МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

Г.П. СИТНИК, Г.П. ЗАВОРІТНЯ, Р.Р. МАРУТЯН

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Навчальний посібник

Академ прес
Київ - 2024

УДК 351.86:004:005.3/.4](075.8)
С-41

Рекомендовано до друку Вченою Радою Навчально-наукового інституту публічного управління та державної служби (протокол № 6 від 6 листопада 2024 року)

Рецензенти:

***Д.А. Купрієнко**, доктор військових наук, професор, Національна академія Державної прикордонної служби імені Богдана Хмельницького*

***О.С. Твердохліб**, доктор наук з державного управління, професор, Інститут державного управління та наукових досліджень у сфері цивільного захисту*

***Н.М. Корчак**, доктор юридичних наук, професор, Київський національний університет імені Тараса Шевченка*

Ситник Г.П., Заворітня Г.П., Марутян Р.Р.

С-41 **Інформаційно-комунікаційні технології у сфері національної безпеки**: навчальний посібник / за заг. ред. Г.П. Ситника ; ТОВ «Академпрес». – Київ, 2024. – 176 с.

ISBN 978-966-7541-59-0

У навчальному посібнику викладено найважливіші теоретичні та практичні питання щодо ролі інформації, інформаційно-аналітичної діяльності та ІКТ в управлінні у сфері національної безпеки та практичні аспекти їх використання у вказаній сфері

Посібник підготовлено у відповідності з робочою навчальною програмою дисципліни «Інформаційно-комунікаційні технології у сфері національної безпеки»», яка є компонентом освітньої програми «Урядування у сфері національної безпеки» бакалаврського освітнього рівня за якою навчаються студенти Навчально-наукового інституту публічного управління та державної служби Київського національного університету імені Тараса Шевченка (спеціальність 256 - «Національна безпека (за окремими сферами забезпечення і видами діяльності)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону»).

Посібник також може бути корисними і для фахівців, на яких покладаються аналітичні, консультативно-дорадчі й організаційно-розпорядчі функції щодо адекватного реагування на загрози національним інтересам України в межах своєї професійної компетенції.

УДК 351.86:004:005.3/.4](075.8)

ISBN 978-966-7541-59-0

ЗМІСТ

ПЕРЕДМОВА

Головним наслідком науково-технологічної революції є стрімкий розвиток інформаційно-комунікаційних технологій (ІКТ) та становлення на цій основі нової форми цивілізації, яку почали називати «інформаційним суспільством». Тому визначальним стратегічним ресурсом розвитку суспільства та держави стала інформація, ефективне накопичення та використання якої у всіх сферах суспільного життя стало неможливим без впровадження ІКТ. Таким чином, у сучасному світі інформаційна складова визначає сутність основних суспільних процесів та управління, серед яких особливе місце посідає сектор оборони і безпеки.

На жаль багато помилок в управлінні у сфері національної безпеки є наслідком того, що нерідко важливі рішення ухвалюються, без належного врахування впливу на різні підсистеми взаємозалежного суспільного організму інформаційно-комунікаційного аспекту управлінської діяльності. Водночас, володіння основами знань щодо ролі інформації та інформаційно-аналітичної діяльності в управлінні у сфері національної безпеки, а також практичних аспектів використання ІКТ у вказаній сфері є важливим елементом культури сучасного управлінця. Врешті-решт, будь-який фахівець змушений «мати справу» з систематизацією інформації, яку можна здійснювати лише володіючи спеціальними знаннями і навичками. Особливо це важливо для фахівців-управлінців, які приймають рішення або готують відповідні пропозиції щодо забезпечення національної безпеки.

Виходячи з цих міркувань, була розроблена робоча навчальна програма дисципліни «Інформаційно-комунікаційні технології у сфері національної безпеки». Вона є обов"язковим компонентом освітньої програми «Урядування у сфері національної безпеки» за якою навчаються студенти бакалаврського освітнього рівня Навчально-наукового інституту публічного управління та державної служби Київського національного університету імені Тараса Шевченка (спеціальність 256 -«Національна безпека (за окремими сферами забезпечення і видами діяльності)» галузі знань 25 «Воєнні

науки, національна безпека, безпека державного кордону»). У відповідності з вказаною робочою навчальною програмою підготовлено цей навчальний посібник. Він складається з трьох розділів.

Перший розділ «Роль інформації в управлінні у сфері національної безпеки», спрямований на формування у студентів сукупності знань про: інформацію як специфічну субстанцію (проблема розкриття змісту концептів «інформація» та «інформаційна безпека», їх об'єктивно-суб'єктивна природа; інформація, як атрибут буття об'єктів соціальних взаємодій та підходи щодо розкриття її змісту); інформаційну компоненту влади та національної безпеки (інформація як джерело влади, чинник забезпечення державної безпеки та соціального порядку; інформація як чинник модернізації державного управління та цілі сучасних інформаційних війн; роль інформації у сфері національної безпеки та інформаційна складова масової культури); інформаційний аспект управлінської діяльності у сфері національної безпеки (роль інформації в управлінні у сфері національної безпеки та еволюція різних аспектів її сутності; роль інформації в суб'єкт-об'єктній взаємодії в управлінні та як її системоутворювальний фактор).

Другий розділ «Інформаційно-аналітична діяльність у сфері національної безпеки» спрямований на формування у студентів сукупності знань про: інформаційно-аналітичну діяльність як складову управління у сфері національної безпеки (інформаційно-аналітична діяльність та взаємозалежність управлінської інформації і управлінських функцій; класифікація управлінської інформації та вимоги до соціальної інформації; особливості аналітичної діяльності в управлінні та його інформаційно-аналітичне забезпечення; зміст та основні завдання інформаційного та інформаційно-аналітичного забезпечення у сфері національної безпеки); ІКТ та проблеми їх розвитку у контексті національної безпеки (взаємозвязок інформації та інформаційних технологій та етапи їх розвитку; структура ІКТ та інформатизація суспільства; компоненти створення та функціонування ІКТ та виклики, які є наслідком їх розвитку; класифікація новітніх ІКТ у контексті забезпечення

безпеки та стандарти їх розвитку; проблема захисту ІКТ від кіберзагроз та проблемні питання їх розвитку в Україні); кризові ситуації у соціальних системах (співвідношення кризових та надзвичайних ситуацій та світоглядний аспект природи кризових ситуацій соціального характеру; нормативно-правове трактування кризових ситуацій та поняття "криза", як вимір буття соціальної системи; характерні риси кризової ситуації, як об'єкта управління та їх стадії).

Третій розділ «Практичні аспекти використання ІКТ у сфері національної безпеки» спрямований на формування у студентів сукупності знань про: використання інформаційних систем при прийняття рішень у сфері національної безпеки (переваги автоматизації процесів прийняття рішень та компоненти інформаційної системи управління; класифікація інформаційних систем; інформаційні системи підтримки прийняття управлінських рішень); проксі-війни як простір використання сучасних ІКТ (проксі-війни: поняття, причини, історія ведення; гібридна війна як простір невизначеності та інформаційний аспект кризових ситуацій; новітні інформаційні та кібер компоненти гібридної війни; можливості та пріоритети розвитку штучного інтелекту в Україні у контексті гібридної війни); стратегічні комунікації та стратегічні наративи як інструменти досягнення цілей політики національної безпеки (поняття та складові стратегічних комунікацій; стратегічні наративи як інструмент досягнення цілей політики національної безпеки; інфодемія як результат неефективних стратегічних комунікацій, її наслідки та інструменти протидії).

