Інформаційна і національна безпека

УДК 342(477)

ЯЩЕНКО В.А., *доктор юридичних наук, професор,* головний науковий співробітник наукової лабораторії права національної та міжнародної безпеки ДНУ ІБП НАПрН України
ORCID: https://orcid.org/0000-0002-2257-318X

ДІАЛЕКТИКА ПРИНЦИПІВ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ УКРАЇНИ

DOI: https://doi.org/10.37750/2616-6798.2025.2(53).334057

Анотація. *У статті розглядаються фундаментальні принципи управління інформаційною безпекою, відзначається необхідність системного підходу, стратегічного планування та технологічних рішень для ефективного захисту інформаційного простору.*

Здійснено аналіз законодавчої бази та стратегії управління забезпеченням інформаційної безпеки України та пропонується власна система ключових управлінських принципів, які, власне, і формують політику у цій сфері. Запропоновано до основних принципів інформаційної безпеки віднести не лише захищеність від загроз, а більш узагальнений підхід - принцип безпечності існування як домінуючий, як природна людська потреба, в даному випадку існування в інформаційному полі. Цей принцип зумовлює таке розуміння безпеки, яке робить її ключовою складовою ієрархії потреб людини, створює необхідні умови для її самореалізації.

В тріаді: людина, суспільство, держава – як об'єктів управління інформаційною безпекою, запропоновано прийняти концепцію забезпечення безпеки окремої людини, індивіда, яка ще не знайшла свого належного відображення у правових актах, державній управлінській діяльності, що спричиняє складність у питаннях практичного втілення в життя цього феномену.

Здійснено критичний аналіз розуміння принципу доступності інформації, висвітлено організаційні та практичні напрямки управління процесами забезпечення доступності. В ході розгляду принципу пропаганди та контрпропаганди пропонуються стратегії комплексного підходу, який поєднує офіційні заяви, соціальні мережі, медіапроєкти, міжнародну дипломатію та ініціативи громадянського суспільства. Відзначено, що сучасна практика управління інформаційною безпекою реалізується із застосуванням методів стратегічної комунікації, підкреслюється важливість довгостроковості, узгодженості та координації у побудові інформаційної безпеки. Наголошується на розвитку проактивних методів захисту – важливості випереджувальних заходів та систем зворотного зв'язку для виявлення потенційних загроз ще до їх реалізації.

Ключові слова. *інформаційна безпека, принципи управління, стратегічні комунікації, доступність інформації, інформаційний простір, контрпропаганда, діалектика окремого та загального.*

Summary. *The article discusses the fundamental principles of information security management, notes the need for a systematic approach, strategic planning and technological solutions for effective protection of the information space.*

Based on the analysis of the legislative framework and strategy of information security management in Ukraine, the author proposes their own system of key management principles, which, in fact, form the policy in this area. It is proposed that the basic principles of information security include not only protection from threats, but also a more generalised approach - the principle of

security of existence as a dominant one, as a natural human need, in this case, existence in the information field. This principle leads to an understanding of security that makes it a key component of the hierarchy of human needs and creates the necessary conditions for its self-realisation.

In the triad of a person, society, and the State as objects of information security management, the author proposes to adopt the concept of ensuring the security of a person, an individual which has not yet been properly reflected in legal acts and public administration, which causes difficulties in the practical implementation of this phenomenon.

The author makes a critical analysis of the understanding of the principle of information accessibility, and highlights the organisational and practical areas of managing the processes of ensuring accessibility. In the course of consideration of the principle of propaganda and counter-propaganda, the author proposes strategies for an integrated approach that combines official statements, social networks, media projects, international diplomacy and civil society initiatives. It is noted that the modern practice of information security management is implemented using strategic communication methods, and the importance of long-term coherence and coordination in building information security is emphasised. The author emphasises the development of proactive methods of protection - the importance of proactive measures and feedback systems to identify potential threats before they are implemented.

Keywords. *information security, management principles, strategic communications, information accessibility, information space, counter-propaganda, dialectic of the individual and the general.*

Постановка проблеми. Управління інформаційною безпекою України останнім часом зазнало позитивних змін: удосконалюється його нормативна база, уточнюються функції суб'єктів управління, удосконалюються технології управління, зокрема за рахунок впровадження стратегічних комунікацій тощо. Нові виклики інформаційній безпеці України з боку рф зумовлюють нагальну необхідність пошуку шляхів подальшого розвитку інформаційної політики як ключового напряму національної безпеки, серед інструментарію якого закономірно виступають основні принципи безпеки, як засадні регулятивні положення.

