ПУБЛІЧНЕ УПРАВЛІННЯ У СФЕРІ ДЕРЖАВНОЇ БЕЗПЕКИ ТА ОХОРОНИ ГРОМАДСЬКОГО ПОРЯДКУ

УДК 351.746.1
DOI https://doi.org/10.32840/1813-3401.2021.4.18

І. В. Кукін
кандидат наук із державного управління,
докторант кафедри прикордонної безпеки
Національної академії Державної прикордонної служби України
імені Богдана Хмельницького

ОСНОВНІ ПІДХОДИ ЩОДО ФОРМУВАННЯ КОНЦЕПЦІЇ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИСТОСТІ

У статті наведено основні етапи розвитку державної інформаційної політики, окремі недоліки проєкту Концепції інформаційної безпеки України. Окреслені базові підходи до розробки Концепції інформаційної безпеки особистості. Актуальність удосконалення державної інформаційної політики України зумовлена постійним розвитком технологій ведення гібридних війн та продовженням поширення Російською Федерацією небезпечної для українського суспільства інформації.

Зазначено, що на кожному з шести етапів трансформації державної інформаційної політики України виникали нові загрози інформаційної безпеки. З урахуванням накопиченого державою досвіду постійно удосконалювались процеси правового регулювання в інформаційній сфері діяльності, структура та повноваження державних інституцій, організація спільної діяльності суб'єктів публічного управління.

Зазначено, що складність розробки загальної Концепції інформаційної безпеки полягає в необхідності поєднання різних за своїми властивостями об'єктів, які потребують захисту. Так інтереси людини, громадянина, суспільства та держави не завжди збігаються. Це потребує застосування органами публічної влади різних форм, механізмів, способів та засобів в інтересах забезпечення інформаційної безпеки.

Підкреслено, що реформування упродовж 2019–2020 років Міністерства культури та інформаційної політики, введення в дію низки нових нормативно-правових актів, які визначають основні засади інформаційної реінтеграції Автономної Республіки Крим та організації в Україні національного спротиву також зумовлюють необхідність відокремлення напряму діяльності щодо забезпечення інформаційної безпеки особистості.

Наведено способи захисту об'єктів від інформаційних загроз. Найбільш пріоритетним для досягнення поставленої мети визначено сукупність заходів формування в людини імунітету до шкідливої та небезпечної інформації, що позитивно впливає на безпеку суспільства. Введено поняття ризику інформаційної безпеки особистості. Надані рекомендації щодо визначення підходів до його оцінки.

Акцентовано на тому, що зміцнення стану забезпечення інформаційної безпеки особистості потребує вжиття цілеспрямованих заходів, що сприяють соціально-культурному розвитку особистості. Наведені найбільш пріоритетні з них.

Ключові слова: *інформаційна безпека, інформаційна політика, інформаційна безпека особистості, концепція інформаційної безпеки, правове регулювання.*

Постановка проблеми в загальному вигляді. Процеси публічного управління потребують збору, обробки, накопичення та поширення інформації в інтересах прийняття управлінських рішень. Необхідність врегулювання державою суспільних відносин, особливо в інформаційній сфері діяльності виникає за умови ідентифікації певної проблеми, збільшення її реального або потенційного впливу на суспільство.

На кожному етапі розвитку України виникали нові виклики та загрози національній безпеці, які важко було заздалегідь передбачити. З 2014 року Україна постійно відчуває негативні наслідки небезпечного інформаційного впливу з боку Російської Федерації. Рівень небезпеки від інформаційної компоненти сучасних гібридних війн не зменшується, що свідчить про нагальну необхідність удосконалення правового регулювання у сфері інформаційної діяльності.

Існують чисельні загрози інформаційній безпеці усередині держави, що виникають унаслідок боротьби політичних партій за отримання влади, спроб просування на ринок недоброякісної продукції окремими її виробниками та недосконалості профілактики та протидії злочинній діяльності. Це також зумовлює подальше вдосконалення державної інформаційної політики.

