на сьогоднішній день лише сформовано розуміння того, що для ефективного виконання поставлених завдань «методи переконання, заохочення й примусу... повинні розумно поєднуватись, тобто не протистояти одне одному, а доповнювати, підпорядковуватись загальним завданням керівного впливу»¹.

Але інформаційна безпека має в цьому аспекті істотну специфіку, яка полягає у специфічному об'єкті цієї безпеки – інформації. А це означає, що з огляду на висвітлені нами в попередніх розділах проблеми формування інформаційного суспільства та ролі інформації у соціальному управлінні на перше місце виходить саме метод переконання. Адже інформацію в сучасних умовах дуже часто називають найбільш потужним і практично невичерпним ресурсом соціального управління, який обумовлює принципові перетворення у найбільш владних механізмах².

Таким чином, саме переконання, у рамках якого здійснюється цілеспрямований вплив на свідомість людей шляхом роз'яснення їхніх прав та обов'язків, привернення уваги, підвищення інтересу, поєднання соціальних інтересів конкретної особи з інтересами держави та суспільства, можна вважати одним з головних ресурсів захисту інформаційної безпеки.

Ясна річ, невід'ємною умовою дієздатності та ефективності методів переконання є розуміння громадянами цілей та завдань держави на конкретному етапі, відповідність національних інтересів держави конкретним особистим соціальним інтересам та потребам, активна участь громадян у відстоюванні та забезпеченні національних інтересів. Результатом застосування методів переконання повинно бути добровільне виконання об'єктом управління правових норм та приписів, що виражають волю суб'єкта. Правильне застосування методів переконання забезпечує високий рівень правосвідомості громадян.

Практичне застосування цього методу в сфері інформаційної безпеки є багатоваріантним. Наприклад, забезпечення режимів доступу до інформації багато в чому залежить саме від переконання. Так, дуже

¹ Колпаков В. К. Адміністративне право України. – Київ: Юрінком Інтер, 1999. – С. 191

² Див.: Toffler A. Powershift. Knowledge, wealth, and the violence at the edge of the 21 century. New York: Bantam books, 1990.

часто дослідники пов'язують причини витоку таємної і конфіденційної інформації безпосередньо з особистими якостями осіб, які відповідають за збереження та нерозповсюдження цієї інформації. Згідно з опитуваннями, проведеними на російських режимних об'єктах, 35% опитаних виправдовують скоєні порушення режиму таємності незнанням норм режиму таємності, 59% – непередбачуваністю деяких обставин (економічні, виробничі і фінансові труднощі виробництва), які вплинули на невиконання вимог режиму таємності, 61% – недосвідченістю і невмінням працювати з документами та виробами, що мають гриф «таємно» або «комерційна таємниця»¹.

Високоєфективними є методи переконання і у напрямках забезпечення додержання законодавства в інформаційній сфері, захисту інформаційних прав і свобод людини, захисту моральності тощо. Це вже не кажучи про інформаційне забезпечення державної політики взагалі, яке також є предметом інформаційної безпеки держави.

Застосування державного примусу є більш актуальним в аспектах відповідальності за правопорушення в інформаційній сфері, фізичного захисту об'єктів інформаційної інфраструктури і носіїв інформації з обмеженим доступом.

Певні аспекти інформаційної безпеки є широким полем для застосування методу заохочення. Окрім суто внутрішньоапаратного застосування з метою заохочення співробітників або посадових осіб, величезне значення має зовнішній напрямок. Цей зовнішній напрямок полягає у заохоченні діяльності фізичних та юридичних осіб, результатом якої є поліпшення параметрів і характеристик інформаційних відносин в Україні. В цьому напрямку заохочення може здійснюватись двома шляхами.

По-перше, це прийняття індивідуальних актів та заходів, наприклад, різного роду державні премії, нагороди та інші заохочувальні заходи діячам науки, освіти та мистецтва, які є основними «виробниками» високоякісної інформаційної продукції, працівникам інформаційних галузей промисловості та засобів ЗМІ.