Наприкінці кожного розділу наведено запитання та завдання для самоконтролю, список рекомендованої літературу, а в кінці навчального посібника – перелік тем для самостійних робіт та список використаних при його підготовці джерел.

Таким чином, наведений у навчальному посібнику матеріал є органічним поєднанням знань щодо системних уявлень про роль інформації та ІКТ в управлінні у сфері національної безпеки та практичні аспекти їх використання ІКТ у вказаній сфері Тому головною метою навчального посібника є розвиток у майбутніх фахівців-управлінців у сфері національної безпеки системи знань про роль інформації та ІКТ в управлінні

у сфері національної безпеки як передумови формування у них вмінь і навичок, які дозволять їм розв'язувати складні спеціалізовані завдання щодо адекватного реагування на загрози національним інтересам України в межах своєї професійної компетенції, у тому числі в умовах кризових ситуацій.

Автори висловлюють щиру подяку своїм колегам, друзям та шановним рецензентам за зауваження та пропозиції, які надійшли від них під час редагування остаточного варіанта тексту навчального посібника.

РОЗДІЛ 1
РОЛЬ ІНФОРМАЦІЇ В УПРАВЛІННІ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

ГЛАВА 1. ІНФОРМАЦІЯ ЯК СПЕЦИФІЧНА СУБСТАНЦІЯ

1.1. Проблема розкриття змісту концептів «інформація» та «інформаційна безпека», їх об'єктивно-суб'єктивна природа

Стан вирішення проблеми розкриття змісту концептів «інформація» та «інформаційна безпека». В сучасну епоху інформація є основним джерелом влади та визначальним ресурсом суспільного розвитку, а відтак невід'ємним атрибутом соціальних взаємодій. Тому вона може використовуватися не тільки як ресурс щодо забезпечення національної безпеки, а й бути фактором, який породжує небезпеки для неї. З огляду на сказане проблема забезпечення інформаційної безпеки постійно перебуває у колі наукового дискурсу.

Водночас продовжує мати місце відсутність одностайного трактування понять, які використовуються науковцями та в нормативно-правових актах, у яких розглядаються ті чи інші аспекти інформаційної складової національної безпеки.

Це зумовлює світоглядну та методологічну невизначеність при вирішені комплексної проблеми щодо забезпечення національної безпеки та інформаційної безпеки зокрема, у тому числі при побудові інформаційно-комунікаційних систем.

З огляду на це актуальним завданням залишається подальше уточнення сутності концепту (поняття) «інформація» та пов'язаних з нею соціальних явищ, зокрема "інформаційної безпеки" шляхом визначення її ознак крізь призму властивостей інформації, як специфічної субстанції.

Є всі підстави стверджувати, що сьогодні проблемі забезпечення національної безпеки та її складової інформаційної безпеки належить одне з лідируючих місць серед

наукових публікацій. При цьому представники різних галузей знань акцентують увагу на тому, що в сучасних умовах боротьба за інформаційні ресурси та необхідність їх захисту потребує іншої моделі поведінки суб'єктів управління, особливо в кризових ситуаціях.

Тому різним аспектам проблеми забезпечення інформаційної безпеки присвятили свої роботи багато науковців, зокрема, О. Архипов, Є. Архипова, І. Арістова, У. Ільницька, О. Рижук, Д. Сулацький, А. Турчак, В. Шаньгін.

Ці та інші автори здійснювали аналіз інформації та інформаційної безпеки людини, як споживача телекомунікаційних послуг, парадигм забезпечення інформаційної безпеки, підходів щодо з'ясування її сутності, сучасних викликів та загроз негативних інформаційно-психологічних впливів.

Не залишалася проблема забезпечення інформаційної безпеки й поза увагою вітчизняних законодавців.

Проте виконаний нами аналіз дозволяє дійти висновку, що в наявних наукових дослідженнях, сутність явища, яке позначають поняттям "інформація" та "інформаційна безпека" недостатньо розкрита передусім у контексті властивостей інформації, як специфічної субстанції, що є важливою передумовою його розкриття і в цілому забезпечення національної безпеки.

Вказаний аналіз також свідчить, що проблеми інформаційної безпеки в інформаційно-комунікаційних системах вирішуються головним чином у контексті захисту інформації, а от проблема віртуалізації середовища, захисту від деструктивного інформаційного впливу, руйнування культурно-цивілізаційної ідентичності не займає гідного місця в науковому дискурсі щодо вирішення комплексної проблеми забезпечення національної безпеки.

Таким чином, незважаючи на значний науковий доробок у науковців відсутня єдність у розумінні сутності інформаційної безпеки, що не дозволяє сформувати системні уявлення про проблемне поле формування адекватних управлінських рішень щодо реагування на небезпеки інформаційній безпеці, й, відповідно, створення та забезпечення належного

функціонування інформаційно-комунікаційних технологій та систем. Тому актуальним завданням залишається подальша концептуалізація соціального явища, яке позначають поняттями "інформація" та "інформаційна безпека" у контексті властивостей інформації, як специфічної субстанції.

Об'єктивно-суб'єктивна природа інформації крізь призму інформаційної безпеки. Проблема забезпечення інформаційної безпеки як складової національної безпеки є багатоаспектною. Це об'єктивно зумовлює неоднозначні трактування її змісту.

Існують десятки її визначень, в які вкладається досить різний зміст. Так, Архипов О. та Архипова Є. під інформаційною безпекою пропонують розуміти "поточний стан захищеності об'єкта від інформаційних загроз, який визначається рівнем шкоди, що може бути заподіяна існуванню, функціонуванню чи діяльності об'єкта у разі реалізації цих загроз" У визначенні використовується словосполучення "стан захищеності", як функція рівня шкоди, який є результатом небезпек інформаційній безпеці, а питання запобігання вказаній шкоді не передбачається.

Вони також вважають що "основними властивостями інформації як об'єкта захисту є *доступність, цілісність та конфіденційність*". Проте з позицій системного підходу навряд чи ці ознаки інформації є тими, які свідчать про її відмінність від інших предметів та явищ реального світу, тобто властивостями інформації. Скоріш всього, вони є просто ознаками-характеристиками, які визначають її подібність до інших об'єктів.

А. Турчак розглядає "інформаційну безпеку" в якості стану, за якого життєво важливі особистісні, суспільні і державні інтереси є захищеними, мінімізуються збитки, спричинені неповнотою, невчасністю і недостовірністю інформації, негативним інформаційним впливом, негативними наслідками функціонування технологій в інформаційній сфері, а також несанкціонованим поширенням даних.

На думку В. Шаньгіна інформаційна безпека це "захищеність інформації від незаконного ознайомлення, перетворення і знищення, а також захищеність інформаційних ресурсів від впливів, спрямованих на порушення їх

працездатності". Тобто соціальна складова інформаційної безпеки ігнорується.

Згідно чинного законодавства "інформаційна безпека – стан захищеності життєво-важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через:

неповноту, невчасність та невірогідність інформації, щовикористовується; негативний інформаційний вплив;

негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації".

