УДК 351.741:007]:004

Олег Панченко
директор Державного закладу «Науково-практичний медичний реабілітаційно-діагностичний центр МОЗ України», Президент Всеукраїнської професійної психіатричної ліги (Київ), депутат Краматорської районної ради VIII скликання, голова постійної комісії Краматорської районної ради з питань соціального захисту населення, освіти, науки, охорони здоров'я, культури, духовності, фізкультури, спорту, молодіжної політики та туризму, головний науковий співробітник, д.держ.упр., д.мед.н., професор, Заслужений лікар України,
ORCID iD https://orcid.org/0000-0001-9673-6685

ПУБЛІЧНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УМОВАХ ДІДЖИТАЛІЗАЦІЇ

Сьогодні існує певна напруженість між концепцією прозорості публічного управління і необхідністю захисту суспільно значущої інформації. У статті розглядається те, які види інформації уряди захищають із міркувань національної безпеки, а також які аргументи вони при цьому використовують. Із різних причин уряди прагнуть обмежити потоки інформації, але ці причини не завжди співвідносяться з типом політичного режиму в країні. Політика і політичні рішення залежать від безлічі акторів і від того, які суб'єкти мають найбільший вплив на даний момент, що найчастіше призводить до поступової зміни державної інформаційної політики та її механізмів реалізації.
***Ключові слова**: публічне управління; політика; інформаційна безпека; національна безпека; діджиталізація; політичні стратегії; політичні рішення.*

Oleg Panchenko
Chief Researcher, Director State Institution «Scientific and Practical Medical Rehabilitation and Diagnostic Center of the Ministry of Health of Ukraine», President of the All-Ukrainian Professional Psychiatric League, Kyiv, Deputy of the Kramatorsk district council of the VIII convocation, Head of Standing Committee on Social Protection, Education, Science, Health, Culture, Spirituality, Physical Education, Sports, Youth Policy and Tourism, Doctor of Science in Public Administration, Doctor of Medicine, Professor, Honored Doctor of Ukraine,
ORCID iD https://orcid.org/0000-0001-9673-6685

PUBLIC ADMINISTRATION OF INFORMATION SECURITY IN THE CONDITIONS OF DIGITALIZATION

Today there is a certain tension between the concept of transparency of public administration and the necessity to protect socially significant information. The article examines what types of information governments protect for national security reasons, as well as what arguments they use. For various reasons, governments aspire to limit the flow of information, but these reasons do not always correspond to the type of political regime in the country. Policy and political decisions depend on the many actors and on which subjects have the strongest influence at the moment, which often leads to a gradual change in public information policy and its implementation mechanisms.

In an information-rich society, a combination of factors and characters, including different political and economic interests, policy-making processes, types of governments and technical knowledge, result in disparate information security policies in different countries.

Under modern conditions, the information component of national security plays an extremely important role due to its risks and threats, which include cyber terrorism, cybercrime, aggressive propaganda, the spread of unconstitutional and anti-state slogans, restricting public access to public information and more.

In order to create an effective information security system, first of all it is necessary to conduct significant analytical training, on the basis of which it is legibly to determine the priorities and guidelines of further state information policy. In addition, it is important to choose information security tools that would be quite effective at the moment. It also requires a serious conceptual and theoretical search to determine the basic principles of state information security policy.

Continuation of conceptual and theoretical research in the field of information security should be the creation of systematized national legislation that would bring the legal framework for the activities of various persons, including the state, in the field of ensuring different levels of information security.
***Key words**: policy; information security; national security; digitalization; state policy; political strategies; political decisions; government administration.*

Постановка проблеми

Захищаючи свої національні інтереси, кожна держава повинна піклуватися про свою інформаційну безпеку. Інформаційна політика України, спираючись на пріоритети національних інтересів і загрози національній безпеці країни, формується як складова її соціально-економічної політики. Із правової точки зору вона ґрунтується на принципах правової демократичної держави та впроваджується шляхом розробки та реалізації відповідних національних доктрин, стратегій, концепцій і програм у відповідності до чинного законодавства. В Україні назріла об'єктивна необхідність у державно-правовому регулюванні науково-технологічної та інформаційної діяльності, яка відповідала б реаліям сучасного світу і рівню розвитку інформаційних технологій, нормам міжнародного права, але й одночасно ефективно захищала б власні національні інтереси. Відносини, пов'язані із забезпеченням інформаційної безпеки, як найважливіші сьогодні для суспільства і держави, вимагають якнайшвидшого законодавчого регулювання.

Однією зі складових суспільного розвитку України є стабільність і збалансованість у системі публічного управління інформаційною безпекою в умовах діджиталізації. Ефективність функціонування політичної системи держави у вирішенні складних соціально-політичних проблем сучасності безпосередньо пов'язана з роботою громадських об'єднань та окремих громадян. Інформатизація, що захопила всі сфери суспільного буття, набула статусу важливого об'єкта, стратегічного ресурсу як держави, так і будь-якої управлінської структури в системі суспільного управління.