Між тим, формування таких принципів, особливо у сфері управління, залишається далеким від досконалості. В першу чергу через недостатнє узагальнення змістовних елементів управління принципи зводяться до процедурно – технологічних аспектів, звідси їх визначеність, кількість та сутність постійно змінюється, що обмежує безпекову політику тактичними засобами, ускладнює формування її відповідних стратегій, створення ефективних програм інформаційної безпеки. Так, у публікаціях та безпекових системах традиційно вказується на три основних принципи інформаційної безпеки: конфіденційність, доступність, цілісність, які часто доповнюються принципом власності, законності. Такі системи безпеки як NIST Cybersecurity Framework [1] та ISO 27001[2], передбачають питання управління ризиками, обізнаності користувачів і т.п.

Ці обставини зумовили потребу проаналізувати чинні підходи до формування принципів управління інформаційною безпекою та запропонувати власну концепцію системи таких принципів, побудовану на основі закономірностей функціонування інформації та управління.

Результати аналізу наукових публікацій. Управління інформаційною безпекою є багатовимірним процесом, що вимагає комплексного підходу до формування стратегій, політик та механізмів захисту інформаційних систем. У сучасних наукових дослідженнях розглядаються різні аспекти цієї проблематики, починаючи від нормативно-правового забезпечення та організаційних підходів, закінчуючи технічними рішеннями та методами оцінки ризиків.

В змісті профільної наукової літератури простежується декілька підходів до визначення принципів управління інформаційною безпекою. Серед них висвітлення як загальнодержавних так і окремих принципів управління О.В. Олійником, Є. Низюк, які більшою мірою виступають процедурно – технологічними засобами діяльності, а не принципами. С.О. Лисенко висвітлює загальні принципи управління та акцентує увагу на потребі посилення контролю за впровадженням штучного інтелекту. Визначення поняття управління інформаційною безпекою та застосування системного підходу до управлінського процесу розглядається в конспекті лекцій (автори: С.О. Носок, О.М. Фаль, В.М. Ткач). З метою розгляду питання формування інформаційної політики безпеки людини використані публікації Золотар О.О., Тихого В.П.

Організаційно-правовий підхід акцентує увагу на розробці функцій управління інформаційною безпекою, утому числі доступністю інформації (Марущак А.І.), механізмів реалізації стратегічних комунікацій (Кукін І.В., Почепцов Г.). Також здійснено аналіз окремих нормативно-правових актів та регламентів, що забезпечують безпеку інформаційних ресурсів.

Ефективність реалізації стратегічних комунікацій досліджувалась за допомогою програми штучного інтелекту Chat GPT.

Мета статті. На основі аналізу висвітлених у нормативних актах та наукових публікаціях принципів управління інформаційною безпекою України, дослідження природи інформації та керівництва організованими системами запропонувати таку систему принципів, яка дала б можливість більш цілеспрямовано, на стратегічному рівні розвивати безпекову інформаційну політику України.

Виклад основного матеріалу. Зважаючи на важливість та комплексність питання управління (менеджменту) інформаційною безпекою, пропонуємо сконцентруватися на проблемі формування та дотримання принципів управління, які власне і визначають його фундаментальну основу, що зумовлює інформаційно – безпекову політику. Оскільки принципи виступають найбільш загальними сутнісними аспектами проблеми, вихідними положеннями, якими мають керуватися органи управління, здійснюючи управлінську діяльність, то звідси вони виступають засадними критеріями управління інформаційною безпекою, тобто, принципи фактично виступають ключовими фундаментальними змістовними елементами в ході розгляду питання стратегії інформаційно – безпекового менеджменту.

Таким чином, принципи управління інформаційною безпекою виступають регулятивними факторами цього процесу, адже вони формують стратегічні підходи, які мають використовувати органи управління під час реалізації політики безпеки. Саме тому принципи є ключовими концептуальними елементами, що визначають стратегію інформаційно-безпекового менеджменту. Це є свідченням того, що саме принципи, як базисна основа управління, дають можливість розкрити все багатство змісту керівництва забезпеченням інформаційної безпеки.

Аналіз публікацій з питання формування принципів управління інформаційною безпекою свідчить про те, що найчастіше до них відносять: принцип централізованого управління, комплексності, адаптивності, відповідальності, міжнародного співробітництва, захисту критичної інфраструктури, контролю та моніторингу. У конспекті лекцій з управління інформаційною безпекою це поняття визначається структурно досить близько до вказаних принципів: “сукупність засобів, методів і процесів (процедур), які забезпечують захист інформаційних активів і гарантують збереження ефективності та практичної корисності як технічної інфраструктури

інформаційних систем, так і відомостей, які в таких системах зберігаються і обробляються". [3,с.5].

