PUBLIC ADMINISTRATION

ДЕРЖАВНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В ТУРБУЛЕНТНОМУ СУСПІЛЬСТВІ

Панченко О. А.,
Заслужений лікар України, доктор медичних наук, професор, директор ДЗ «Науково-практичний медичний реабілітаційно-діагностичний центр МОЗ України», Президент Громадської організації «Всеукраїнська професійна психіатрична ліга», м. Київ, Україна
ORCID: https//orcid.org/0000-0001-9673-6685

DOI: https://doi.org/10.31435/rsglobal_ws/31052020/7082

ARTICLE INFO

Received: 18 March 2020
Accepted: 13 May 2020
Published: 31 May 2020

KEYWORDS

Security,
informationsecurity,
turbulence,
turbulentsociety,
publicadministration.

ABSTRACT

The article examines the main state management approaches to information security in terms of ascertaining the turbulent state of modern society.
State management of information security is considered based on security interpretation in terms of risk management. There are four paradigms of information security management specified: systemic, synergetic, phenomenological, and cognitive. It is emphasized that the above approaches to public administration, firstly, are not demarcated and universal, and secondly must consider the peculiarities of the management process that inevitably arise in a situation of growing turbulence in society, nature, and the technosphere. In conditions of turbulence, new approaches are proposed, one of which may be the concept of heterogeneity. In this case, the emphasis in information security management should be on the micro-level, ie on direct practices of interaction that consider local specifics and features.

Citation: Панченко О. А. (2020) Derzhavne Upravlinnia Informatsiinoiu Bezpekoiu v Turbulentnomu Suspilstvi. *World Science.* 5(57), Vol.3. doi: 10.31435/rsglobal_ws/31052020/7082

Актуальність теми дослідження. Сучасний етап світового розвитку за сукупністю економічних, політичних, екологічних, культуральних, інформаційних трансформацій набув ознак епохи турбулентності, що характеризується низкою важливих особливостей: плинність, нестійкість, невизначеність. Представники соціальних і економічних наук почали вживати терміни «турбулентні часи», «турбулентний світ», «соціальна турбулентність», «турбулентний соціум» (наприклад, [1-5]).Серед науковців існує думка, що саме інформатизація суспільства призвела до прискорення появи нових тенденцій у світовому розвитку, адже інформація супроводжує всі сфери суспільних відносин. Характеризуючи «турбулентні часи», О.Н. Яницький виділяє опосередковано декілька негативних сторін процесу інформатизації» [6]:

– процес вимагає більшої прозорості інформаційних відносин, а це неминуче призводить до порушення прав і свобод;

– прихід «пост-паперової» культури істотно змінює структуру і функції інститутів управління, освіти і науки;

– загострюється боротьба між глобальними гравцями за роль «програмістів» і «перемикачів» засобів масової інформації і комунікації, мережевих систем, за допомогою яких формується глобальна політика.

В. Моско вважає, що нині відбувається перехід від постіндустріального і постінтернетного суспільства до суспільства цифрового, побічні ефекти якого змінюють власне людські комунікації на людино-машинні, які в свою чергу радикально змінюють природу влади, насильства і справедливості [7].

У. Вандербург підкреслює, що диджиталізація представляє не тільки блага, але і ряд негативних побічних ефектів даного процесу [8]. На його думку, в сучасному суспільстві утвердився соціальний тип «гомо інформатикус». Крок за кроком світ робиться безпечним для техніки і небезпечним для людей, співтовариств і екосистем.

Отже хаотичні нелінійні процеси в суспільстві, в тому числі і інформаційного характеру, мають вирішальний вплив на життя сучасної людини. Особливе значення в турбулентному суспільстві набуває управління безпекою.

У наших попередніх роботах досліджувалась турбулентність інформаційного середовища і пов'язані з цим явищем проблеми психологічної турбулентності, особистістних і суспільних відносин, забезпечення інформаційно-психологічної безпеки, втому числі і за рахунок формування турбулентного мислення [9-11].

В той же час набуває актуальності розгляд інформаційної безпеки у ракурсі державного управління. Збої у системі інформаційної безпеки можуть привести до економічних, соціально-політичних, і техногенних зрушень, аж до підриву належного функціонування держави.

Мета статті – визначити головні державні управлінські підходи до забезпечення інформаційної безпеки з точки зору констатації турбулентного стану сучасного суспільства.

Виклад основного матеріалу.