Розвиток новітніх інформаційних технологій обумовлює збільшення технологічного розриву між вимогами, які постійно ускладнюються до показників захищеності інформаційних ресурсів у суб'єктів публічного управління і можливостей інформаційних технологій та програмно-апаратних засобів, що використовуються при забезпеченні інформаційної безпеки. Зростає потреба в науково обґрунтованих методах і технологічних рішеннях для поновлення і вдосконалення системи забезпечення інформаційної безпеки не тільки держави, а й суспільства й особистості зокрема. Недосконалі механізми публічного управління цією сферою, недостатність науково обґрунтованих методів і технологічних рішень для вдосконалення системи забезпечення інформаційної безпеки призводить до колосальних збитків як держави, так і суспільства й особистості.

Таким чином, актуальності набирає потреба в перезавантаженні діючої системи інформаційної безпеки у відповідності до сучасного суспільного запиту й турбулентних викликів. Нагальними виступають удосконалення та структуризація нормативно-правового, технічного, інформаційно-організаційного, медико-психологічного й превентивно-просвітницького функціоналу.

Аналіз останніх досліджень і публікацій

Проблема інформаційної політики та інформаційної безпеки є предметом дослідження багатьох вітчизняних і зарубіжних учених. Причому ці дослідження мають багатовекторний характер і здійснюються в різних напрямках. Зокрема, це створення нових і модернізація існуючих технічних засобів передачі, накопичення, зберігання та захисту інформації, розробка нових інформаційних технологій та програмних продуктів, формування ефективної нормативно-правової бази для регламентації дій в інформаційному просторі і напрацювання дієвих механізмів протидії деструктивним проявам.

Так, Г. Г. Почепцов акцентує увагу на тому, що з усіх аспектів інформаційної політики особливу увагу варто приділяти інформаційній безпеці [1]. Г. В. Виноградова, розкриваючи зміст державної інформаційної політики, розглядає її як сукупність напрямів і способів діяльності держави з одержання, використання, поширення та зберігання інформації [2].

У своїх наукових працях І. В. Арістова зазначає, що головною довгостроковою метою державної інформаційної політики України є формування відкритого інформаційного суспільства на основі розвитку єдиного інформаційного простору цілісної держави, його інтеграція у світовий інформаційний простір з урахуванням національних особливостей і інтересів під час забезпечення інформаційної безпеки на внутрішньодержавному та міжнародному рівнях [3].

Мета

Мета статті полягає в дослідженні публічного управління інформаційної політики з метою захисту національного інформаційного простору та забезпечення інформаційної безпеки в умовах діджиталізації.

Виклад основного матеріалу

З огляду на той факт, що інформація і новітні інформаційно-телекомунікаційні технології все більше визначають розвиток держави та суспільства, з огляду на стрімкий розвиток інформаційно-телекомунікаційних технологій, їх інтенсивне впровадження в усі сфери суспільного життя, у тому числі широке їх застосування в управлінні державою, особливої актуальності та значущості набуває розробка і реалізація концептуальних основ державної інформаційної політики, у тому числі належне забезпечення інформаційної безпеки на законодавчому рівні. Забезпечення інформаційної безпеки має включати в себе діяльність із забезпечення інформаційної безпеки людини, суспільства і держави, захисту прав і свобод в інформаційній сфері. Обов'язок забезпечення інформаційної безпеки покладається на всіх суб'єктів, що функціонують в інформаційній сфері, але ключову роль у проведенні інформаційної політики має відігравати держава в особі відповідних органів державної влади.

У зв'язку з цим набуває актуальності питання про те, наскільки сучасна система публічного управління здатна відповідати на виклики, поставлені глобальною діджиталізацією та загострені сучасними епідемічними процесами. Зокрема, необхідно отримати відповідь на питання, чи відповідають потребам системи державного управління сучасні інформаційно-телекомунікаційні системи. Величезні потоки інформації складаються у великі дані, які передбачається колись використовувати у цифровій економіці, але до кінця мало хто може зрозуміти, які дані нам необхідні і для чого. Чи ефективно використовуються об'ємні дані, що збираються тисячними командами чиновників? Які цифрові можливості є у чиновника для виконання поставлених завдань?

Технологічною основою формування моделі публічного управління стають електронні платформи – відкриті і технічно нейтральні засоби, що забезпечують умови вільного обміну ресурсами. Такі платформи визначають розповсюджуваний контент, аудиторію користувачів, способи підключення до контенту і взаємодії один з одним. Споживання суспільством платформних цифрових технологій і їх продуктів потужно впливає на внутрішню і зовнішню політику, державне управління, економіку, соціальні практики, освіту, суспільні цінності. Здійснюючи модерацію медіаконтенту, платформи мають величезний вплив на способи отримання знань, організовують участь користувачів у соціальних комунікаціях і породжують певні види публічного дискурсу. Таким чином, життєдіяльність суспільства значною мірою стає продуктом їх дизайну та контролю.