В цілому ці принципи слід визнати правомірними, вони характеризують ті чи інші аспекти управлінської діяльності, однак стосуються більшою мірою процедурних складових управління, тобто, обмежених цільовим призначенням, тому цілком ймовірно зробити висновок про те, що вони все ж є результатом витягу з більш загальних положень, що відповідають суспільному статусу управлінської діяльності як такої. За великим рахунком управління – це керівництво організованою системою, яке включає політичні, адміністративні, технологічні складові, які досить часто трактують як принципи. В такому разі у сфері інформаційної діяльності практично будь – яка дія з формування інформаційної системи має ознаки управління.

Одразу зауважимо, що визначення принципів будь – якої діяльності пов'язано з проблемою співвідношення сутності і проявів, тому до принципів іноді відносять ті аспекти питання, які не виконують своєї регулятивної функції, а є похідними від її елементів. Так, навряд чи можна погодитися з думкою Олійника О.В. про необхідність систематизації окремо правових та організаційних принципів менеджменту. Цей автор стверджує, що "Зважаючи на те, що процес удосконалення системи забезпечення інформаційної безпеки триває, найбільш прийнятним підходом буде систематизація принципів окремо правових і окремо організаційних. Це сприятиме вдосконаленню як правової бази забезпечення інформаційної безпеки, так і системи його організаційного забезпечення. Визначення, обґрунтування і практичне застосування правових і організаційних принципів слугуватиме базою для вирішення широкого кола завдань забезпечення інформаційної безпеки. До правових принципів забезпечення інформаційної безпеки доцільно включення наступних: законності; пріоритету норм міжнародного права над національним законодавством; права власності; економічної доцільності" [4,с.172].

Справа в тому, що маючи засадну основу, саме принципи і визначають всі складові системи управління, у тому числі й правову їх регуляцію та організаційний аспект. Тобто, як правова регуляція, так і організаційна діяльність в даному випадку зумовлені саме принципами менеджменту, залежні від цих принципів і не можуть мати самостійного статусу принципових положень.

Водночас цілком доцільними вважаємо пропозиції автора про формування єдиної державної інформаційної політики, участь України у розробці міжнародних нормативних актів, які захищають інформаційну сферу [4,с.172]. Власне, ця єдність інформаційної політики і може виступати одним із принципів менеджменту інформаційної безпеки, однак цей аспект автором не розглядається.

Спробу з'ясувати принципи забезпечення інформаційної безпеки окремого підприємства також здійснила Низюк Є., яка виокремила наступні положення: принцип комплексності, безперервності, надійності, ешелонування, розумної достатності [5, с.546]. Незважаючи на те, що авторка здійснила коментар вказаних принципів через призму інформаційної безпеки, вони все ж залишаються процедурно-технологічними, неспроможними за своєю суттю повною мірою регулювати таку специфічну сферу, як забезпечення інформаційної безпеки.

Інформативною є стаття С.О. Лисенка про принципи державного управління інформаційною безпекою, в якій автор характеризує загальні принципи державного управління та концентрує свою увагу на проблемі актуалізації, можливих напрямків та способів належного контролю штучного інтелекту в умовах інформаційного суспільства з посиланням на дослідження американських експертів. Водночас автор вказує на

потребу застосування галузевого та територіального принципів управління, та використання їх в процесі управління інформаційною безпекою. Цей посил С.О. Лисенко підтверджує характеристикою вказаних підходів: "… галузевий принцип державного управління інформаційною безпекою відповідає за однорідні за характером функціонування об'єкти адміністративної діяльності. Вони закріплюються за відповідним органом управління, що забезпечує спеціалізований підхід до інформаційної безпеки. Натомість, територіальний принцип державного управління передбачає управління інформаційною безпекою на визначених територіях, що дозволяє враховувати специфіку регіонів, населення та їхні потреби у захисті інформації. Це також стосується і боротьби із інформаційно-психологічними операціями агресорів під час оголошеної та неоголошеної війни" [6,с.170].