У цьому визначенні використовується словосполучення "стан захищеності". Він є величиною, що залежить від інтенсивності впливу факторів, які є причинами небезпек та ефективності реагування на них. Це означає, що йдеться про деякий рівень, нижче якого виникають проблеми щодо інформаційної безпеки. У визначенні його пропонується операціоналізувати через "життєво-важливі інтереси людини, суспільства і держави" та фактори, які породжують небезпеки вказаній безпеці. Ці інтереси та переліки мають суб'єктивно-об'єктивну природу.

Крім того, інтереси людини, суспільства і держави не співпадають, що породжує, так звану проблему соціального порядку, відому, як "Гоббсова проблема". Це одна із причин того, що у нормативно-правовому полі, проблема визначення рівня інформаційної безпеки до цього часу залишається невирішеною.

В цілому ж, можна дійти висновку, що однією із причин різного трактування змісту поняття "інформаційна безпека", є неоднозначність уявлень про властивості інформації, як специфічної субстанції.

Водночас, циркуляція інформації в соціальних системах є базовою передумовою умов їх життєдіяльності, оскільки вона завжди була важливим джерелом влади, а відтак і публічного управління.

Таким чином, в соціальних системах інформація, як і інформаційна безпека мають об'єктивно-суб'єктивну природу

та є атрибутом буття об'єктів живої природи і соціальних взаємодій.

Концептуалізація змісту концепту «інформація» має здійснюватися у контексті властивостей інформації, як специфічної субстанції, серед яких принципово важливими є її фізичні властивості, дискретність, ціннісний аспект, розсіювання, можливість стискування та старіння внаслідок надходженням нової інформація.

Тобто інформаційна складова є визначальною у відображенні взаємодії соціальних систем, тому системний аналіз цієї складової має бути основою при вирішені проблем забезпечення безпеки життєдіяльності людини (індивіда), соціальних груп та соціальних інститутів.

1.2. Інформація як атрибут буття об'єктів соціальних взаємодій та підходи щодо розкриття її змісту

Інформація як атрибут буття об'єктів соціальних взаємодій. Інформаційна складова взаємодії людини (індивіда), соціальних груп та соціальних інститутів відображає їх ціннісні орієнтації, пріоритети та мотиви соціальної поведінки. Тому окремої уваги заслуговує думка Н. Вінера щодо соціального характеру обмежень, які покладаються на засоби комунікацій, зокрема, що: засоби знаходяться в руках обмеженого класу багатих людей і тому висловлюють передусім його думки, а також, що вони є однією з основних доріг до влади.

Зважаючи на це елементи інформаційно-комунікаційні системи, яка повинна сприяти системі скоординованих дій, спрямованих на забезпечення, підтримання або відновлення сталості суспільства потраплять до рук тих, хто більш всього зацікавлений в грі за владу і гроші, тобто стає одним з основних чинників його диференціації. Тому, як стверджує Н.Вінер, не дивно, що великі співтовариств мають значно менше суспільно доступної інформації, ніж малі співтовариства, не говорячи вже про окремих людей.

З іншого боку, стрімкість розвитку інформаційно-комунікаційних технологій все більше віддаляє нас від розуміння сутності самої інформації, форм і способів її прояву.

Як зазначав А. Гор нові інформаційні технології змінили і нас самих, і наші умови життя і чим далі, тим більше тяжіли ми до винайдення нових способів одержання опосередкованої інформації, що вимагають усе більш і більш ускладнених пояснень" .

З іншого боку, різні науки вкладають в поняття "інформація" різний зміст. Досить широким є й діапазон її тлумачення.

Як відомо, інформація циркулює у трьох середовищах: біологічному, технічному і соціальному. Тому стосовно поняття "інформація" загального визначення скоріш за все не може бути. Так, один із творців теорії інформації К. Шеннон стверджував, що за певних обставин різноманітність значень слова "інформація" може виявитися корисною, але не можна очікувати, що єдине її визначення може задовольнити його застосування у різних областях.

Водночас з усього різноманіття уявлень про інформацію виокремлюють два підходи щодо розкриття її сутності: *органічний та атрибутивний*.

Згідно органічного підходу вона розглядається як властивість живої матерії відображати об'єктивну реальність і використовувати це в інтересах свого буття (існування). При цьому людина, на відміну від інших об'єктів живої природи, здатна свідомо впливати на середовище свого існування, що ґрунтується на сприйнятті, накопиченні, використанні інформації та передачі її у формі повідомлень.

Атрибутивний підхід розглядає інформацію, як невід'ємний атрибут матерії, тобто припускає можливість обміну інформацією і між об'єктами неживої природи.

В кінцевому підсумку, проблема відсутності однозначного трактування слова "інформація" трансформується у відсутність єдиної думки щодо сутності соціального явища, яке позначають поняттям "інформаційна безпека" та у її, так би мовити, двоїстого характеру, а саме два аспекти вивчення інформаційної безпеки: як одну зі складових національної безпеки, або як невід'ємний атрибут цих складових.

У загальному розумінні інформація – це певні відомості, сукупність певних даних, знань. При цьому прийнято виокремлювати два аспекти існування інформації як субстанції:

внутрішню, яка є мірою впорядкованості системи (процесу);

зовнішню, яка пов'язана з відображення у матеріальному та нематеріальному світі.

Так, якщо предмет зазнає певних змін під впливом іншого предмету, то він стає носієм інформації про цей предмет.

Очевидно, що для об'єктів неживої природи відображення має пасивний характер, а для живої природи – активний, оскільки пов'язаний з аналізом та переробленням інформації.

Таким чином, усі відносини між будь якими об'єктами та їх елементами ґрунтуються на процесі обміну інформацією, яка є ресурсом їх розвитку. Тому Н. Вінера вважав, що інформація є особливою субстанцією, яка відрізняється від матерії та енергії, бо має певні особливості та властивості, які зумовлюють специфіку інформаційних процесів .

Очевидно, що інформація для об'єктів живої природи є об'єктивно-суб'єктивна категорія, оскільки значущість того чи іншого повідомлення, факту тощо залежить не тільки від джерела, а й від того, хто його приймає (оцінює). Тому для когось інформація може мати значення, а для іншого – ні. З огляду на це ті чи інші інформаційні впливи на соціальну систему можуть кардинально змінити структуру її інтересів та мотиви поведінки.

Викладене вище дозволяє стверджувати, що, якщо розглядати інформацію у контексті соціальних взаємодій, то повідомлення набуває статусу інформації тоді, коли зачіпає інтереси людини (індивіда), соціальної групи чи соціальних інститутів.

Таке уявлення про інформацію, яка циркулює у соціальних системах, не заперечує атрибутивну концепцію (парадигму) інформації згідно якої вона є об'єктивною внутрішньою властивістю таких систем, яка відображає різноманітність їх структур та упорядкованості. Таким чином вказана інформація створює уявлення про природу, структуру, впорядкованість, принципову відмінність тієї чи іншої

соціальної системи. Тому інформація про систему не може виникнути поза нею.

Тобто інформація про соціальну систему виникає з моменту її появи та існує вічно, оскільки вона еволюціонує (змінюється) разом із системою. При цьому її можна накопичувати, зберігати та переробляти.

Вказане уявлення про інформацію, яке стосується соціальних систем, не заперечує й функціонально-кібернетичну концепцію інформації, оскільки йдеться про інформацію в системі з активними елементами.