Аналіз останніх досліджень і публікацій. Питання щодо формування основних засад державної інформаційної політики досліджували О. Яременко, В.М. Дрешпак, Г.З. Юксель, О.О. Яковенко, І.В. Пампуха, О.М. Марченко-Бабіч, Ю.В. Дем'янчук, О.В. Семченко, І.І. Біляєва, Д.В. Дубов, А.І. Невольніченко. Крім цього, за підтримкою Організації з безпеки і співробітництва в Європі у 2015 році був розроблений проєкт Концепції інформаційної безпеки України, який досі знаходиться на розгляді.

Виділення не вирішених раніше частин загальної проблеми. Незважаючи на значну кількість проведених досліджень, є суперечності у визначенні змісту, завдань та шляхів реалізації Концепції інформаційної безпеки України, які негативно впливають на результативність діяльності органів державної влади з питань протидії поширенню країною-агресором небезпечної для українського суспільства та міжнародної спільноти інформації. Це потребує пошуку нових підходів щодо вдосконалення правового врегулювання у сфері інформаційної діяльності.

Мета статті – визначення основних підходів щодо підвищення стійкості людини та громадянина до інформаційних загроз в інтересах розробки Концепції забезпечення інформаційної безпеки особистості.

Виклад основного матеріалу. Погоджуємось із думкою І.І. Біляєвої, що основні особливості інформаційної політики держави полягають в її формуванні та впровадженні державою, спрямованості на досягнення конкретних цілей, впливі на всі сфери суспільного життя. Вона слугує гармонізації інтересів людини, громадянина, суспільства та держави [1]. Інформаційні права визначають межі допустимої поведінки людини або групи осіб в інформаційному просторі. Їх захист передбачає створення системи норм права, діяльність уповноважених від імені держави суб'єктів, попередження протиправної діяльності, застосування санкцій до правопорушників [2, с. 45].

Складність формування державної інформаційної політики зумовлена наявністю джерел загроз інформаційній безпеці. Найбільш суттєвими серед них є: формування окремими державами сфер впливу; імперські амбіції Російської Федерації та наявність спільного з нею державного кордону, договірно-правове оформлення якого остаточно не завершене; наявні проблеми щодо забезпечення прав національних меншин; використання агресором міжнародного інформаційного простору для дискредитації України як суверенної держави [3, с. 126].

Діяльність органів державної влади щодо забезпечення інформаційної безпеки була розпочата з набуттям Україною незалежності. Так, О. Яременко визначає чотири етапи трансформації інформаційної політики, які відбулись упродовж 1991–2008 рр. та полягали у продовженні використання радянських норм права та їх адаптації до нових реалій суспільного життя, реформуванні державних інституцій [4]. В. Дрешпак використовує інші характерні риси діяльності державних інституцій. На його думку, перший етап (1991–1994 рр.) був пов'язаний із необхідністю перехідного періоду. Як наслідок, інформаційна безпека держави переважно розглядалась через призму запровадження свободи слова та забезпечення реалізації прав громадян в інформаційній сфері. На другому етапі (1995–1999 рр.) відбувся стрімкий розвиток електронних засобів масового інформування, що призвело до актуалізації небезпек в інформаційному просторі та удосконалення правового регулювання в інформаційній сфері діяльності [5, с. 6].

На третьому етапі (2000–2004 рр.) відбулась реорганізація суб'єктів управління та розпочато впровадження технологій електронного урядування. Проведені уніфікація та вдосконалення нормативно-правової бази. Четвертий етап (2005–2010 рр.) характеризувався визначенням основних напрямів розвитку інформаційного

суспільства, ратифікацією міжнародних норм права, формуванням Доктрини інформаційної безпеки. На п'ятому етапі (2011–2015 рр.) були реформовані державні та комунальні друковані засоби масового інформування, запроваджено технології цифрового мовлення, що також потребувало вдосконалення нормативно-правової бази [6, с. 4]. Також у 2015 р. був розроблений проєкт Концепції інформаційної безпеки України [7].