Ідея активного використання інформаційно-телекомунікаційних технологій для підвищення ефективності діяльності органів влади з'явилася в процесі реалізації адміністративних реформ на основі концепції нового державного менеджменту, що отримала в кінці XX ст. підтримку і поширення в системі публічного управління. У ході здійснення програми електронного уряду ця концепція адміністративних перетворень виявилася вузькою, такою, що недостатньо враховує особливість публічного управління. До того ж проявилися більш чітко деякі нові тенденції в суспільному розвитку, пов'язані з діджиталізацією соціуму (виникнення мережевих структур, комунікаційна революція, формування суспільства знань). Критика менеджеріальної ідеології супроводжувалася спробою нової концептуалізації публічного управління на основі теорії політичних мереж, соціальної синергетики, репрезентативного уряду, державного менеджменту публічних цінностей.

Вигода від потенціалу діджиталізації публічного управління не завжди очевидна, оскільки деякі проєкти зазнають невдачі ще на стадії реалізації, а реалізовані проєкти не ведуть до отримання очікуваного результату. Велике занепокоєння викликає та обставина, що універсальних рецептів трансформації не існує, і, як наслідок, значна частина «цифрових» ініціатив, які намагаються реалізувати органи влади, не досягають задуманих цілей. Проблеми діджиталізації публічного управління можуть бути виправдані наявністю ризиків і загроз, які заважають реалізації проєктів.

Виділення слабких сторін діджиталізації публічного управління слід почати з констатації наявності такого явища, як проведення «діджиталізації заради діджиталізації». Сьогодні в області публічного управління потрібна орієнтація роботи на цифрові технології. Але дані технології є лише інструментом, що дозволяє зробити більш зручними, доступними та прозорими взаємодії між різними елементами системи публічного управління. Абсолютно втрачається сенс діджиталізації, якщо головною метою стає освоєння виділених бюджетів і складання відповідних звітів.

Під державною інформаційною політикою необхідно розуміти політику, яка засобами державної (політичної) влади створює і забезпечує функціонування системи правового регулювання інформаційних відносин, захист прав і основних свобод людини, збалансованість інтересів людини, суспільства і держави у всіх сферах інформаційної діяльності [4]. Існує дві проблеми в розумінні того, як держави вирішують питання політики інформаційної безпеки. По-перше, існує безліч суб'єктів, як державних, так і приватних, зацікавлених у тому, як функціонує політика інформаційної безпеки. Однак ці актори не працюють у вакуумі. Вони обмежені політичними, ідеологічними та інституційними факторами. Це призводить до другої проблеми, яка полягає в тому, що інституційний характер уряду (будь то демократичний чи авторитарний) також впливає на те, як він вирішує ці питання. У той час, як директивні органи та приватні суб'єкти як в демократичних, так і в авторитарних країнах взаємодіють із метою забезпечення збереження того, що вони вважають життєво важливою інформацією, ці взаємодії можуть відрізнятися в залежності від типу режиму. Отже, процес формування політики інформаційної безпеки може нагадувати «перетягування канату» в країнах, де повноваження у цій сфері розмиті. Адже взаємодія між політиками та приватними суб'єктами «тягне» політику в тому чи іншому напрямку в залежності від політичного й ідеологічного клімату. У такому середовищі рідко можна виявити, що політика інформаційної безпеки повністю підпорядкована одному образу мислення. Однак це меншою мірою стосується випадків концентрації директивних повноважень, як це має місце в авторитарних країнах. Незважаючи на те, що в цьому зацікавлені кілька суб'єктів, вони менш здатні впливати на політику, яка відповідно стає менше схожа на «перетягування канату» і більше орієнтована на власні інтереси держави.

Коли мова заходить про захист інформації, уряди по-різному займаються розробкою політики. Зокрема, широке коло суб'єктів і інтересів, залучених до процесу розробки рішень у демократіях, створює унікальну напруженість, якої немає в авторитарних країнах, де доступ може бути більш обмеженим, а процес розробки політики більш централізованим. Хоча є дослідження, де стверджується, що демократії не завжди можуть відповідати своїм заявленим ідеалам, особливо тим, які стосуються інформаційної прозорості, та в періоди, коли стикаються з серйозними загрозами національній безпеці [5; 6]. Існує загальна думка, що демократії повинні прагнути до транспарентності у своїй політиці і діях перед громадянами та іншими країнами. Керуючись цими ідеалами, директивні органи повинні будувати свою політику в області інформаційної безпеки на основі мети створення товариства відкритого доступу, в якому інформація є доступною, а державні процеси прозорими. Відстоюючи переваги такого підходу і підзвітності політичних акторів електорату, деякі прихильники цієї точки зору визнають, що навіть у демократичних суспільствах для захисту життєво важливих державних інтересів може бути необхідна більш жорстка форма інформаційної безпеки, але такий контроль повинен бути якомога більш обмеженим [7]. Одним з обмежень цього аргументу є те, що в ньому не розглядається перехідний період між нормами та політикою. Навіть якщо припустити, що демократичні норми підтримують повну або майже повну прозорість і протистоять державній таємниці, усе одно залишається питання: яким чином норми знаходять свій шлях через політичний процес у закони, які виконуються. Хоча виконавча влада може бути зацікавлена в збереженні секретності, у цьому аргументі не береться до

уваги той факт, що в умовах демократії в процесі розробки політики беруть участь численні суб'єкти.