З іншого боку, варто мати на увазі, що знання та інформація – різні категорії.

Інформація має об'єктивну природу, тобто відображає реальні енергетичні процеси якісно-кількісних змін у просторі і часі, які відбуваються в об'єктах неживої і живої природи, а також у створених людиною машинах. По суті, вона є своєрідною сировиною для одержання знання, яке є продуктом свідомості.

Тобто знання є явище ідеальне, яке циркулює у сфері суспільного життя, а відтак воно якісно відмінне від інформації. Тому інформація одночасно розглядається як феномен, функція, об'єктивні дані, суб'єктивне сприйняття тощо. Це породжує суперечності та неоднозначності серед науковців при трактуванні ними її сутності та інших пов'язаних з нею понять.

Підходи щодо розкриття змісту інформації у контексті її властивостей та джерел. Важливим чинником уникнення неоднозначності при трактуванні сутності будь-якого предмета чи явища природи є визначення його властивостей.

Властивості розкривають особливість об'єкта та спосіб його буття, що притаманні йому як цілісності, дозволяють ідентифікувати, відрізняти або встановити схожість з іншими об'єктами. Очевидно, що принципово важливими є фізичні властивості інформації, серед яких передусім:

здатність ідентифікації властивостей предметів і явищ, тобто того, що визначає їх властивості в навколишньому світі;

відсутність заряду і маси, тобто вона не є матерією;

здатність впливати на формування матеріальної сутності предметів і явищ природи;

невичерпність (може використовуватися необмежене число разів залишаючись незмінною);

незалежність її змісту, який може бути будь-яким і про все від форми його фіксації і способу пред'явлення.

Принципово важливим є й те, що в живій природі інформація пов'язана з енергією, оскільки створюється різницею енергетичних потенціалів, закріплених пам'яттю, а відтак має місце розсіювання інформації в процесі її передачі та зберігання.

Для соціальних систем важливою є її суспільна природа, оскільки джерелом інформації є пізнавальна діяльність людей, суспільства та мовна природа. Інформація зажди виражається за допомогою мови, яка служить засобом спілкування, мислення, висловлювання думки. Тому в соціальних системах властивостями інформації є її *дискретність* (її одиницями є слова, уривки тексту, знаки, символи тощо) та розсіювання. Останнє є наслідком її існування у різних джерелах та старіння, оскільки з надходженням нової інформація попередня перестає адекватно передавати явища та закономірності матеріального світу.

У багатьох випадках інформацію можна стискувати, тобто застосовувати процедури перекодування даних, яка проводиться з метою зменшення їхнього обсягу, розміру, об'єму і транспортування.

Як зазначалось, принципово важливим є ціннісний аспект інформації для об'єктів живої природи.

Цінність інформації має об'єктивно-суб'єктивну природу та визначається її: корисністю; актуальністю; оперативністю; адекватністю; об'єктивністю; повнотою. Вона не є її природною властивістю, тобто тією, що визначає її сутність. Вказана цінність виникає в результаті взаємодії об'єкта інформації та суб'єкта (користувача), якщо вона потрібна для досягнення тих чи інших цілей.

Таким чином, в соціальних системах джерелом інформації є пізнавальна діяльність людей, соціальних утворень та мова, яка служить засобом спілкування, мислення, висловлювання думки. Саме тому інформаційна безпека, як явище не існує поза межами соціальних взаємодій в процесі яких між їх учасниками

здійснюється обмін інформацією, а відтак і вплив один на одного.

Цей вплив може бути як позитивний, так і негативний, оскільки основою цієї взаємодії може бути як спільність, так і розбіжність інтересів, цілей, тощо її учасників.

Достовірність інформації як її визначальна властивість. Для людини найбільш цінною є *вірогідна інформація*, тобто та яка відображає дані (знання), істинність яких незаперечна. З огляду на те, що в науковому дискурсі та правовому полі широкого розповсюдження набуло поняття "*достовірна інформація*", варто зазначити, що воно не є тотожним поняттю "вірогідна інформація", оскільки достовірність — не те ж саме, що істинність.

Ті чи інші дані можуть бути достовірними або недостовірними для того, хто їх сприймає, а не взагалі, тому достовірність завжди має суб'єктивну природу, а істина — об'єктивну.

Незважаючи на це, очевидно, що для людини цінністю може бути лише достовірна інформація, тобто та в основі якої істинні дані.

Достовірність є поняття, яким позначають відповідність нашого знання дійсності, тобто сприйняття істини чи переконань в істинності певного знання. Якщо відповідність знання дійсності є проблематичною чи предметом суб'єктивного переконання, то достовірність завжди є варіантною, оскільки залежить від ситуацій прийняття того, що вважається суб'єктом незаперечним чи інтуїтивно очевидним.

Що ж до істинності тих чи інших даних, то, як відомо, істина характеризує результат пізнавального процесу – знання, як адекватне відображенню суб'єктивної та об'єктивної реальності в свідомості людини.

Оскільки будь-якому об'єкту притаманна пізнавальна невичерпність, то вона є безперервним процесом послідовного наближення до повноти відтворення об'єктивної реальності. Тому в ідеальному випадку, достовірною інформацією будуть дані, які не мають помилок, які можуть бути спричинені неповнотою даних через недостатнє вивчення того чи іншого предмету чи явища реального світу або прихованими чи

випадковими через навмисні або ненавмисні спотворення змісту даних людиною та збоїв технічних систем при їх опрацюванні та передачі.

Вказана вище обставина породжує проблему щодо оцінки ідентичності інформації, яку використовує людина, тобто її тотожності наявним знанням.

З огляду на викладене, можна дійти висновку, що достовірність інформації не є її визначальною властивістю, як про це стверджують деякі дослідники, а однією з суб'єктивно-об'єктивних її характеристик та однією із вимог, що висуваються до неї з боку суб'єктів інформаційних відносин.

Таким чином, інформаційна безпека як явище не існує поза межами соціальних взаємодій в процесі яких між їх учасниками здійснюється обмін інформацією, а відтак і вплив один на одного.

Цей вплив може бути як позитивний, так і негативний, оскільки основою цієї взаємодії може бути як спільність, так і розбіжність інтересів, поглядів тощо її учасників.

Негативний вплив можна ідентифікувати як прояв небезпеки інформаційній безпеці людині (індивіду) соціальній спільноті чи інститутам держави, як суб'єктам інформаційних відносин.

Таким чином, достовірність інформації не є її визначальною властивістю, а однією з суб'єктивно-об'єктивних її характеристик та вимог, що висуваються до неї з боку суб'єктів інформаційних відносин.

Ця інформація завжди є варіантною, а відтак не є тотожною вірогідності інформація, яка має об'єктивну природу. Це породжує проблему при оцінці ідентичності інформації наявним знанням, зокрема, при ідентифікації небезпек інформаційній складовій національної безпеки.

Врешті-решт, інформаційний простір є атрибутом буття об'єктів реального світу. Функціональним призначенням цього простору є породження, сприйняття, накопичення, запам'ятовування, переробка та обмін інформацією між вказаними об'єктами, а зміст цього простору є безмежним через невичерпність матерії. Це означає, що кількість інформації в інформаційному просторі є нескінченною.