На думку О.О. Яковенко, основні недоліки зазначеного проєкту нормативно-правового акта пов'язані з недосконало визначеними потребами суспільства, цілями діяльності органів державної влади та перспективами. Не визначені ризики та шляхи їх мінімізації. Так, інформаційна безпека людини неможлива без забезпечення свободи слова, можливості отримання повної та правдивої інформації, захисту від шкідливої та небезпечної інформації очищення інформаційного простору від пропаганди вживання алкоголю та тютюну, забезпечення доступу до культурного надбання людства, розвитку здібностей щодо розуміння причин та наслідків суспільно значущих подій у суспільстві [8, с. 38].

На шостому етапі (який досі триває) під впливом негативних наслідків російської агресії відбулась активізація громадських організацій та окремих осіб щодо їх добровільної участі у протидії поширенню країною-агресором небезпечної для суспільства інформації. Крім цього, у 2019 році відбулась реорганізація Міністерства культури України в Міністерство культури, молоді та спорту, яке з 2020 р. було реформоване у Міністерство культури та інформаційної політики України. Також з 2022 р. набуває чинності Закон України «Про основи національного спротиву». Зокрема, він передбачає проведення інформаційних заходів із протидії інформаційним загрозам із боку країни-агресора та військово-патріотичного виховання громадян [9]. Реалізація цього закону сприяє зменшенню ризиків інформаційної вразливості громадян.

У 2018 р. запроваджена Стратегія інформаційної реінтеграції Автономної Республіки Крим і м. Севастополя. Вона передбачає проведення інформаційних, просвітницьких, культурних, роз'яснювальних заходів, дослідження культурної спадщини кримськотатарського та інших народів [10]. Важливість розширення впливу інформаційної політики України за межі контрольованої території держави також наведена в роботі Г.З. Юксель. Основу такої діяльності становлять інформаційні заходи, діяльність щодо руйнування російських міфів про історичне минуле України, доведення суспільно-корисної інформації, фіксація фактів та документування порушення прав людини на тимчасово окупованих територіях тощо [11, с. 188].

Відповідно до проєкту Концепції інформаційної безпеки України задоволення комунікативних потреб громадян досягається державою шляхом формування і регулювання інформаційного середовища в рамках державної інформаційної політики. Вразливими об'єктами, які потребують державного захисту, є людина, громадянин, суспільство, держава [7].

На нашу думку, зазначені об'єкти суттєво відрізняються за інтересами, способами та наслідками їх інформаційного враження. Як приклад, особа бажає усунення обмежень та перешкод у своїй діяльності. Крім цього, в демократичному суспільстві вона є найвищою соціальною цінністю. Водночас необхідність протидії загрозам інформаційної безпеки потребує використання державою обмежених ресурсів, що призводить до необхідності обмеження прав громадян, збільшення заборон та посилення відповідальності за порушення норм права.

Швидкість поширення інформації в суспільстві може перевищувати можливості держави щодо припинення її розповсюдження та знешкодження. Цілеспрямований розвиток здібностей людини щодо самостійного захисту від деструктивної інформації спрощує вимоги до побудови загальнодержавної системи протидії загрозам інформаційної безпеки. На тимчасово окупованих територіях взагалі неможливо силовими діями протидіяти поширенню небезпечної інформації. Саме необхідність підвищення імунітету громадян до шкідливої та небезпечної інформації потребує розробки Концепції забезпечення інформаційної безпеки особистості, яка є підґрунтям для реалізації державної інформаційної політики.

На думку Д.В. Дубова, органи державної влади та недержавні організації виконують різні функції щодо протидії загрозам інформаційної безпеки. Так, недержавні організації більш оперативно реагують на зміни інформаційного середовища, але вони не можуть виконувати правоохоронні функції. Проблемним питанням залишається поширення в Україні медіаосвіти та активізація протидії поширенню небезпечної

інформації на міжнародній арені [12]. Отриманий Україною досвід показує, що недержавні організації за умовою організації їх діяльності, відповідної мотивації та контролю з боку держави можуть ефективно впливати на формування інформаційного імунітету в суспільстві без дублювання діяльності органів державної влади та місцевого самоврядування.