На відміну від демократичного ідеалу прозорості, авторитарні уряди покладаються на принцип самозбереження [8]. Результативна політика в області інформаційної безпеки зазвичай відображає цей принцип, зосередивши увагу на державному доступі до інформаційних вузлів і надаючи прямий законний інтерес представникам уряду запитувати інформацію з мінімальними засобами правового захисту. Однією з сильних сторін цієї позиції є те, що державні структури створюються для затвердження і реалізації політики інформаційної безпеки без формальних питань із боку опозиції. Якщо така є, то вона знаходиться у відносно слабкому становищі. Звичайно, авторитарні уряди не застраховані від політичних суперечок і розбіжностей. Зокрема, вони можуть зіткнутися із загрозою протесту через свою політику.

Бурхливий розвиток Інтернету мав би означати більшу демократизацію інформації, тобто більший потік інформації призводить до більшої відкритості. Але вчені одразу ж почали спростовувати це припущення. Демократичні уряди можуть мати більш автократичні тенденції, коли мова заходить про обмеження інформації [9]. Також більшість урядів схиляються на бік безпеки інформації, а не її поширення.

Політика інформаційної безпеки є результатом вибору конгломерату незалежних політичних акторів, які мають свій власний набір інтересів і цілей. Розуміючи, як ці сили діють і протидіють одна одній, стає яснішим кінцевий результат, тобто фактична політика інформаційної безпеки, що прийнята конкретною державою.

Теоретична проблематика інформаційної безпеки досліджується також і у рамках сучасного філософсько-політологічного дискурсу, доводячи свою актуальність і в питаннях державного і громадського управління. Саме інформація стає інклюзивним, інтегративним, наскрізним ресурсом, що дозволяє максимально ефективно управляти спільнотою в рамках сучасної інформаційної цивілізації.

Ефективне управління сучасним інформаційним суспільством має обов'язково передбачати формування державної інформаційної політики та створення умов її реалізації, а метою цієї діяльності має стати узгодження системно-функціональної та інформаційної складових в умовах стрімкого поширення процесів діджиталізації. Звідси зрозуміло, чому проблема забезпечення інформаційної безпеки увійшла до числа найбільш значущих і пріоритетних завдань, вирішення яких необхідне для існування і подальшого розвитку нашого суспільства. Інформаційна безпека важлива тому, що ми захищаємо свій інформаційний простір, а отже, свої інформаційні ресурси, свою національну культуру. Таким чином, філософська специфіка проблематики інформаційної безпеки полягає в тому, що інформація сьогодні стала ресурсом глобального об'єднання людства, що несе багато нових можливостей, але ставить перед окремими спільнотами і людством у цілому нові виклики та ризики. Від того, чи зможемо ми відповісти на ці виклики максимально адекватно, захистивши свій інформаційний простір від багатьох небезпек, багато в чому залежить успіх і своєчасність державних зусиль.

Сьогодні успішний розвиток демократично-правової держави та громадянського суспільства можливий тільки в умовах повноцінного використання інформаційних ресурсів, а також встановлення чіткої державної політики, яка забезпечила б високий рівень національної інформаційної безпеки. Фактично інформаційна безпека держави та національного соціуму стає ключовим фактором демократичних перетворень усередині країни, а також її виходу на конкурентоспроможний рівень у регіональному і глобальному масштабах. Практичне забезпечення національної інформаційної безпеки можливе за рахунок єдності різноманітних факторів: політичних, економічних, правових, організаційних та ін. Національна інформаційна безпека – реальний фактор успішної геостратегічної політики одночасно з демократичним суспільним розвитком. Це й обумовлює значний рівень актуальності концептуально-теоретичних досліджень філософсько-політологічного характеру, спрямованих на вивчення всієї повноти можливостей, які дозволяють сучасним державам і товариствам захищати свій інформаційний простір від величезної кількості викликів і проблем, що виникають у рамках глобальної інформаційної цивілізації.

Україна як демократична держава, розробляючи свою інформаційну політику, має усвідомлювати, що проблеми, пов'язані із забезпеченням інформаційної безпеки (формування інформаційного законодавства, протидія загрозам в інформаційній сфері, протидія конфліктам інформаційного характеру, інформаційним війнам, розробка правових засобів і організаційних заходів захисту від інформаційних війн), повинні вирішуватися комплексно, послідовно на основі суспільного та партійного порозуміння, для отримання якісно нового результату, що відповідало би стану і тенденціям розвитку світового інформаційного суспільства і загальновизнаним міжнародним і європейським стандартам у досліджуваній сфері.