Водночас ступінь захищеності інформації від негативного впливу факторів, які заперечують природню визначеність буття інформаційної компоненти об'єктів реального світу, зумовлює відповідний рівень інформаційної безпеки, який має об'єктивно-суб'єктивну природу.

ГЛАВА 2. ІНФОРМАЦІЙНА КОМПОНЕНТА ВЛАДИ ТА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

2.1. Інформація як джерело влади, чинник забезпечення державної безпеки та соціального порядку

Інформація як визначальне джерело влади. Інформаційна складова взаємодії суб'єктів соціальних систем відображає їх ціннісні орієнтації, пріоритетні інтереси, мотиви їх поведінки в тих чи інших умовах їх буття (існування). Тому наявність та ефективність засобів і способів, які дозволяють здійснювати цілеспрямований інформаційний вплив на соціальні об'єкти, тобто інформаційно-комунікаційних системи та технологій, визначає можливості суспільства щодо вирішення соціальних конфліктів у процесі його еволюційного розвитку. Ефективність використання цих засобів і способів у кінцевому підсумку буде визначати й рівень національної та державної безпеки, зокрема.

Водночас, соціальні проблеми завжди мають ту чи іншу інформаційну природу, оскільки циркуляція інформації в соціальних системах є базовою передумовою їх життєдіяльності та важливим джерелом влади. Відповідно, існують й досить ефективні інформаційні технології для системної активізація факторів, які є причинами дискримінації державної влади, її делегітимізації, обмеження державного суверенітету (підпорядкування зовнішньому впливу), порушення територіальної цілісності, руйнації конституційного ладу тощо.

Можливість їх використання актуалізує важливість адекватної протидії загрозам державній безпеці, зокрема, розробки та реалізації заходів з підвищення стійкості держави до деструктивного інформаційного впливу у контексті загострення суспільно-політичних протиріч. Це зумовлює

системний аналіз тенденцій трансформації інформаційної компоненти критичних (надзвичайних) ситуацій у контексті забезпечення державної безпеки.

Традиційно основними джерелами влади, а відтак і чинниками забезпечення державної безпеки розглядались багатство (економічні ресурси) та організоване насильство (у різних їх комбінаціях).

Роль інформації (знань), як джерела влади була відносно другорядною. Проте в індустріальну епоху її роль починає зростати, на що одним з перших звернув увагу англійський філософ Ф.Бекон.

В сучасному суспільстві, яке Е.Тоффлер – американський філософ та один із авторів концепції постіндустріального суспільства пропонував називати "суперіндустріальним", дослідження ролі та місця інформації у контексті засобів і способів, які дозволяють здійснювати цілеспрямований владний вплив на соціальні об'єкти, постійно перебуває в колі наукового дискурсу.

Аналіз наявних досліджень дозволяє дійти висновку, що сьогодні дієздатні та сильні держави мають значно більше шансів подолати можливі критичні (надзвичайні) ситуації, зумовлені політичними, економічними та іншими чинниками зберігши при цьому свій суверенітет, територіальну цілісність та національну ідентичність.

У даному випадку йдеться передусім про інформаційний компонент владного впливу на соціальні об'єкти при вирішенні соціальних конфліктів у процесі розвитку держав.

Водночас, наявні наукові дослідження, недостатньо розкривають сучасні тенденції трансформації інформаційної компоненти вказаних ситуацій у контексті забезпечення державної безпеки, оскільки вони акцентують увагу головним чином на захисті інформації (кібербезпеці) або інформаційних війнах.

Інформація як чинник забезпечення державної безпеки та соціального порядку. Згідно чинного законодавства під державною безпекою розуміється "захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво-важливих національних інтересів від реальних і потенційних загроз

невоєнного характеру". Ці загрози зумовлені зовнішніми та внутрішніми факторами.

Серед зовнішніх – наслідки глобалізації та інформаційної революції, які тісно пов'язані з міждержавним протиборством, зростанням транснаціональної злочинності, активізацією діяльності екстремістських організацій, інформаційними війнами та іншими чинниками.

Значним є й спектр внутрішніх факторів: корупція у державних структурах; домінування "тіньових" груп "впливу"; некомпетентність політиків при прийнятті рішень з питань забезпечення державної безпеки та інші.

Водночас існують ефективні методи активізації факторів, які є причинами загроз державній безпеці, які зазвичай передбачають використання інформаційних технологій, зокрема, так званих "кольорових" революцій та мають своїм кінцевим наслідком генерування критичних (надзвичайних) ситуацій.

Варто зазначити, що ті чи інші кризові ситуації є невід'ємним атрибутом соціальної системи та сприяють зміні якісно-кількісних характеристик її буття у руслі формування нової соціальної реальності.

Кризові ситуації розвиваються у часі та просторі. Це дозволяє виокремити їх певні стадії, у тому числі ті, на яких можуть виникнути критичні (надзвичайні) ситуації для державної безпеки. Характерною особливістю останніх на відміну від кризових ситуацій, є те, що наслідки *критичних* (надзвичайних) ситуацій завжди негативні, а кризові ситуації, через амбівалентність їх властивостей, можуть мати як негативні так і позитивні наслідки.

Крім того, в критичних (надзвичайних) ситуаціях стрімко зростає напруженість у відносинах між суб'єктами соціальних взаємодій, яка призводить до трансформації потенційних небезпек державній безпеці у реальні.

Визначальними рисами та причинами таких ситуацій сьогодні є зростання ролі масових комунікацій та нових технологій їх генерування. Тому принципово важливою є акумуляція та системний аналіз інформації, мобілізація інтелектуального потенціалу політиків й управлінців як базової

передумови напрацювання відповідних пропозицій і рекомендацій до управлінських рішень щодо забезпечення державної безпеки.

З іншого боку, в соціальних системах будь-яка інформація має об'єктивно-суб'єктивну природу. Її джерелом є пізнавальна діяльність людей та соціальних систем. Тому інформаційний компонент державної безпеки, як явища не існує поза межами соціальних взаємодій в процесі яких між їх учасниками здійснюється обмін інформацією. Цей вплив один на одного, може бути як позитивний, так і негативний, оскільки основою цієї взаємодії може бути як спільність, так і розбіжність інтересів, цілей її учасників тощо.

З огляду на це достовірність інформації не є її визначальною властивістю, а однією з вимог, що висуваються до неї з боку суб'єктів інформаційних відносин. Тому вказана інформація завжди є варіантною, що породжує проблему при оцінці ідентичності інформації наявним знанням, зокрема, при ідентифікації небезпек державній безпеці та, відповідно, формуванні адекватних управлінських рішень щодо реагування на вказані небезпеки.

Актуальність вирішення цього завдання зумовлена тим, що в сучасних умовах інформація у процесі соціальних взаємодій стала визначальним фактором (джерелом) становлення тієї чи іншої системи владних відносин між її учасниками.

Як ми зазначали, традиційно основними джерелами влади, а відтак і чинниками забезпечення державної безпеки розглядались багатство та організоване насильство у їх взаємозв'язку.

Проте вже на початку XX ст. один із основоположників неомарксизму, італійський філософ А.Грамші вважав, що наявність економічних ресурсів не гарантує їх власникам державну владу, оскільки важливим чинником перебування при владі є згода на деякий соціальний порядок, справедливість (доцільність) якого не заперечується переважною частиною членів соціуму.