Будь-яке дослідження починається з визначення понять, що розкривають його сутність. В даному контексті вихідним поняттям є безпека, яка є об'єктом управління. В теорії безпеки життєдіяльності добре відома аксіома про потенційну небезпеку: «Всі дії людини і всі компоненти середовища існування, насамперед, технічні засоби і технології, крім позитивних властивостей і результатів, мають здатність генерувати травмуючі і шкідливі фактори. При цьому, будь-яка нова позитивна дія або результат неминуче супроводжуються виникненням нових негативних факторів». [12]. В умовах турбулентного суспільства цей принцип правомірно використовувати для оцінки не тільки технічних, а й соціальних, економічних, політичних систем. Невизначеність середовища, в якій протікає життя людини, нестійкість соціальних і природних процесів змушує розглядати це середовище як потенційне джерело різних небезпек, загроз, факторів ризику і приймати запобіжні заходи забезпечення безпеки. Оскільки сучасна людина крім природного і соціального знаходиться ще і в інформаційному середовищі, логічно в цьому контексті вести річ і про інформаційну безпеку.

Сутність управлінських підходів розглядається нами на основі трактування безпеки в термінах управління ризиками. На відміну від загроз ризики підкреслюють динамічний характер викликів, що виникають в турбулентному суспільстві. Найбільш відповідне трактування безпеки в такому ракурсі дає Н. Луман, який ототожнює безпеку зі збереженням і розуміє як відсутність втрат, забезпечене індивідуальною калькуляцією ризиків, успішне конструювання ситуації [13]. Схоже трактування пропонує А.І. Поздняков [14], де безпека визначається як захищеність цінностей суб'єкта (держави, суспільства, особистості) від небайдужого для цього суб'єкта збитку. При цьому можна використовувати простий і зрозумілий критерій рівня небезпеки – ймовірний збиток або ризик в широкому його трактуванні.

Ризик – поняття, що має багато значень, але в даному випадку зрозуміло, що річ іде про можливі події, явища і процеси, наслідки яких можуть мати несприятливий вплив на різні аспекти стану людського життя (в тому числі і на інформаційну безпеку).

Управління безпекою передбачає не тільки розрахунок-вимір ризиків, але також зниження і управління ними. Рівень того чи іншого ризику кількісно характеризує ефективність прийнятих заходів безпеки. Діяльність по їх плануванню та здійсненню є безпосередньою функцією державного управління. Тому, на наш погляд, закономірно трактувати рівень захищеності населення від впливу інформаційних ризиків, рівень забезпечення інформаційної безпеки, як критерій оцінки ефективності управління.

В самому загальному вигляді інформаційна безпека – *цестан інформаційного середовища, який забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин, безпеку інформації та захист суб'єктів від негативного інформаційного впливу.* В

даному визначенні суб'єктами інформаційних відносин можуть бути: держава, суспільство, організація, людина.

У контексті національної безпеки, інформаційна безпека може розглядатися, з одного боку, як самостійний її елемент, а з іншого – як інтегрована складова будь-якої іншої безпеки: військової, економічної, політичної і т.д. У такому руслі більш повним визначенням інформаційної безпеки можна вважати наступне: «інформаційна безпека – це стан захищеності життєво важливих інтересів особистості, суспільства і держави, при якому зводиться до мінімуму завдання шкоди через неповноту, невчасність та невірогідність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації»[15]. Але і це визначення не розкриває всю сутність поняття, адже воно дається в статичних категоріях. Найбільш доречним нам видається динамічний підхід, який показує дії задля забезпечення належного стану суб'єкта. Релевантним у цьому плані виглядає визначення А.Д. Урсул, Т. (Ф). Н. Цирдя[16], яке з нашими правками виглядає наступним чином: інформаційна безпека – «здатність держави, суспільства, соціальної групи, особистості, по-перше, забезпечити з певною ймовірністю достатні і захищені соціальний інтелект і інформаційний ресурс, оптимальну соціальну ентропію і інформаційне середовище для підтримки життєдіяльності і життєздатності, стійкого функціонування і розвитку соціуму; по-друге, протистояти інформаційним небезпекам і загрозам, негативним інформаційним впливам на індивідуальну і суспільну свідомість і психіку людей, а також на комп'ютерні мережі та інші технічні джерела інформації; по-третє, виробляти особистісні та групові навички та вміння безпечної поведінки; по-четверте, підтримувати постійну готовність до адекватних заходів в інформаційному протиборстві, ким би воно не було нав'язане; по-п'яте, постійно і послідовно за певною безпечною програмою «вмонтувати» штучний інтелект в суспільне середовище».