Правову основу для ефективного забезпечення інформаційної безпеки людини, суспільства і держави в Україні становить інформаційне законодавство як система нормативно-правових актів, спрямованих на врегулювання суспільних відносин в інформаційній сфері. Невід'ємною частиною інформаційного законодавства України на сьогодні є й електронне законодавство (е-законодавство), під яким розуміють систему нормативно-правових актів, що забезпечує регулювання суспільних інформаційних відносин у процесі збору, реєстрації, накопичення, зберігання, використання та поширення даних (обробка даних), а також захист інформаційних ресурсів (продуктів, технологій), які здійснюються за допомогою інформаційно-комп'ютерних технологій та телекомунікаційних мереж [10; 11]. Необхідно відзначити, що е-законодавство трансформується у сферу інформаційного законодавства (у тому числі законодавства у сфері забезпечення інформаційної безпеки) шляхом врахування особливостей електронного середовища при створенні норм інформаційного законодавства. З огляду на зростання кількості випадків незаконного застосування інформаційної зброї, несанкціонованого поширення й отримання інформації за допомогою мережі Інтернет, поширення кіберзлочинності, особливої актуальності та значущості набуває так само і процес формування інформаційної політики в е-середовищі, під яким необхідно розуміти не тільки правові норми,

але і загальновизнані моральні канони поведінки, тобто специфічні правила інформаційної культури, нехтування якими негативним чином відбивається на реалізації вимог інформаційного законодавства (у тому числі законодавства у сфері забезпечення державної інформаційної політики та інформаційної безпеки). Таким чином, з огляду на прагнення України вивести діяльність щодо забезпечення інформаційної безпеки на якісно новий рівень, органам державної влади та вченим необхідно звернути увагу на конструктивну розробку моральних канонів поведінки та відповідне їх законодавче закріплення. Необхідно звернути увагу і на те, що питання належного забезпечення інформаційної безпеки безпосередньо залежить від врегулювання на законодавчому рівні прав і свобод людини в галузі інформації, визначення чіткого механізму реалізації зазначених прав, створення умов для реалізації цих прав і здійснення неупередженого контролю за їх безперешкодною реалізацією в рамках закону. Тобто належне забезпечення інформаційної безпеки потребує нормативно-правового закріплення прав людини в інформаційній сфері та гарантій їх реалізації.

Основним документом, який закріплює права і свободи людини, є Конституція України. Такими правами і свободами є таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції; таємниця приватного життя; свобода думки та слова, свобода вираження власних поглядів і переконань; право вільно збирати, зберігати, використовувати та поширювати інформацію (ст. 31, 32, 34 Конституції України) [12].

Одним із перших нормативно-правових актів, який був підписаний на початковій стадії формування інформаційного суспільства в Україні та закріпив основні принципи діяльності щодо забезпечення інформаційної безпеки людини, суспільства і держави, є Закон України «Про інформацію» [13]. Він є ключовим як в області забезпечення інформаційної безпеки, так і у сфері інформаційного права, оскільки його основним призначенням є врегулювання на належному рівні суспільних відносин в інформаційній сфері (у тому числі забезпечення безперешкодної реалізації прав і свобод у сфері інформації, захист інформації та інформаційної інфраструктури держави від загроз, у тому числі від інформаційних війн і т. ін.).

До правової бази забезпечення інформаційної безпеки відносяться й інші нормативно-правові акти (зокрема, закони і підзаконні акти), які регулюють окремі питання державної інформаційної політики та діяльності щодо забезпечення інформаційної безпеки: закони України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про інформаційні агентства», «Про авторське право і суміжні права», «Про друковані засоби масової інформації (пресу) в Україні», «Про телебачення і радіомовлення», «Про розповсюдження примірників аудіовізуальних творів та фонограм», укази Президента України «Про Стратегію національної безпеки України», «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні», Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» регламентують цілий ряд правовідносин, з яких і складається державна інформаційна політика і діяльність із забезпечення інформаційної безпеки людини, суспільства і держави [14-19].

На сьогодні, в умовах гібридної війни, є надзвичайно актуальним завдання забезпечення кібербезпеки України. Для його вирішення необхідний комплексний цільовий методологічний підхід на основі власного та міжнародного досвіду. Слід зазначити, що ряд кроків вже зроблено. По-перше, затверджена «Стратегія кібербезпеки України», по-друге, прийнятий Закон «Про основні засади забезпечення кібербезпеки України», по-третє, Україна підтримує міжнародну «Конвенцію про кіберзлочинність» [20–22].

У першому документі зазначені фактори загроз кібербезпеки:

- невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку і захищеності сучасним вимогам;
- недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації від кіберзагроз;
- безсистемність заходів із кіберзахисту критичної інформаційної інфраструктури;
- недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки і кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів;
- недостатня ефективність суб'єктів сектора безпеки й оборони України у протидії кіберзагрозам військового, кримінального, терористичного та іншого характеру;
- недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

У другому документі визначено правові та організаційні засади забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства і держави, національних інтересів України в кіберпросторі, повноваження і обов'язки державних органів, підприємств, установ, організацій, осіб і громадян, основних принципів координації їх діяльності.