На важливості встановлення такого порядку та складності вирішення цієї проблеми акцентував увагу ще Аристотель, який

розглядав її у контексті підвищення стійкості державного ладу та як один з засобів досягнення загального благополуччя. Він зазначав, що багато законодавців, у тому числі ті, які мають на увазі встановлення аристократичного устрою, терплять невдачу не лише унаслідок того, що вони надають надто багато переваг заможним, але і тому, що прагнуть обійти простий народ, а відтак з часом із помилково зрозумілого блага, неминуче наступить справжнє зло, і державний лад губить швидше жадібність багатих, ніж простого народу.

Тому щодо того, яким чином найкраще влаштувати життя для більшої частини держави, тобто яким має бути найкращий державний лад, то на його думку найбільшим благополуччям для держави є те, щоб його громадяни мали власність середню, але достатню; а в тих випадках, коли в одних дуже багато, інші ж нічого не мають, виникає або крайня демократія, або олігархія в чистому вигляді, або тиранія, саме під впливом протилежних крайнощів.

Та найбільш системний аналіз концепту "соціальний порядок" виконав один із творців теорії суспільного договору, англійський філософ Т. Гоббс. Він розглядав його у контексті стійкості держави (через це вона в науковому дискурсі отримала назву "Гоббсова проблема"). Він стверджував, що різниця між здібностями людей не настільки велика, щоб одна людина могла претендувати на яке-небудь благо для себе, а інша не претендувати на нього з таким саме правом. Тому виникає рівність надій на досягнення цілей і якщо дві людини бажають однієї і тієї ж речі, якою, проте, вони не можуть володіти удвох, вони стають ворогами. На шляху до досягнення їх мети вони прагнуть згубити або підкорити один одного.

Т. Гоббс. доходить висновку, що там, де немає влади, здатної тримати всіх в підпорядкуванні, люди не мають жодного задоволення від життя у суспільстві. Поки люди живуть без загальної влади, що тримає всіх їх в страху, вони знаходяться у тому стані, який називається війною, а саме у стані війни "всіх проти всіх".

Таким чином, який би соціальний клас не перебував при владі володіння переважною часткою економічного багатства або контроль над ним не гарантує йому державну владу,

оскільки важливим чинником стабільного перебування при владі є стійкість соціального порядку. Його руйнація, тобто відсутність суспільної злагоди щодо існуючого порядку речей є основною небезпекою для державності.

Таким чином підтримка стійкості соціального порядку є головною функцією держави (органів державної влади), що обумовлює її право на використання силового компоненту влади (поліції, спецслужб, збройних сил тощо), оскільки там, де немає влади, здатної тримати всіх в підпорядкуванні, наступає стан війни всіх проти всіх.

2.2. Інформація як чинник модернізації державного управління та цілі сучасних інформаційних війн

Погляди Е. Тоффлера на інформацію як чинник модернізації моделей державного управління. Е. Тоффлер одним із перших довів, що якщо спочатку основою влади було насильство, а потім гроші та фінансова могутність, то сьогодні нею є знання та інформація. Це означає, що сталася фундаментальна зміна в співвідношенні насильства, багатства і знання у контексті заволодіння та утримання державної влади.

Володіння знаннями (інформацією) сьогодні перекривають переваги інших джерел влади.

Вони можуть не тільки служити для примноження багатства і сили, а й служать еліті для управління і контролю. Тому існуючі технології управління радикально змінюються, народжуються нові організаційні структури, а сучасне управління (передусім у сфері безпеки) потребує нових стилів лідерства та інтуїції, які не притаманні бюрократу.

Е. Тоффлер окремо акцентує увагу на зростаючому впливі засобів масової інформації та комунікацій, які продукують потік суперечливих образів, символів і “фактів”. Тому чим більше даних, інформації та знань використовується системою управління, чим більшою мірою ми стаємо “інформаційним суспільством”, стверджував він. І водночас тим складніше може стати для будь-кого, включаючи політичних лідерів, отримання уявлення про те, що відбувається насправді.

Як зазначає Е. Тоффлер, основною причиною цього є те, що у політичних кризах, всі сторони стануть використовувати різні прийоми, засновані на маніпуляціях з інформацією, головним чином до того, як вона поступає в засоби масової інформації". Внаслідок цього:

з одного боку, якомога більша обізнаність стає насущною необхідністю для будь-якої влади;

з іншого боку – лише небагато заяв, повідомлень або "фактів" в політичному житті можуть вважати істиною, бо на них лежить відбиток протиборства у владних структурах, а повідомлення, поширювані засобами масової інформації, ще більше змінюють "факти".

З огляду на це Е. Тоффлер констатує, що пронирливі і хитрі політики і бюрократи відмінно знають, що дані, інформація і знання – це зброя противника, заряджена і готова вистрілити в боротьбі, що відбувається, за владу, яка складає основу політичного життя.

У контексті сказаного доцільно згадати позицію одного із основоположників кібернетики, американського математика Н. Вінера, стосовно ролі систем комунікацій в сучасному суспільстві. На його думку, вони знаходяться в руках обмеженого класу багатих людей і тому висловлюють передусім його думки. Тому система комунікацій, яка повинна сприяти підтриманню або відновленню сталості суспільства потрапляє до рук тих, хто більш всього зацікавлений в грі за владу і гроші, тобто стає одним з основних чинників диференціації суспільства.

Передумови та цілі сучасних інформаційних війн. Німецький філософ Е. Фромм не без підстав стверджував, що політичні технології, озброєні засобами інформатики, можуть упевнено формувати громадську думку, маніпулювати суспільною свідомістю, а інформація може стати засобом інформаційного тиску і панування, а відтак ми живемо на порозі інформаційного імперіалізму.

І дійсно, як зазначає В. Пугач, транснаціональні актори вимагають прилаштування управлінської діяльності держави до потреб транснаціонального капіталу, культивуючи, тим самим, транснаціонально-орієнтований управлінський клас –

своєрідний адміністративний ресурс, чи навіть “обслуговуючий персонал”, “акторів поза суверенітетом.

На цьому тлі існує не тільки загроза маргіналізації національно-орієнтованої адміністрації, яка має бути націлена на захист інтересів держави.

Реальністю стали інформаційні війни з використанням новітніх інформаційних технологій, які відбуваються на національному, регіональному та глобальному рівнях. Їх основними цілями є заволодіння та утримання влади в усіх сферах життєдіяльності держави: політичній, економічній, військовій та інших.

Так, В. Кіхтан та З. Качмазова стверджують, що вказані війни задіюють на всьому просторі держави-мішені протягом тривалого часу з урахуванням всіх доступних механізмів, включаючи пропаганду, психологічні атаки всередині держави, а також дипломатичні кола – у всьому світі.

При цьому, як зазначає Самохвалова В., обман виступає загальною методологією інформаційної війни, а брехні буде все більше, і вона буде все більш уточненою, що вимагає більш розвинутої здатності мислення, наявності певної загальної моделі розуміння світу і раціональної поведінки, заснованої на здатності адекватної самоідентифікації.

Водночас сучасні інформаційні впливи часто спрямовані головним чином саме на руйнування, деформацію, фальсифікацію даних, людських здібностей і характеристик.

На думку науковців феномен інформаційних війн набуває домінуючої форми активації і перебігу політичних, військових, економічних та інших конфліктів на національному та глобальному рівнях.