Що до сутності державного управління, то воно розглядається нами як один із видів соціального в широкому трактуванні, тобто є особливою функцією, що виникає з потреб суспільства як самодостатньої системи та здійснюється у відповідних державних чи недержавних формах шляхом організаторської діяльності спеціально створеної для цього групи органів. Головне, що система державного управління повинна бути близькою до потреб суспільства, підконтрольною йому, прозорою та ефективною.

Беручи до уваги дослідження Щекотина Є.В.[3], та базуючись на власному аналізі, було виділено чотири парадигми управління інформаційною безпекою.

Перша опирається на системний підхід і бере до уваги ряд базових постулатів: система є цілісним і якісно своєрідним утворенням; вона знаходиться в стані динамічної рівноваги з середовищем і здатна самовідтворюватися. Ризик у парадигмі системного підходу потрібно розуміти як порушення рівноваги системи, що виникає внаслідок неузгодженості елементів всередині системи або впливу зовнішніх факторів. В основі управління ризиком лежить максимально повний облік всіх можливих дестабілізаційних факторів, вразливостей, як всередині, так і зовні системи.

Управління ризиком повинно бути зосереджено на розробці і впровадженні заходів, що сприяють підвищенню стійкості системи до внутрішніх та зовнішніх чинників нестабільності. Як правило, така сукупність заходів спрямована на посилення контролю над елементами системи, над каналами взаємодії із зовнішнім середовищем. Системний підхід в управлінні ризиками полягає в посиленні заходів контролю, секретності, чітке розрізнення потенційних загроз і ризиків, калькуляція можливих втрат і т.д. Такий підхід характерний для систем, де інформаційна безпека є складовою державної, військової, банківської і т.п. безпек.

Друга базується на синергетичному підході, що є розвитком системного підходу. В даному підході розглядаються нелінійні динамічні системи, еволюція яких визначається внутрішніми процесами самоорганізації. Синергетичний підхід в управлінні спрямований на створення умов для саморозвитку системи, можливостей еволюціонувати в напрямку властивих системі характеристик і цілей.

В синергетичній парадигмі ризик розглядається як ймовірність реалізації катастрофічного сценарію еволюції системи. Система у неврівноваженому стані знаходиться під загрозою руйнування, і в цьому випадку управління ризиком вимагає більше не калькуляції втрат, а здатності передбачати можливі сценарії і робити попереджувальні дії на ранніх етапах.

Враховувати потрібно не тільки системні чинники небезпеки і загрози, а й їх можливе взаємне накладення, резонанс взаємно підсилюючих нелінійних коливань.

У даній парадигмі управління ризиками слід розцінювати як вплив на поведінку системи для того, щоб уникнути руйнівних наслідків. Важливо підкреслити зв'язок ризику і темпоральності явища. У період нестійкості системи ризик різко зростає, чутливість до випадкових факторів загострюється. У зв'язку з цим особливого значення набуває здатність управлінця передбачати траєкторії руху системи по слабким сигналам.

Прикладом застосування синергетичного підходу в управлінні є сценарні прогнози, наприклад, щодо інформаційного ажіотажу навколо проблеми коронавірусу.

Третя парадигма управління – феноменологічна. Для пояснення її сутності наведемо декілька супутніх понять. Згідно класичного визначення Е. Гуссерля, *феноменологія* – дескриптивна наука про сутності трансцендентально чистих переживань в межах безпосередньої інтуїції. Ф*еноменологічний підхід* – розгляд проблем управління з позицій життєвого досвіду і особистісного сенсу учасників спільної діяльності, тих інтерсуб'єктивних значень предметів, якими люди керуються при прийнятті рішень [17]. *Інтерсуб'єктивність*– здатність людини в процесі комунікації встановлювати співвідношення між декількома точками зору – своєї і чужої, тобто враховувати, порівнювати, протиставляти, примиряти різні точки зору на об'єкти і події [18].

Виходячи з наведених визначень, можна констатувати, що першочерговими у феноменологічному підході є питання цінностей, значень, переконань людей, підтримання прийнятого порядку і т.д. Управлінський вплив, щоб бути ефективним, направляється на релевантні предмети життєвого середовища та проблемні життєві ситуації, він повинен враховувати ситуативний характер взаємодії. Умовою ефективного управління є розуміння тієї реальності, в якій живуть різні люди і спільноти, знання механізмів конструювання інтерсуб'єктивності реальності, здатність до виявлення неявних ознак, фонових очікувань, фонових знань, що лежать в основі інтерпретації дій і подій. У цьому контексті доречно згадати введене нами поняття *турбулентне мислення:* мислення, засноване на неформальному, евристичному підході до аналізу ситуації і прийняття рішень (досвід, інтуїція, винахідливість і т.д.), що приводить до формування умов для забезпечення інформаційної безпеки.