Серед напрямів державної інформаційної політики Г. Красноступ виділяє створення національних інформаційних систем, організацію охорони та доступу до інформації, правове регулювання, розвиток основ інформаційної діяльності, оновлення інформаційних ресурсів, розвиток міжнародного співробітництва в інформаційній сфері [13]. Слід зазначити, що Російська Федерація в процесі гібридної війни проти України використовує військовий, економічний, політичний, ідеологічний, інформаційний компоненти [14]. Це впливає на визначення в концепції пріоритетних напрямів діяльності щодо соціально-культурного розвитку людини, який також позитивно впливає на підвищення культури політичного життя в суспільстві.

Інформація від органів державної влади має бути достовірною, але потребують удосконалення процеси забезпечення балансу негативної та позитивної інформації в новинах, тому що висвітлення викритих кримінальних справ не впливає на покращення криміногенної ситуації. Потрібне запровадження інструментів для перевірки всіма бажаючими особами суспільно значущої інформації. Це є запорукою унеможливлення свідомих маніпуляцій суспільною думкою окремими особами та зміцнення довіри громадян до діяльності державних інституцій.

У рамках Концепції забезпечення інформаційної безпеки особистості загрози доцільно розглядати як зовнішні фактори, що впливають на сприйняття інформації та породжені на її основі потреби людини. Вони можуть бути чітко визначені органами державної влади.

Існує кілька способів захисту об'єктів від інформаційних загроз: а) силовий, що полягає у фізичній діяльності правоохоронних органів у разі виявлення ознак протиправної діяльності; б) правовий, тобто нормативна регламентація порядку, правил створення, розповсюдження, використання, зберігання та обробки інформації, встановлення відповідальності за порушення норм права; в) стимулюючий – заохочення діяльності конкретної людини, що позитивно впливає на зміцнення стану інформаційної безпеки держави; г) запобіжний – формування в людини імунітету до шкідливої та небезпечної інформації.

У рамках Концепції забезпечення інформаційної безпеки особистості запобіжний спосіб захисту має бути пріоритетом державної інформаційної політики. Його застосування зменшує критичність для суспільства інформаційних загроз та дає змогу витрачати менше ресурсів на виконання силових способів захисту.

На нашу думку, ризик інформаційної безпеки особистості – це реальна (перевірена практикою в процесі протидії відповідним загрозам) та потенційна (уявна, не перевірена практикою) здатність людини здійснювати самостійний захист від шкідливої та небезпечної інформації без втручання органів публічного управління. Його ступінь залежить від соціально-культурного розвитку особистості, який не повністю доступний для визначення. Кожна особа незалежно від свого громадянства та місця проживання має свої погляди на процеси міжнародного, національного, регіонального, місцевого та побутового характеру. Унікальність кожної людини зумовлюється гендерними, віковими, біологічними, фізичними властивостями, її життєвим досвідом, рівнем соціального та культурного розвитку.

Залежно від ставлення людини до норм права, праці, здорового способу життя та харчування в суспільстві збільшується або зменшується кількість правопорушень, нещасних випадків, травматизму та захворювань. Окремі негативні явища пов'язані, наприклад, розповсюдження та вживання наркотиків.

Крім цього, будь-яка особистість може створювати небезпеки для оточуючих та себе особисто. В умовах поширення пандемії COVID-19 виникла нова потреба в культурному розвитку людини, яка виявилася критичною для виживання людства. Вона полягає і необхідності вживати заходи щодо захисту оточуючих осіб.

Не завжди людина здатна розуміти негативні для суспільства та себе наслідки невиконання норм права. Наприклад, в особи, яка за умови відсутності транспортних засобів завжди намагається здійснити перехід дороги на червоне світло світлофора, не закріплюються у підсвідомості моторні навички. Якщо така людина буде рухатись під впливом емоцій або складних роздумів, вона може не помітити особливостей дорожньої обстановки та потрапити

в дорожньо-транспортну пригоду. Зазначений приклад також показує обмеженість результативності профілактичних заходів лише ознайомленням людини з нормами права.