У третьому документі акцентується увага на необхідності спільної політики, спрямованої на захист суспільства від кіберзлочинності шляхом створення відповідного законодавства і налагодження міжнародного співробітництва.

Отже, держава робить поступальні кроки в напрямі удосконалення своєї інформаційної політики. Однак належний рівень останньої може бути забезпечений лише за умови ефективної соціалізації інформаційних процесів, тобто добре розвиненого інформаційного суспільства. Щодо цього ще існують ряд недоліків, насамперед: застаріла нормативно-правова база в інформаційній сфері, забезпеченні інформаційної безпеки; недостатній рівень комп'ютерної та інформаційної грамотності населення, низький темп запровадження новітніх методів навчання із застосуванням сучасних інформаційно-комунікаційних технологій; нерівномірність забезпечення можливості доступу населення до мережі Інтернет; низькі темпи розробки відповідної інформаційної інфраструктури та інші. Подолання цих недоліків потребує ряду першочергових кроків: удоско-

налення нормативно-правової бази щодо захисту інформаційних ресурсів, протидії інформаційним війнам, протидії комп'ютерній злочинності, захисту персональних даних; концентрації діяльності органів державної влади та ресурсів держави на пріоритетних завданнях розвитку інформаційного суспільства та забезпечення інформаційної безпеки; підвищення рівня координації діяльності органів державної влади щодо виявлення, оцінки та прогнозування загроз інформаційній безпеці, запобігання таких загроз і забезпечення ліквідації їх наслідків, здійснення ефективного міжнародного співробітництва з цих питань; створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її елементів на належному рівні відповідно до світових стандартів.

Одним із головних пріоритетів розвитку національного інформаційного законодавства має стати, на наш погляд, створення цілісної системи у вигляді Інформаційного кодексу. Актуальність такого кроку обумовлена наявністю значного масиву нормативно-правових актів, що регламентують суспільні інформаційні відносини та забезпечують інформаційну безпеку; не всі ці нормативно-правові акти пов'язані між собою, спостерігається їх концептуальна і термінологічна неузгодженість, діють застарілі та неефективні норми. При його створенні необхідне серйозне переосмислення підходів до законодавчого врегулювання питань забезпечення інформаційної політики та безпеки, захисту прав на інформацію, гармонізації з європейськими та іншими міжнародними стандартами. Розробка кодексу має відбуватися з урахуванням принципів справедливості, державних гарантій, охорони та захисту загальновизнаних прав людини на інформацію в інформаційному просторі суспільства. Слід враховувати і такі відмінні риси процесу кодифікації:

1) при підготовці кодифікованого документа переглядається вся система правових норм із метою їх оновлення, усунення неузгодженостей, суперечностей;

2) кодифікація здійснюється періодично, залежно від накопичення нормативного матеріалу й об'єктивної необхідності;

3) кодифікація зачіпає правові приписи та юридичні інститути;

4) у результаті кодифікаційної роботи система права поповнюється новим джерелом.

Висновки

Таким чином, кодифікація національного законодавства в області інформаційної безпеки може вирішити проблему систематизації даної сфери державної та суспільної життєдіяльності. Важливо лише, щоб така кодифікація відбувалася на основі чітко розроблених і структурно збудованих теоретико-методологічних основ дослідження інформаційно-безпечного сегмента діяльності держави та громадянського суспільства.

Рушійною силою перебудови методів роботи в публічному управлінні є ефективне використання потенціалу інформаційно-телекомунікаційних технологій. Технологія сама по собі є ключовим фактором, що сприяє здійсненню стратегій діджиталізації публічного управління. Цифрові технології прискорюють час, збільшують масштаб і зменшують відстань. Але якщо такі можливості не затребувані, то технології нічого не можуть змінити і навіть навпаки – будуть заважати. У той же час важливо визнати, що існують як певні проблеми у суб'єкта публічного управління, так і загрози, які визначаються станом суспільства як об'єкта управління і станом прямих і зворотних зв'язків. На наш погляд, ці аспекти рано чи пізно повинні призвести до необхідності впровадження відповідних управлінських рішень. Можна констатувати, що механізм публічного управління та адміністрування у сфері цифрових перетворень має системно удосконалюватися, оскільки діджиталізація повинна стати головним інструментом для досягнення стратегічної мети держави – економічного зростання, що забезпечить добробут, комфорт та якість життя населення.

Проблеми інформаційної безпеки на сьогодні актуалізуються значним зростанням ролі накопичення, обробки та поширення інформації, зокрема, в ухваленні стратегічних рішень, збільшилася кількість суб'єктів інформаційних відносин і споживачів інформації. Інформація стала одним із чинників, здатних призвести до великомасштабних аварій, військових конфліктів і дезорганізації публічного управління. І чим вищий рівень інтелектуалізації й інформатизації суспільства, тим надійнішою має бути його інформаційна безпека.