Зазначимо, що територіальний аспект менеджменту інформаційної безпеки реалізується також у Стратегії інформаційної безпеки, п.5 стратегічних цілей якої передбачає: "Інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них територіях України, до загальноукраїнського інформаційного простору". [7]. Водночас поставленої мети: здійснити характеристику принципів забезпечення інформаційної безпеки у їх комплексі не досягнуто, автор обмежується, знову ж таки, аналізом загальних принципів і не формує на їх основі суто інформаційно- безпекові положення. На нашу думку, це положення є не стільки принципом, скільки технологією реалізації принципу доступності інформації.

Включення змістовних елементів інформаційно-безпекового процесу до державних принципів управління застосовано також і в більшості інших досліджень. Зокрема, у конспекті лекцій "Управління інформаційною безпекою" - уклад.: С.О. Носок, О.М. Фаль, В.М. Ткач. У ньому висвітлюються як загальні принципи управління інформаційною безпекою, так і питання інформаційної безпеки конкретного підприємства [3]. На перший погляд такий спосіб висвітлення даної проблеми здається правомірним, оскільки загальне завжди містить в собі елементи окремого, одиничного, того, що має місце в реальності. Водночас логічна операція з абстрагування визначених принципів до їх узагальненого рівня не здійснюється.

На нашу думку, з такими підходами до виокремлення принципів інформаційної безпеки навряд чи можна погодитися, оскільки специфіка саме інформаційної їх складової, яка має як загальні, так і індивідуальні ознаки, зв'язки, властивості залишається не розкритою. Багатий арсенал логічних засобів мислення передбачає застосування не лише категорії окремого, одиничного, а й особливого та загального, які виступають ступенями пізнання явищ чи предметів вивчення. Як відомо, принципи менеджменту інформаційної безпеки виступають особливим по відношенню до загальних принципів державного управління. Специфіка особливого у тому, що ця категорія не лише діалектично пов'язує знання окремого та загального, а ще й у тому, що особливе розвивається не лише за загальними законами існування, а формує і власні закономірності функціонування. Тобто, спроба авторів характеризувати принципи інформаційної безпеки виходячи лише з процедурно-технологічних положень не розкриває закономірностей їх функціонування, що в кінцевому рахунку знижує ефективність виконання принципами їх регулятивної функції, а значить і спроможність виконувати інформаційний захист, в тому числі у протидії інформаційній війні, яку веде рф проти України. Очевидно, саме через цю наукову невизначеність і в нормативних актах, що регулюють інформаційну безпеку, мова йде про цілі, завдання, виклики та загрози, при цьому з яких принципів ця діяльність має здійснюватися, не визначено.

Слід визнати, що за своїм ступенем узагальненості визначені вище принципи більшою мірою зводяться до складових, структури інформаційної безпеки, уособлюють в собі окремі безпекові дії та процеси, що відповідає лише вимогам рівня особливого, а не загального, що має міститись у понятті. Пропонується застосувати наступний спосіб виокремлення принципів управління інформаційною безпекою. Ним може стати поєднання як загальноуправлінських, так і інформаційних, безпекових складових менеджменту інформаційної безпеки в їх діалектичній єдності, тобто, виходити із змісту інформаційної безпеки шляхом аналізу та узагальнення її сутнісних особливостей.

Очевидно, що рухаючись від окремого до загального, стан захищеності державного суверенітету, територіальної цілісності, життєво важливих інтересів людини та громадянина, захист інформаційних активів тощо має на меті створення умов для безпечного існування людини, самого життя, що й виступає загальним по відношенню до вищеназваних напрямків та складових. Як з високим ступенем узагальненості стверджує В.П. Тихий: “безпека – це об’єктивний стан і суб’єктивне відчуття фізичної, майнової, соціальної, психологічної і моральної захищеності людини, її прав і свобод” [8,с.36-37].

Таким чином стратегія управління інформаційною безпекою має виходити з принципу безпечності існування як домінуючого, як природної людської потреби, в даному випадку існування в інформаційному полі. Фактично саме цей принцип відповідає статусу загального і визначає всі наступні дії, напрямки, методи забезпечення інформаційної безпеки, що виступають об’єктивно змістом її управління. Його особливістю є те, що даний принцип передбачає не лише протидію можливим та наявним інформаційним загрозам, а й конструктивну складову – зміцнення потенціалу безпеки, її розвиток, удосконалення.