Поведінка людини зумовлена свідомим або несвідомим прийняттям нею рішення на підставі отриманої органами чуття інформації. Її неможливо достеменно передбачити. Разом із тим тенденції зміни групових ризиків інформаційної безпеки особистості можуть бути оцінені на підставі результатів статистичних спостережень, інтерв'ювання, опитування громадської думки. Під час анонімного опитування людина більше схильна надавати правдиву інформацію. Це дозволяє більш точно ідентифікувати найбільш суттєві та реальні ризики. Зазначені заходи дозволяють визначити пріоритети діяльності суб'єктів публічного управління для роботи з групами ризику або населенням окремої території, регіону, держави та міжнародної спільноти.

Поряд із розвитком здібностей особистості щодо пошуку, сприйняття, обробки, накопичення, поширення інформації для забезпечення безпеки свого життя, взаємно корисної діяльності в суспільстві є нагальна необхідність удосконалити знання людини з питань історії держави, загальних основ конституціоналізму, розподілу державної влади, функціонування державного механізму стримування та противаг, діяльності органів державної влади, місцевого самоврядування та політичних партій, здорового способу життя, основ безпеки життєдіяльності.

Ще до набуття віку, з якого встановлюється адміністративна та кримінальна відповідальність, у неповнолітньої особи мають бути сформовані навички ідентифікації правової та неправомірної поведінки. Особливо в прикордонних регіонах потрібне проведення заходів доведення та роз'яснення для населення законодавства України з прикордонних питань.

Концепція забезпечення інформаційної безпеки має передбачати корегування діяльності бібліотек, театрів, музеїв, розвитку туризму для соціально-культурного розвитку людини, що підвищує її компетенції самостійного захисту від шкідливої та небезпечної інформації.

Контроль за реалізацією концепції поряд із передбаченими нормами права вимогами, формами громадського контролю, потребує використання рекомендацій стандартів ISO серії 9000 та ISO 26000 з метою забезпечення постійного вдосконалення якості діяльності та соціальної відповідальності органів державної влади, місцевого самоврядування та інших організацій.

Висновки. Отже, забезпечення інформаційної безпеки особистості потребує запровадження та регламентації державою скоординованої спільної діяльності органів державної влади, місцевого самоврядування, інституцій громадянського суспільства у співпраці з міжнародною спільнотою. Її кінцевою метою має бути забезпечення сталого соціально-культурного розвитку людини, що характеризується набуттям нею здібностей, які необхідні для здійснення самостійного захисту від шкідливої та небезпечної інформації.

З огляду на відмінності інтересів та складності об'єктів, які потребують захисту від загроз інформаційної безпеки, є потреба у відокремленні в окремий напрям діяльності, що пов'язана із забезпеченням інформаційної безпеки особистості. Концепція забезпечення інформаційної безпеки особистості має стати основою подальшого вдосконалення та реалізації інформаційної політики держави.

Напрямом подальших досліджень може бути розробка інструментарію для визначення та зіставлення ваги ризиків інформаційній безпеці особистості в суспільстві.

Список використаної літератури:

1. Біляєва І.І. Державна та національна інформаційна політика: теоретико-концептуальний аспект. *Гілея: науковий вісник*. 2016. Вип. 105. С. 236–242. URL: http://nbuv.gov.ua/UJRN/gileya_2016_105_64.pdf (дата звернення: 30.11.2021).
2. Дем'янчук Ю.В. Концепція захисту прав і свобод людини в умовах інформаційної сфери. *Актуальні проблеми вдосконалення чинного законодавства України.* 2014. Вип. 34. С. 45–52.
3. Невольніченко А.І., Пампуха І.В., Марченко-Бабіч О.М. Концепція інформаційної боротьби в ідеологічній сфері. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка.* 2015. Вип. 49. С. 124–130.
4. Яременко О. Державне управління інформаційною сферою в Україні: структурно-функціональний аспект. *Правова інформатика.* 2008. № 2(18). С. 9–17. URL: http://ippi.org.ua/sites/default/files/08yosfa.pdf (дата звернення: 30.11.2021).
5. Дрешпак В.М. Становлення державної інформаційної політики України: зміст і хронологіч-