Спектр методів їх ведення дуже широкий: від медіавоєн за участю впливових корпорацій массмедіа до прямолінійних кібератак і впроваджень вірусів в комп’ютерні мережі реального або передбачуваного противника. Іншими словами, глобальні інформаційні технології часто виступають в ролі зброї нового типу.

2.3. Роль інформації у сфері національної безпеки та інформаційна складова масової культури

Сучасна роль інформації в управлінні у сфері національної безпеки. Сучасні битви за владу (глобальну, регіональну, національну), основою якої є боротьба за знання (інформацію), зумовлюють перехід до нового типу урядування.

Це досить драматичний процес, який породжує критичні ситуації у відповідних системах управління. Проте, у будь-якому випадку, наявні системи управління вимушені перебудовуватися, бо сучасна її організаційно-функціональна структура має базуватися на інтелекті. Саме сьогодні, як ніколи, підтверджується позиція (теза) Ф. Бекона, що знання та могутність людини співпадають, а саме його загальновідомий афоризм: "знання – сила". І в цьому контексті важливим є дослідження сутності влади, яка ґрунтується на компетентності та сприяє зростанню людини, яка на неї спирається. Їх виконав згаданий вище Е. Фромм.

Е. Фромм стверджував, що з утворенням ієрархічно організованих суспільств, компетентність не обов'язково є невід'ємним елементом влади.

Це стосується й сучасних демократичних суспільств, де влада людей може бути наслідком суми грошей, яку вони в змозі вкласти в передвиборну кампанію, а відтак між компетентністю і владою може не бути майже ніякого зв'язку.

Крім того, зазначає він мільйонам людей сьогодні дуже важко оцінити поведінку особи, яка обіймає владу, коли все, що їм відомо про неї, - це, скоріш всього її штучний образ, створений пропагандою. Повіривши у вигадку, люди втрачають здатність покладатися на власну думку та перестають бачити дійсність в її істинному світлі.

Та які б не були причини втрати якостей, що становлять компетентність державних службовців, якщо її розглядати у контексті забезпечення державної безпеки, в умовах глобалізації виробничих та фінансових систем відбувається процес відчуження влади та проявляється тенденція формування "транснаціонального блоку" капіталістів, державних управлінців та інтелектуалів.

Їх головною метою є побудова нового транснаціонального ладу та отримання надприбутків, і аж ніяк не захист національних інтересів. Як наслідок, предметом наукового дискурсу все частіше стає нездатність національної держави вирішувати завдання навіть у безпекових сферах діяльності. Водночас це супроводжується генерацією різноманітних постмодерністських проектів типу: "мережевого суспільства", "космополітичної держави", "глобального громадянства" "цифрового врядування» та інших.

Так, оцінюючи спроможність держави адекватно реагувати на сучасні реалії, німецький соціолог та філософ У.Бек констатує, що європейці тільки, роблять вигляд, що існують Німеччина, Франція, Італія, тощо. Але їх давно вже нема, так як немає усього того, на чому донедавна тримався національно-державний світ. Тому національна держава, як соціальний інститут давно перестала створювати загальний порядок взаємовідносин, що мав би містити у собі всі інші принципи поведінки, та нездатна давати відповіді на політичні виклики сучасності. У тому числі безпекового характеру.

Близькою до нього є й думка британського соціолога З.Баумана, який стверджував є, що немає надії на державні установи, призначенням яких є забезпечення безпеки, оскільки "свобода державної політики невпинно руйнується новими глобальними силами". Він також вважав, що причинами цього є процеси *дерегулювання* соціально-економічних і політичних відносин, посилення ролі неконтрольованих чинників і тенденцій, наростання невизначеності, придушення проявів людського духу, які спонукали людей до суспільно-політичних перетворень.

З ним повністю погоджувався французький соціолог та філософ Ж. Бодрійяр, на думку якого в сучасну епоху ідентифікація відбувається не через ідеологічну та політичну мобілізацію, а через доступ до задоволень, який контролюється, бо споживач отримує від фрагментованого культурного середовища специфічну ідентичність, яка є продуктом, що зійшов з конвеєра масової культури.

Інформаційна складова масової культури як загрози національній безпеці. Зростаюча множинність релігійної,

етнічної тощо самоідентифікації знижує ступінь політичної мобілізованості громадян, перетворюючи їх в індивідуалізовану масу. Тому сучасна масова культура є ефективним механізмом *символічної* інтеграції, який формує ідентичність *глобального споживача*.

Водночас в політиці зростає маніпулювання. Воно дезорієнтує масову свідомість, внаслідок цього прискорюється формування суспільств з розмитою національною ідентичністю. Через це відбувається ерозія культурного коду, що є реальною загрозою соціальним порядкам, розвитку національних держав і. відповідно, їх безпеці. Тому, на думку З. Баумана, глобалізація більш успішніша в розпалюванні міжобщинної ворожнечі, ніж у сприянні мирному співіснуванню громад.

Звичайно, мати одночасно бажаний рівень безпеки держави та добробуту кожної людини досить складно важко. Матеріальні потреби є величезною силою, яка тримає людину у контакті з повсякденною реальністю. Тому, як правило, індивіди, надають пріоритет своїм прагматичним цілям.

Водночас в умовах активної генерації симулякрів, неефективність традиційних способів інтеграції та координації дій індивідів, сформувала проблемне поле конституювання соціальності сучасного типу, яке б відповідало реаліям постіндустріального (інформаційного) суспільства. В межах цього поля необхідно здійснювати пошук оптимального балансу влади в трикутнику: індивід - суспільство-держава. Це дасть змогу мінімізувати небезпеки дезінтеграції суспільства, держав та їх стійкості.

Врешті-решт, глобалізаційні процеси та інформаційні технології кардинально змінюють суспільне життя, ускладнюють систему владних відносин, генерують низку загроз для державної безпеки, здійснюють потужний вплив на людську природу та свідомість. Вказані чинники потребують адекватних управлінських рішень щодо забезпечення державної безпеки в основі яких, як правило, завжди нові знання. Тому в сучасну епоху дієздатність органів державної влади передусім залежить від того, наскільки вони:

використовують при підготовці своїх рішень рекомендації науковців, експертів, аналітиків;

забезпечують інформаційне насищення управлінських рішень достовірною інформацією з питань забезпечення державної безпеки.

Визначальною передумовою вирішення і першого і другого завдання є передусім підготовка фахівців-управлінців, спроможних ефективно вирішувати проблемні питання щодо забезпечення національної безпеки.

Таким чином, сьогодні інформація (знання) є визначальним джерелом влади, а інформаційний простір атрибутом буття держав, через що принципово важливим є належна його захищеність.

Загрози національній безпеці зумовлені різними факторами, а для їх системної активізації існують різні методи, які передусім передбачають використання ІКТ та мають своїм кінцевим наслідком генерування критичних (надзвичайних) ситуацій, у сфері національної безпеки.

Їх особливістю є стрімке зростання напруженості між суб'єктами соціальних взаємодій, що, як правило, призводить до трансформації потенційних небезпек національній безпеці у реальні.

При цьому інформаційний компонент державної безпеки не існує поза межами соціальних взаємодій в процесі яких між їх учасниками здійснюється обмін інформацією, а їх вплив один на одного, може бути як позитивний, так і негативний, оскільки основою взаємодії може бути як спільність, так і розбіжність інтересів та цілей учасників соціальних взаємодій.