На нашу думку, принцип безпечності існування зумовлює таке розуміння безпеки, яке робить її ключовою складовою ієрархії потреб людини, створює необхідні умови для її самореалізації, впевненості в майбутньому. Якщо протидія загрозам – це значною мірою боротьба з наслідками негативного впливу на безпеку, то принцип безпечного існування орієнтує процес управління не лише на протидію загрозам, а в першу чергу на запобігання, на попередження загроз, зміцнення потенціалу безпеки як своєрідного безпекового імунітету як окремої людини, так і суспільства та держави в цілому. Такий підхід свідчить про потребу якісно вищого рівня управління інформаційною безпекою, основними напрямками якого має стати поліпшення законодавчого регулювання питань інформаційної безпеки, актуалізація роботи інституційних механізмів захисту, міжнародної співпраці.

Зважаючи на людиномірність безпекових зусиль, в центрі яких знаходиться людина, її права та свободи, закономірно, що одним із ключових принципів управління інформаційною безпекою в тріаді: людина, суспільство, держава, має бути орієнтація на забезпечення безпеки окремої людини, індивіда. В такому разі об’єктом управління виступає наявне буття людини у всій його повноті. При цьому однією з важливих безпекових політичних проблем виступає питання співвідношення національної безпеки та безпеки окремої людини. Досліджуючи на фундаментальному рівні інформаційну безпеку людини як особистості О.О. Золотар підкреслює необхідність зосередження безпекових зусиль саме на забезпеченні безпеки окремої людини, яка є складовою елементу соціальної системи: “Як об’єкт соціальних відносин особистість, з одного боку, індивідуально виражає значимі риси певного суспільства, інтегрує соціальні відносини зовнішнього середовища і виробляє своє, особливе ставлення до зовнішнього світу. З іншого боку, економічні, політичні та соціальні відносини переломлюються

через внутрішній світ особистості, виявляються в її діяльності як особисте ставлення до об'єктивної дійсності. В цьому випадку особистість виступає як суб'єкт соціальних відносин, який керується в поведінці своїми потребами, інтересами, соціальними установками, ціннісними орієнтаціями" [9,с.44].

Методологія діалектичного підходу розглядає зв'язок між особистістю та суспільством як співвідношення загального та одиничного. Тому пріоритет особистості в даному випадку цілком правомірний з точки зору методології, оскільки одиничне завжди є виразом, втіленням загального, суспільного і навпаки, суспільне існує лише маючи місце в одиничному і інакше воно існувати не може.

Іноді поведінка особи може набувати антисоціального характеру (поширення недостовірної інформації, несанкціонований обіг інформації тощо), тобто небезпечного, загрозливого для нації, соціуму. Цей виключно суб'єктивний момент соціум контролює і вживає відповідні заходи впливу, в тому числі і безпекового. Іншими словами, суспільство, нація виконують безпекову функцію не лише по відношенню до самого себе, а в першу чергу до цієї особистості. В такому разі пріоритет особистості не є антиподом національного, суспільного, а його невід'ємним атрибутом. Таким чином, протиріччя між особистим і соціальним вирішується шляхом надання пріоритетності особистості, але виправленій соціально закономірним.

Зосередження інформаційно – безпекової політики на безпеці окремої людини, особи, формування її національної самосвідомості, здатності протистояти негативним інформаційним впливам, зумовлює потребу функціональних змін в управлінні процесами забезпечення безпеки. У дослідженні з управління інформаційною безпекою особистості І.В. Кукін вказує, що його сучасні функції: "полягають у забезпеченні безпечних умов життєдіяльності людини, визначенні загроз безпеки особистості, розвитку безпеки соціальних комунікацій, формуванні світогляду, розвитку знань, умінь і навичок людини з питань прийому, створення, поширення, накопичення, пошуку, оцінювання й обробки інформації, розвитку форм фіксації інформації та їх творчого поєднання. Використання механізмів державного управління інформаційною безпекою особистості впорядковує культурний розвиток особистості, формування правосвідомості, усвідомлення необхідності об'єднання зусиль з іншими членами суспільства в інтересах створення колективної системи забезпечення безпеки життєдіяльності…" [10, с.28]

В Україні виокремлення управління безпекою особистості розвивається у контексті програми сталого розвитку суспільства. Водночас цей концепт, як і інформаційна безпека людини в цілому, ще не отримала належного наукового обґрунтування і не знайшла свого відображення у правових актах, державній управлінській діяльності, що спричиняє складність у питаннях практичного втілення в життя цього феномену. Нагальною вбачається проблема формування та впровадження цілеспрямованих управлінських кроків щодо розвитку механізмів інформаційного захисту для безпеки людини (особистості).