У феноменологічній парадигмі ризик пов'язаний з неправильним розумінням, неузгодженістю смислів, якими люди наділяють події і дії, розбіжність ціннісних орієнтирів. Державне управління ризиком має бути спрямоване на прояснення значень, встановлення прозорості смислових систем, коригування ціннісних установок суб'єктів взаємодії. Тому величезне значення набуває комунікація, узгодження ціннісно-смислових орієнтирів керманичів і керованих.

Феноменологічний підхід в управлінні інформаційною безпекою важливий, коли мова заходить про оцінку тих чи інших подій і явищ як ризикованих, ступеня їх небезпеки для суспільства, сприйнятті соціальних ризиків і т.д.

Четвертий підхід – когнітивний, що набув широкого поширення в зв'язку з розвитком концептуальних моделей «суспільства знання», «інформаційного суспільства», «постіндустріального суспільства», і т.п. У всіх цих концепціях підкреслюється зростання ролі знання і наукомістких технологій для процесу виробництва і управління.

Якщо розглядати ризик з позиції когнітивного підходу, то його можна інтерпретувати як форму знання. Ризик – це знання, інформація про можливі небезпеки. Управління ризиками в рамках даної парадигми пов'язане з кваліфікованою експертизою ситуації, ризик-комунікацією (своєчасне інформування суспільства про ризики) і т.д. Яскравим прикладом реалізації когнітивного підходу в управлінні безпекою – це феномен інформаційних війн, який набуває все більшого значення у зв'язку з розвитком засобів масової комунікації.

Повертаючись до визначення інформаційної безпеки, дане А.Д. Урсул, Т. (Ф). Н. Цирдя, можемо стверджувати, що кожен із його пунктів в тій чи іншій мірі може бути забезпечений наведеними управлінськими підходами. В той же час, слід зазначити, що наведені підходи до державного управління, по-перше, не є універсальними і обособленими в якомусь конкретному випадку, тобто вони мають системний характер, і управлінець повинен уміти комплексно застосовувати підходи в залежності від ситуації; по-друге, повинні враховуватися особливості процесу управління, що неминуче виникають в ситуації зростаючої турбулентності в

суспільстві, природі та техносфері. Треба брати до уваги той факт, що при аналізі підходів до управління інформаційною безпекою зазвичай береться за основу базове припущення про можливу редукцію ризиків до гомогенної абстрактної схеми їх взаємодії. У той же час в умовах соціальної турбулентності особливо важливим виявляється враховувати їх гетерогенність. Так, у випадку системного підходу за основу береться припущення типізації керованих елементів, тобто гомогенність в цьому контексті означає встановлення фактичної їх рівності (або, щонайменше, еквівалентності). Абстрактний підхід розширює можливості контролю за поведінкою, обчислення строгих алгоритмів поведінки. Однак в ситуації турбулентності, коли керовані елементи стають «текучими об'єктами» такі системи стають занадто громіздкими і неефективними. Вони просто не встигають слідом за потоками. Наприклад, Х. Молотч в роботі з характерною назвою «Проти безпеки» показує основні недоліки сформованої «мілітаристської» ідеології [19]. Побудовані за стандартизованими схемами, ці системи безпеки спрямовані на уніфікацію, посилення контролю і неухильне підпорядкування цим абстрактним правилам. На численних прикладах Х. Молотч показує, що такі «мілітаристські» системи виявляються нездатними запобігти терактам і часто самі стають причиною численних неприємностей і навіть небезпеки для населення. З цього можна зробити висновок, що складні закриті системи, що базуються на посиленні контролю як головному інструменті в забезпеченні інформаційної безпеки методами уніфікації і конструюванні абстрактних типів, закритості і суворому розмежуванні, універсальності правил і схем і т.д., ефективні для стабільних суспільств, в яких ступінь дифузії, рухливості і проникності кордонів невелика.

В умовах же соціальної турбулентності потрібні нові підходи, одним із яких може стати концепт гетерогенності. У цьому випадку акцент в управлінні інформаційною безпекою повинен бути зроблений на мікрорівні, тобто на безпосередніх практиках взаємодії, які враховують локальну специфіку і особливості. Держава повинна зменшити монополію на управління інформаційною безпекою та делегувати більш широкі повноваження місцевому самоуправлінню, суспільним та громадським інститутам, які є більш динамічними в розрахунку-виміру ризиків і управлінні ними.