В Україні в результаті проведення державою відповідної інформаційної політики та політики інформаційної безпеки, активізації діяльності з розробки нормативно-правового забезпечення в аналізованій сфері фактично почалася перебудова інформаційного законодавства, орієнтованого, перш за все, на інтереси людей і суспільства в інформаційній сфері, спрямованого на вдосконалення діяльності органів державної влади щодо якісного забезпечення інформаційної безпеки та кібербезпеки. Однак реалізація вже прийнятих норм на практиці просувається дуже повільно.

Одним з основних принципів забезпечення інформаційної безпеки в державі повинен стати принцип людиноцентризму, який оснований на актуалізації гуманних тенденцій через дотримання демократизації, визнанні людської гідності та поваги до особистості і кожного суб'єкта інформаційної безпеки. У той же час на рівні особистості інформаційна безпека повинна забезпечити захищеність психіки і свідомості людей від небезпечних інформаційних впливів: маніпулювання, дезінформування і т.п.

На сьогодні в нашій країні ще не сформовано відповідної сучасним геополітичним викликам системи інформаційної безпеки. Існує необхідність посилення буквально на всіх напрямках: нормативно-правовому (створення Інформаційного кодексу), організаційно-управлінському, інформаційно-технологічному. Для цього необхідне вироблення чіткої стратегії здійснення перетворень, яка має ґрунтуватися на міцному концептуально-теоретичному, науково-практичному базисі, що повинен сформуватися в рамках національного політологічного дискурсу відповідно до «Стратегії національної безпеки України».

Література.

1. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти: монографія / за ред. О.М. Бандурки. Харків : Ун-ту внутр. справ, 2000. 368 с.

2. Виноградова Г. В. Правове регулювання інформаційних відносин в Україні. Київ: «Юстиніан», 2006. 176 с.

3. Почепцов Г. Г., Чукут С. А. Інформаційна політика : навч. посіб. Київ: Знання, 2006. 663 с.

4. Арістова, І. В. Діяльність органів внутрішніх справ щодо реалізації державної інформаційної політики : монографія. Харків: Нац. ун-т внутр. справ, 2006. 354 с.

5. Rosenzweig P. Cyber warfare: How conflicts in cyberspace are challenging America and changing the world. Westport, CT: Praeger Publishers. 2013.

6. Anderson J. Public policymaking. Boston: Wadsworth Publishing. 2011.

7. Florini A. Behind closed doors: Governmental transparency gives way to secrecy. Harvard International Review. 2004. V. 26. P. 18-21.

8. O'Donnell G., Schmitter P. C., Whitehead L. Transitions from authoritarian rule: Southern Europe. Baltimore, MD: The Johns Hopkins University Press. 1986.

9. McChesney R.W. The Internet and U.S. communication policy-making in historical and critical perspective. Journal of Communication. 1996. V. 46. P. 98-124.

10. Старіш О. Г. Інформаційна політика держави в контексті глобалізації : дис. на здобуття наукового ступеня д-ра політ. наук : 23.00.16 / Київський національний університет ім. Т. Шевченка. Київ, 2008. 401 с.

11. Забезпечення інформаційної безпеки як функція сучасної держави : монографія / Тихомиров О.О.; заг. ред. Р. А. Калюжний. Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.

12. Конституція України : станом на 1 січ. 2020 р. / Відомості Верховної Ради України. Закон від 28.06.1996 № 254к/96-ВР Ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення 16.10.2021).

13. Про інформацію : Закон України від 02 жовт.1992 р. № 2657-XII. URL: http://zakon.rada.gov.ua (дата звернення 16.10.2020).

14. Про Концепцію Національної програми інформатизації: Закон України від 07 лип. 2011 р. № 3610-VI. Відомості Верховної Ради. 2012. № 7. Ст. 53.

15. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України від 09 січ. 2007 р. № 537-V. Відомості Верховної Ради України. 2007. № 12. Ст.102.

16. Про рішення Ради національної безпеки і оборони України від 14 вер. 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14 вер. 2020 р. № 392/2020 URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення 16.10.2021).

17. Про рішення Ради національної безпеки і оборони України від 6 трав. 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 р. № 287/2015 URL: http://zakon4.rada.gov.ua/laws/show/287/2015/paran7#n7 (дата звернення 16.10.2021).

18. Про Стратегію національної безпеки України: Указ Президента України від 12 лют. 2007 р. № 105/2007. URL: http://zakon1.rada.gov.ua/laws/show/105/2007 (дата звернення 16.10.2021).

19. Скулиш Є., Прокоф'єва Д. Безпека кіберпростору як елемент національної безпеки в умовах глобалізації інформаційних процесів. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2007. Вип. 2 (15). С. 26–31.

20. Житко А.О. Кібервійна як складова гібридної війни. Українське суспільство в умовах війни: виклики сьогодення та перспективи миротворення: матеріали Всеукр. наук.-практ. конф. / Маріуполь: ДонДУУ. 2017. С. 263–266.

21. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. 2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 16.10.2021).

22. Конвенція про кіберзлочинність : ратифікація 07 вер. 2005 р. : Рада Європи; Конвенція, Міжнародний документ від 23 лист. 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення 16.10.2021).

References.

1. Aristova, I. (2000) Derzhavna informatsiina polityka: orhanizatsiino-pravovi aspekty: monohrafiia. State information policy: organizational and legal aspects: monograph. Kharkiv: Vyd-vo Un-tu vnutr. Sprav.

2. Vynohradova, H. (2006) Pravove rehuliuvannia informatsiinykh vidnosyn v Ukraini. Legal regulation of information relations in Ukraine. Kyiv: Vydavnytstvo «Iustynian».

3. Pocheptsov, H., Chukut S. (2006) Informatsiina polityka: Navch. posib. Information policy: a textbook. Kyiv.

4. Aristova, I. (2006). Diyalnist orhaniv vnutrishnikh sprav shchodo realizatsiyi derzhavnoyi informatsiynoyi polityky: monohrafiya. [Activity of internal affairs bodies concerning realization of the state information policy: monograph] Kharkiv: Nats. un-t vnutr. cprav.

5. Rosenzweig, P. (2013). Cyber warfare: How conflicts in cyberspace are challenging America and changing the world. Westport, CT: Praeger Publishers.

6. Anderson, J. (2011). Public policymaking. Boston: Wadsworth Publishing.

7. Florini, A. (2004). Behind closed doors: Governmental transparency gives way to secrecy. Harvard International Review, 26, 18-21.

8. O'Donnell, G., Schmitter, P., Whitehead, L. (1986). Transitions from authoritarian rule: Southern Europe. Baltimore, MD: The Johns Hopkins University Press.

9. McChesney, R. W. (1996). The Internet and U.S. communication policy-making in historical and critical perspective. Journal of Communication, 46, 98–124.

10. Starish, O. H. (2008). Informatsiyna polityka derzhavy v konteksti hlobalizatsiyi [Information policy of the state in the context of globalization]. (Doctor's thesis) Taras Shevchenko National University of Kyiv. Kyiv.

11. Tykhomyrov, O. O., & Kalyuzhnyy, R. A. (2014). Zabezpechennya informatsiynoyi bezpeky yak funktsiya suchasnoyi derzhavy: monohr. [Ensuring information security as a function of the modern state: monograph]. Center for Educational Sciences. and scientific-practical. kind. NA SB Ukrainy.

12. Constitution of Ukraine. (1996). Vidomosti Verkhovnoyi Rady Ukrayiny. Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

13. Law of Ukraine On information from October 12 1992, № 2657-XII. (1992). Retrieved from http://zakon.rada.gov.ua

14. Law of Ukraine On the Concept of the National

Informatization Program from July 7 2011, № 3610-VI]. (2012). Vidomosti Verkhovnoyi Rady, 7. P 53.

15. Law of Ukraine On the basic principles of information society development in Ukraine for 2007-2015 from January 9, 2007 № 537-V. (2007). Vidomosti Verkhovnoyi Rady Ukrayiny, 12. P.102.

16. Decree of the President of Ukraine On the decision of the National Security and Defense Council of Ukraine of September 14, 2020 «On the National Security Strategy of Ukraine» from September 14, 2020 № 392/2020]. Retrieved from https://zakon.rada.gov.ua/laws/show/392/2020#Text

17. Decree of the President of Ukraine On the decision of the National Security and Defense Council of Ukraine of May 6, 2015 «On the National Security Strategy of Ukraine» from May 26, 2015 № 287/2015]. Retrieved from http://zakon4.rada.gov.ua/laws/show/287/2015/paran7#n7

18. Decree of the President of Ukraine On the National Security Strategy of Ukraine from February 12, 2007 № 105/2007. Retrieved from http://zakon1.rada.gov.ua/laws/show/105/2007

19. Skulysh, Y., & Prokofyeva D. (2007). Bezpeka kiberprostoru yak element natsionalnoyi bezpeky v umovakh hlobalizatsiyi informatsiynykh protsesiv [Cyber security as an element of national security in the context of globalization of information processes]. Pravove, normatyvne ta metrolohichne zabezpechennya systemy zakhystu informatsiyi v Ukrayini - Legal, regulatory and metrological support of the information protection system in Ukraine, 2 (15), 26–31.

20. Zhytko, A.O. (2017) Kiberviina yak skladova hibrydnoi viiny. Cyberwarfare as a component of hybrid warfare. Ukrainske suspilstvo v umovakh viiny: vyklyky sohodennia ta perspektyvy myrotvorennia, materialy Vseukrainskoi naukovo-praktychnoi konferentsii. Mariupol.

21. Law of Ukraine On the basic principles of cybersecurity of Ukraine from October 5, 2017 № 2163-VIII. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19

22. Convention on Cybercrime Council of Europe; Convention, International document of November 23, 2001. Retrieved from https://zakon.rada.gov.ua/laws/show/994_575