По-друге, це створення пільгових умов для різного роду прибуткової і неприбуткової діяльності в галузі інформації, освіти, науки, культури, які б заохочували розвиток необхідних українському суспільству напрямків. Це, зокрема, податкові і тарифні пільги, спрощення адмі-

¹ Северин В.А. Правовое обеспечение информационной безопасности предприятия. – М., 2000. – С. 106.

ністративних процедур і дерегуляція відповідних видів підприємницької та громадської діяльності тощо.

Взагалі ж слід ще раз наголосити на тому, що специфіка форм та методів проведення державної політики інформаційної безпеки обумовлюється насамперед складними і багатограними характеристиками самої інформації та інформаційних відносин. Це обумовлює специфічні принципи побудови державної діяльності.

Насамперед це стосується проблеми балансу між інформаційними свободами людини і необхідністю державного втручання в інформаційні відносини. Проблема цього балансу є першочерговою, враховуючи відсутність в Україні сталих демократичних традицій, високий ступінь корумпованості і криміналізації держави і суспільства. Можливо, часткове її вирішення лежить у площині реформування інформаційного законодавства та створенні дієвих механізмів захисту громадянами своїх прав. Адже на «дух» демократії і законності в Україні сподіватися було б просто смішно. Як зазначають автори одного з досліджень розвитку українського суспільства, «такі поняття, як політичний та ідеологічний плюралізм, правова держава, громадянське суспільство, демократія тощо, стали публіцистичними термінами й дуже часто не містять у собі глибокого змісту, тобто теоретична інтерпретація політичного процесу й сам політичний процес мало пов'язані між собою»¹. Готових рецептів вирішення цієї проблеми, ясна річ, не існує, але остаточна втрата свободи слова, яка є не такою й віддаленою, вимагає рішучих дій. Причому ці дії скоріше будуть ініційовані суспільством, ніж державою.

Таким чином, ми підходимо до другого важливого пункту, який саме і обумовлюється потенціалом *демократичного (підкреслено нами – Б.К.)* суспільства у вирішенні питань інформаційної безпеки. Це стосується не лише контролю над владою через політичні механізми, а й звичайної діяльності великої кількості недержавних суб'єктів, від яких залежать умови інформаційних процесів в Україні. Це і підприємці, і працівники освіти, науки, культури, і політичні та громадські рухи тощо. Але ефективна діяльність недержавного сектора можлива лише за умови демократичної системи влади в державі. Тому дотримання демократичних принципів вимагає від держави переважно застосовувати опосередковані економічні методи регулювання інформаційної

¹ Михальченко М. Самчук З. Україна доби межичасся. Блиск і убогство куртизанів. – Дрогобич: Видавнича фірма «Відродження», 1998. – С. 277 – 278.

сфери, допускаючи безпосереднє адміністративне втручання лише в окремих випадках. Але, з другого боку, широке застосування економічних, опосередкованих методів впливу вимагає наявності значних матеріальних і фінансових ресурсів в державі, що, з огляду на негативні процеси в українській економіці, накладає значні обмеження на можливість їхнього використання.

І, нарешті, третьою вимогою є задекларований принцип адекватності способів і методів захисту інформаційної безпеки конкретним загрозам. Цей принцип так само виступає стримуючим фактором можливих утисків демократичних принципів та громадянських свобод під приводом захисту інформаційної безпеки. Дотримання принципу адекватності насамперед вимагає чіткого законодавчого визначення критеріїв і видів загроз інформаційній безпеці України, можливих дій у відповідь.

З огляду на те, що дане дослідження носить правовий характер, у цьому підрозділі ми практично не торкаємося форм та методів впливу на ситуацію в інформаційній сфері, які є в арсеналі недержавних суб'єктів. Хоча цей вплив є досить помітним. Крім того, створення готових рецептів щодо діяльності державних органів в галузі інформаційної безпеки і інформації взагалі також лежить більшою мірою не в правовій, а в політичній площині. Але основні її аспекти буде розглянуто в розділі, присвяченому інформаційному фактору політики державної безпеки.