ні межі основних періодів. *Державне управління та місцеве самоврядування.* 2013. № 4. С. 3–13.
6. Дрешпак В.М. Періоди розвитку державної інформаційної політики України: Зміст і хронологічні межі. *Державне управління та місцеве самоврядування.* 2014. № 1(20). С. 3–14.
7. Концепція інформаційної безпеки України. URL: https://www.osce.org/files/f/documents/0/2/175056.pdf (дата звернення: 30.11.2021).
8. Яковенко О.О. Концепція інформаційної безпеки України в контексті становлення соціально відповідальної журналістики. *Наукові записки Інституту журналістики.* 2016. Т. 63. С. 36–42. URL: http://nbuv.gov.ua/ UJRN/Nzizh_2016_63_9 (дата звернення: 30.11.2021).
9. Про основи національного спротиву : Закон України від 16.07.2021 р. № 1702-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1702-20#Text (дата звернення: 01.11.2021).
10. Про схвалення Стратегії інформаційної реінтеграції Автономної Республіки Крим і м. Севастополя. URL: https://zakon.rada.gov.ua/laws/show/1100-2018-%D1%80#Text (дата звернення: 01.11.2021).
11. Юксель Г.З. Концепція інформаційної політики України щодо Криму. *Вчені записки Таврійського національного університету імені В.І. Вернадського*. Серія : Філологія. Соціальні комунікації. 2020. Т. 31(70), № 3(3). С. 186–193.
12. Дубов Д.В. Державна інформаційна політика України в умовах гібридного миру та війни. *Стратегічні пріоритети*. 2016. № 3. С. 86–93. URL: http://nbuv.gov.ua/UJRN/spa_2016_3_12.pdf (дата звернення: 30.11.2021).
13. Красноступ Г. Правове забезпечення державної інформаційної політики. URL: https://minjust.gov.ua/m/str_22116 (дата звернення: 20.11.2021).
14. Семченко О.В. Інформаційна політика України в умовах нової соціально-політичної реальності. *Сучасне суспільство.* 2015. Вип. 2(2). С. 157–166. URL: http://nbuv.gov.ua/UJRN/cuc_2015_2(2)__17.pdf (дата звернення: 25.11.2021).

Kukin I. V. Basic approaches to the concept of the individual information security development

The article presents the main stages of state information policy development, some shortcomings of the draft Concept of Information Security of Ukraine. The basic approaches to the development of the Concept of the individual information security are outlined. The urgency of improving the state information policy of Ukraine is due to the permanent development of technologies for hybrid wars and the continued dissemination dangerous information to Ukrainian society by the Russian Federation.

It is noted that at each of the six stages of the state information Ukraine policy transformation there were new threats to information security. Taking into account the accumulated experience, the state has constantly improved the processes of legal regulation in the information sphere, the structure and powers of state institutions, the joint organization activities of public administration.

It is noted that the difficulty of developing a general concept of information security is the need to combine different properties of objects that need protection. Thus, the interests of man, citizen, society and state do not always coincide. This requires the use of various forms, mechanisms, methods and tools by public authorities in the information security interests.

It was underlined that the Ministry of Culture and Information Policy reform in 2019-2020, the introduction of new legal regulations defining the basic principles of information reintegration of the Crimea Autonomous Republic and the organization of national resistance in Ukraine also necessitate the need to separate the direction of activities to ensure the individual information security.

Here are ways to protect objects from information threats. The highest priority for achieving this goal is a set of measures to develop human immunity to harmful and dangerous information that has a positive impact on public safety. The concept of personal information security risk is introduced. Recommendations for determining approaches to its evaluation are provided.

Emphasis is placed on strengthening the state of the individual information security requires the adoption of targeted measures to promote socio-cultural development of the individual. The most priority of them is given.

Key words: *information security, information policy, personal information security, information security concept, legal regulation.*