Важливим інформаційно-безпековим принципом, що забезпечує дотримання прав та свобод людини в роботі з інформацією, видається принцип доступності інформації, який входить до складу поняття інформаційна безпека і є чи не найбільш врегульованим серед технологій управління інформаційною безпекою.

Згідно Закону України "Про інформацію" "режим доступу до інформації – це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації" [11, Ст. 28]. У розвиток цього поняття А.І. Марущак доходить висновку, що: "доступ до інформації у суб'єктивному розумінні – це гарантована

державою можливість фізичних, юридичних осіб і держави (державних органів) вільно одержувати відомості, необхідні їм для реалізації своїх прав, свобод і законних інтересів, здійснення завдань і функцій, що не порушує права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

В об'єктивному розумінні доступ до інформації – це сукупність правових норм, що регламентують суспільні інформаційні відносини щодо одержання їх учасниками відомостей, необхідних їм для реалізації своїх прав, свобод і законних інтересів, здійснення завдань і функцій" [12, с.73].

На нашу думку, здійснене автором визначення терміну доступності інформації досить логічне і його повнота не викликає сумнівів, водночас навряд чи можна погодитися з поділом доступності на суб'єктивне та об'єктивне право. Справа в тому, що в даному випадку право регулює інформаційні відносини, які завжди є об'єктивними, можливе лише суб'єктивне ставлення інформаційних суб'єктів до тих чи інших норм інформаційного права.

Для ефективності реалізації принципу доступності важливо те, що критерії оцінки інформаційної доступності нормативно визначені, зокрема, що стосується адміністративних послуг. Так, Постановою Кабінету Міністрів України "Деякі питання доступності інформаційно-комунікаційних систем та документів в електронній формі" від 21 липня 2023 року № 757 визначені основні критерії комплексного підходу до оцінки інформаційної доступності послуг, до яких зокрема, входять: адаптація веб-сайта для роботи на комп'ютері, смартфоні та планшеті; можливість зворотного зв'язку з відвідувачами; доступність мови та термінології; можливість отримати підказку, консультацію; інформування заявника про хід розгляду заяви / звернення; наявність інформації про послугу, порядок її надання; можливість подання документів або звернення для отримання послуги через онлайн-сервіси, поштою або особисто; отримання послуги через онлайн-сервіси, поштою, особисто. [13]. Одна з основних проблем – підвищення рівня медіаграмотності, обізнаності населення щодо отримання публічних послуг.

Досить часто до принципів управління інформаційною безпекою включають принцип захисту інформації, що дійсно є одним із ключових аспектів доступності, оскільки дає можливість забезпечити її цілісність, та конфіденційність. За висновком експертів: "Існує три основних принципи інформаційної безпеки: конфіденційність, цілісність, доступність. Разом ці принципи відомі як тріада ЦРУ. Кожна програма захисту інформації повинна дотримуватися цих принципів для досягнення максимальної ефективності".[14]. На нашу думку, захист інформації виступає складовою принципу доступності, як більш загального, його вторинним елементом, а магістральним напрямком забезпечення інформаційної безпеки, тобто її принципом є все ж доступність інформації.

Це підтверджується тим, що доступність пов'язана з категорією дійсності, яка відображає у свідомості людини об'єктивну реальність, тобто, існує безпосередньо. У разі зрівнювання понять доступності та захисту через феномен принципу, категорія доступності під впливом надмірної політики захисту може втратити свої власні закономірності функціонування, тобто, позбутись своєї необхідності, а значить, перестати діяти.

Таким чином, одним з основних завдань управлінської діяльності є вирішення питання подальшого формування організаційно – правових засад забезпечення прозорості дій влади, захисту персональних даних, безпекозабезпечувальним управлінням медійним простором.

До стратегічних принципів управління інформаційною безпекою в сучасних умовах широкомасштабної військової агресії рф та інформаційної війни проти України слід віднести також принцип пропаганди та контрпропаганди. Слід відзначити, що сучасна інформаційна політика в Україні за період війни рф проти України набула більш цілеспрямованого, активного характеру, однак все ще не відповідає потребам безпеки, захисту від інформаційної війни, яку веде рф проти України: інформаційний простір як України, так і інших держав перенасичений надуманими, вигаданими російською пропагандою фейками, перекрученням історичної реальності тощо, які здійснюють деструктивний вплив на свідомість українців, у негативному світлі висвітлюють діяльність української держави як у внутрішній, так і зовнішній політиці. Як відомо, навіть окремі посередники переговорного процесу з американської сторони щодо припинення вогню між військами рф та України публічно переповідають російські наративи. Тому розгляд питання пропаганди та контрпропаганди в протидії цій інформаційній війні на принциповому рівні, вважаємо, дасть можливість здійснювати цю роботу на більш вагомих, стратегічних засадах, а значить підвищити ефективність та результативність управлінських рішень у цій сфері.