Висновки. Державне управління інформаційною безпекою, що розглядається на основі трактування безпеки в термінах управління ризиками, на відміну від загроз, враховує динамічний характер викликів, що виникають в турбулентному суспільстві.

Управління інформаційною безпекою базується на чотирьох парадигмах: системна, синергетична, феноменологічна та когнітивна. При цьому зазначені підходи до державного управління, по-перше, не є розмежованими та універсальними, по-друге повинні враховувати особливості процесу управління, що неминуче виникають в ситуації зростаючої турбулентності в суспільстві, природі та техносфері.

В умовах турбулентності пропонуються нові підходи, одним із яких може стати концепт гетерогенності. У цьому випадку акцент в управлінні інформаційною безпекою повинен бути зроблений на мікрорівні, тобто на безпосередніх практиках взаємодії, які враховують локальну специфіку і особливості.

ЛІТЕРАТУРА

1. Гринберг Р. С. Основне проблемы современного турбулентного мира. Гуманитарий Юга России. 2013. Том. 0. № 2. С. 22-28.
2. Резеньков Д.Н., Приходько С.С. Понятие «социальная турбулентность» в современном мире в концепции информационной безопасности России. Культура и общество: история и современность. Материалы II Всероссийской (с международным участием) научно- практической конференции. Под редакцией Колосовой О.Ю, Гударенко Р.Ф., Ряснянской Н.А, Красиковой Е.А. Ставрополь. Издательство ООО «Ветеран».2013. С. 128-130.
3. Щекотин Е.В. Социальное управление в турбулентном обществе: вопросы безопасности и риска. Социум и власть. 2016. № 1 (57). С. 87-92.
4. Щекотин Е.В. Проблема благополучия в турбулентном социуме: аспект безопасности. Вестник науки Сибири. 2017. №4 (27). С. 74-83
5. Чудинов С. И., Щекотин Е. В. Турбулентный социум и концепция безопасности : социально-философские аспекты: монография. Новосибирск: Изд-во НГТУ. 2018. 159 с.
6. Яницкий О.Н. «Турбулентные времена» как проблема общества риска. Общественные науки и современность. 2011. № 6. С. 155-164.

7. Vinsent Mosco. Becoming Digital: Toward a Post-Internet Society. London: Emerald Publishing Limited. 2017. 227p.
8. Vanderburg W.H. Our battle for the human spirit :scientifick nowing, technical doing, and daily living. Toronto: University of Toronto Press. 2016. 421p.
9. Панченко О.А. Психологические аспекты турбулентности информационной среды. Причорноморські психологічні студії. 2017. Вип.1.С. 3–7.
10. Панченко О.А. Турбулентность в информационной безопасности личности. Клінічна інформатика і телемедицина. 2017. Т. 12. Вип. 13. С. 124–129.
11. Панченко О.А. Психологическая турбулентность в условиях информационной войны. 2018. URL: http://www.psyh.kiev.ua/Панченко_О.А._Психологическая_турбулентность_в_условиях_информационной_войны (дата обращения: 21.03.2020).
12. Безопасность жизнедеятельности: учеб. для вузов. Под общ. ред. С.В. Белова. М.: Высшая школа. 1999. 40 с.
13. Luhman N. Risk: a sociologi caltheory. N.Y.: AldinedeGruyter. 1993. 236 p.
14. Поздняков А. И.. Сравнительный анализ основных методологических подходов к построению теории национальной безопасности. Национальные интересы: приоритеты и безопасность. 2013. №21 (210). С. 46-53.
15. Ільницька Уляна. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. URL: http://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf.
16. Урсул А. Д., Цырдя Т. (Ф). Н. Информационная безопасность. Сущность, содержание и принципы ее обеспечения. URL: http://security.ase.md/publ/ru/pubru22.html (дата обращения 13.05.2020).
17. Социология управления: теоретико-прикладной толковый словарь. Отв. ред. А.В. Тихонов. М.: КРАСАНД. 2015. 480 с.
18. СКоДис. URL: http://scodis.ru/студентам/глоссарий/интерсубъективность/ (дата обращения 13.05.2020).
19. Molotch H. Against Security: How WeGo Wrongat Airports, Subways, and Other Sitesof Ambiguous Danger. Princeton, Oxford: Princeton University Press. 2014. 288 p.