Аналіз ефективності дії контрпропаганди України проти Росії, здійснений штучним інтелектом (ШІ) за програмою ChatGPT [15], відповідно до аналогічного запиту, свідчить про те, що на даний момент управлінська складова захисту інформаційної безпеки значно удосконалена, набула багатовимірного, і водночас, цілеспрямованого характеру. Відзначається, що Україна використовує в цій роботі комплексний підхід, поєднуючи офіційні заяви, соціальні мережі, медіапроєкти, міжнародну дипломатію та ініціативи громадянського суспільства. До основних факторів ефективності відносяться: швидкість реагування та факт-чекінг, українські офіційні джерела та незалежні медіа оперативно спростовують фейки російської пропаганди, реалізуються успішні кампанії, наприклад, “Армія дронів” або “Русский корабль, иди …”, які стають вірусними, західні ЗМІ часто посилаються на українські джерела, що зменшує вплив російської дезінформації, аналітичні центри та активісти (наприклад, Bellingcat) аналізують та викривають військові злочини РФ на основі відкритих даних і т.п.

Водночас відзначається можливість України ефективніше боротися з російською пропагандою, подолавши основні виклики, використовуючи такі стратегії: розширення міжнародної медіа присутності, вплив на громадську думку в інших країнах, зокрема, проведення інформаційних кампаній, що розвінчують міфи російської пропаганди (наприклад, через TikTok, Instagram, YouTube), робота з іноземними експертами, які можуть комунікувати правду своїм громадянам, збільшення впливу на російську аудиторію, адаптація контенту під російську аудиторію, посилення технічного захисту інформаційного простору тощо.

Стрижнем реалізації принципу пропаганди та контрпропаганди в інформаційній безпеці України, актуалізації контрпропагандистських кроків в Україні з питань протидії російській пропаганді очевидно, є розвиток такого її організаційного напрямку як стратегічні комунікації, який завдяки змістовному оновленню системи відносин, тісної взаємодії з громадськістю, цілеспрямовано формує таку організацію інформаційного простору, яка дозволяє в нинішніх складних умовах досягти безпекового ефекту. Згідно Стратегії інформаційної безпеки, “стратегічні комунікації – скоординоване і належне використання комунікативних можливостей держави – публічної дипломатії, зв’язків із громадськістю, військових зв’язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави” [7]. Функції стратегічних комунікацій, вважає Г. Почепцов, в тому, що вони,

“трансформуючи інформаційний простір, спрямовані на здійснення змін в інших просторах, враховують позицію опонента, скеровані на вузькі цільові групи” [16, с. 13].

Водночас практика управління інформаційною безпекою свідчить про все ще недостатню ефективність стратегічних комунікацій, яка може бути пов’язана з наступними причинами організаційного характеру:

- не відпрацьованість єдиної координації діяльності між міністерствами та відомствами, коли різні державні органи (РНБО, Міноборони, МВС, МКСК, СБУ) мають власні комунікаційні політики, що часто не узгоджені між собою;
- відсутність єдиного центру стратегічних комунікацій, який би забезпечував узгодженість інформаційної політики;
- повільна реакція на інформаційні загрози, запізнення з відповідями на інформаційні атаки рф, що є свідченням недостатньої активності контрпропагандистських акцій.
- потреба поліпшення системної підготовки фахівців у сфері стратегічних комунікацій;
- рівень довіри до державних інституцій залишається низьким через попередні невдачі у комунікаціях, українці більше довіряють незалежним ЗМІ або соцмережам, які також активно використовуються ворогом;
- потреба запровадження більш сучасних технологій для моніторингу та аналізу інформаційного простору та ін. проблеми.

Висновки.

Аналіз ефективності управлінського аспекту інформаційної безпеки України включає оцінку політики, у тому числі її організаційно - змістовних засад, координації державних органів, виконання стратегій і реагування на загрози.

Відзначається, що управління інформаційною безпекою України має розвинену нормативно-правову базу, міжнародну підтримку, інституційні механізми реалізації, але ефективність впровадження заходів знижується через слабку координацію між органами влади та недостатню швидкість реагування на загрози. Ступінь розробки засадних принципів управління інформаційною безпекою залишається на рівні окремих напрямків, цільових установок, і не досягає належного рівня узагальненості, що негативно позначається на їх регулятивній функції.

Пропонується власна узагальнена система принципів управління інформаційною безпекою, до якої введений принцип безпечного існування, який зумовлює потребу удосконалення управлінських механізмів розробки та впровадження державних стратегій безпеки, кризового менеджменту, підтримання стійкості критичної інфраструктури, а також нормативно-правового регулювання.

Акцентується увага на потребі актуалізації управління інформаційною безпекою з орієнтацією на безпеку окремої людини, індивіда, що має виступати наріжним управлінським принципом, входити до складу державних програм інформаційного захисту, який створює необхідні умови для безпечного існування. Потребує удосконалення також механізм управління медійним простором для уникнення дезінформації.

Внесено новації до розуміння принципу доступності інформації як балансу між відкритістю та потребами конфіденційності, запропоновано організаційні заходи більш ефективного законодавчого забезпечення прозорості влади (доступ до публічної інформації), захисту персональних даних.

Принцип пропаганди і контрпропаганди має на меті управління інформаційним впливом як підтримку державної політики, так і протидію маніпуляціям та

інформаційним атакам. Відзначено, що стратегічні комунікації нині є одним з основних організаційних методів забезпечення безпеки інформаційного простору України, ефективним механізмом протидії російській пропаганді. Окреслено ключові управлінські проблеми реалізації методу стратегічних комунікацій: нерозуміння принципів формування комунікативних стратегій, слабка підготовка спікерів та відсутність якісної взаємодії з цільовими аудиторіями. Це вимагає розвитку кризових і стратегічних комунікацій та навчання відповідальних фахівців.

Таким чином, ефективне управління безпекою та інформаційною політикою потребує комплексного підходу, що включає наукове обґрунтування, орієнтації на узагальнені принципи управління, удосконалення правового регулювання взаємодії державних інституцій та громадянського суспільства.

Використана література.

1. Система безпеки NIST Cybersecurity Framework URL: https://www.nist.gov/cyberframework - дата звернення - 4.04.2025.

2. Система безпеки ISO 27001 - ISO/IEC 27001 Information Security Management Systems - https://www.udemy.com/course/iso27001-information-security-management- systems - lfnf pdthytyyz – 4.04.2025.

3. Управління інформаційною безпекою: конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1114 Кбайт). Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с.

4. Олійник О.В. Принципи забезпечення інформаційної безпеки України. *Науковий вісник Ужгородського університету, 2012 Серія ПРАВО.* Випуск 18. С.170-173.

5. Низюк Є. Принципи забезпечення інформаційної безпеки підприємства в умовах неоіндустріального суспільства. *Інноваційний розвиток та безпека підприємств в умовах неоіндустріального суспільства*: матеріали Міжнар. наук.-практ. конф. (27 жовт. 2020 р.) / відп. ред. О. М. Полінкевич, Л. В. Шостак. Луцьк: ВНУ ім. Лесі Українки, 2020. 754 с.

6. Лисенко С.О. Принципи державного управління інформаційною безпекою та їхня характеристика. *Серія: Публічне управління і адміністрування*. ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», 2024. № 1 С.169-174.

7. Указ Президента України №685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки».

8. Тихий В. П. Безпека людини: поняття, правове забезпечення, значення, види. *Вісник Національної академії правових наук України*. № 2 (85) 2016. С.31-46.

9.Золотар О.О. Інформаційна безпека людини:теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

10. Кукін І.В. Механізми державного управління інформаційною безпекою особистості : реферат дисертації. Київ, 2024. 40 с.

11. Закон України “Про інформацію» від 02.10.1992 № 2657-XII (Чинний)

12. Марущак А.І. Визначення поняття «доступ до інформації» *Правова інформатика*, 2006. № 3 (11)/2006. С. 69-74.

13. Постанова Кабінету Міністрів України «Деякі питання доступності інформаційно-комунікаційних систем та документів в електронній формі» від 21 липня 2023 року № 757.

14. What are the Principles of Information Security? ZenGRC Team · August 30, 2024). URL: https://www.zengrc.com/blog/what-are-the-principles-of-information-security/ дата звернення – 27.03.2025р.

15. Програма штучного інтелекту Chat GPT. URL: https://www.google.com.ua/search? – дата звернення – 27.03.2025.

16. Почепцов Г. Стратегічні комунікації: стратегічні комунікації в політиці, бізнесі та державному управлінні. Київ: Альтерпрес, 2008. 216 с.