Водночас, принципово важливою обставиною є та, що який би соціальний клас не перебував при владі, важливим чинником його стабільного перебування при владі є стійкість соціального порядку, руйнація якого є основною небезпекою для держави, тому його підтримка є її головною функцією та обумовлює її право на використання силового компоненту влади, оскільки там, де немає влади, здатної тримати всіх в підпорядкуванні, наступає стан війни всіх проти всіх.

При цьому стрімко зростає вплив на державну владу ІКТ, які часто продукують потік суперечливих фактів, тому чим більше інформації використовується системою управління, тим складніше отримати уявлення про те, що відбувається

насправді, особливо в умовах інформаційних війн, руйнації національної культури (через домінування домінування масової культури) та зростання маніпулювання у політиці, яке дезорієнтує масову свідомість. Вказані чинники активізують процес формування суспільств з розмитою національною ідентичністю, що є реальною загрозою національній безпеці.

ГЛАВА 3. ІНФОРМАЦІЙНИЙ АСПЕКТ УПРАВЛІНСЬКОЇ ДІЯЛЬНОСТІ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

3.1. Роль інформації в управлінні у сфері національної безпеки та еволюція різних аспектів її сутності

Проблема осмислення сучасної ролі інформації в державному управлінні у сфері національної безпеки. Трансформації цифрової сфери та інформаційного простору, генерування штучного інтелекту є яскравими прикладами сучасних викликів у сфері державного управління.

Насамперед ці, а також інші сучасні тенденції актуалізують потребу впровадження новітніх інструментів, методів і технологій для всебічного розкриття, осмислення феномену інформація.

У глобальному вимірі, владою США й керівними органами Європейського Союзу впорядковано обмін даними та їх захист підписанням офіційної рамки, на основі якої Єврокомісією прийнято відповідний акт [Commission Implementing Decision, 2023].

Правляча верхівка Китаю, беручи до уваги ризики в інформаційній сфері вдалася до обмежувальних заходів доступу нерезидентів до інформації, що циркулює на внутрішньому ринку [Multinationals in China accelerate push to decouple data, 2023].

Результатом реагування інституціями спільного європейського простору стало вдосконалення Європейською Комісією інформаційної політики в протидії дезінформації [The Strengthened Code of Practice on Disinformation, 2022], а окремих провідних країн-членів ЄС, до прикладу Німеччини –

кардинальної модернізації стратегії національної безпеки [Robust. Resilient. Sustainable. Integrated Security for Germany, 2023].

Для України, повномасштабне вторгнення рф й ескалація гібридної війни виступають потужними каталізаторами формування національної стійкості за керівної ролі держави у регулюванні інформаційного середовища, нейтралізації впливу прокремлівських акторів на державно-управлінську діяльність, боротьбі проти дезінформації, забезпеченні ефективності системи національної безпеки.

Таким чином, на тлі сучасних викликів та загроз національній безпеці подальше осмислення ролі інформації в державному управлінні у сфері національної безпеки має важливе теоретичне та практичне значення.

Аналіз досліджень свідчить, інформаційна термінологія («інформація», «дезінформація», «наративи», «пропаганда», «інформаційний розлад», «фейк», фальсифікація, «неправдива/оманлива інформація» тощо) стала невід'ємною частиною процесів державного управління. Тому важливими для розуміння сутності феномену інформація в державно-управлінській діяльності, застосування методології державного управління для його дослідження, є, зокрема, наукові публікації В. Гітта, Л. Климанської, В. Пожуєва, В. Бакуменка, О. Кравченка, Т. Новаченко, Л. Герасіної, І. Підкуркової, В. Погрібної, І. Поліщука, М. Требіна, Г. Почепцова, А. Демартина, О. Звоздецької.

Попри прийняття стратегічних програмних документів і ряду законів, питання методологічних підходів до всебічного розкриття феномену інформація, його проявів передусім у сфері національної безпеки, виокремлення значущих особливостей чи компонентів для ефективного їх практичного втілення в діяльність органів влади при розробці та функціонуванні ІКТ продовжує залишатися актуальним.

Еволюція історико-правових аспектів сутності феномену інформації. Еволюцію історико-правових і світоглядно-філософських аспектів розкриття сутності феномену інформації стисло можна представити, за Т. Куном – як перманентний

процес зміни парадигм (концептуальних підходів) його дослідження:

у «докібернетичну» добу для пояснення цього феномену, як правило, використовувалися терміни «уявлення», «поняття», «відомість», «передача повідомлення»;

«кібернетичний» період суттєво збагатив концептуальне осмислення цього феномену його статистичним визначенням як знакової структури без урахування змісту, тобто різниці між якісним станом системи до й після отримання та використання тієї чи іншої інформації;

за «інформаційного бачення кібернетики» інформація, це лише *нові* і *корисні* відомості, які використовуються при прийнятті та реалізації управлінських рішень для досягнення певних цілей;

на основі консенсусу представників філософської спільноти, даний феномен часто окреслюється (інтерпретується) через його властивості як «специфічної субстанції, чогось «умовного, не існуючого у нашому фізичному світі», «без специфічної форми подання»; «сутнісного прояву матерії», «первинності у порівнянні з вторинністю матерії», «суб'єктивності»;

постмодерністські погляди значно розширили коло наукового трактування цього феномену за рахунок інших наук передусім біології і соціології категорією «освоєння інформації»;

розвиток постіндустріального суспільства поряд зі збагаченням понятійно-категоріального апарату – «глобальне/мережеве суспільство»; «інформаційні ресурси»; «інформаційні системи» тощо – сформував синергійно-інформаційне уявлення про оточуючий світ, що інформація становить глибоку природну сутність, зокрема, що вона знаходиться поза матерією чи ідеї, а відтак трансформує енергетичну людину на інформаційну й є визначальним ресурсом її розвитку, а також суспільства та інститутів держави;

тривалі дискусії щодо співвідношення «відображення» та «інформація» між тими, хто ототожнював інформацію з відображенням, і будучи впевненим що відображення

характерно для усієї матерії, стверджував, інформація властива усій матерії у тому числі неживій – й тими, хто пов'язував феномен інформації, який виникає у процесі управління;

за широкого підходу феномен інформація прирівнюється до *третьої* універсальної і основоположної величини поряд з енергією та матерією [Hitt, 1990];

сучасні допарадигмальні тренди на Заході упродовж останнього десятиліття на тлі кризи світового порядку, нівелювання загальних людських цінностей, поглиблення розламу на осі «правда-дезінформація» з одночасним прискореним розвитком систем штучного інтелекту, світового медійного простору виправдовують формування нового бачення предмету дослідження, спонукають до осмислення феномену через роль й місце держави як ключового стейкхолдера забезпечення національної безпеки, у тому числі інформаційної складової безпеки громадянського суспільства, «компонента критичних (надзвичайних) ситуацій».

У вітчизняному правовому полі, Законом України «Про інформацію» окреслено − інформація, це: «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді».

З суб'єктно-об'єктних позицій, статус суб'єкта владних повноважень закріплено за органами державної влади всіх рівнів.

Пріоритетність держави, як гаранта рівних прав і можливостей полягає у забезпеченні доступу до інформації всім суб'єктам інформаційних відносин.

При цьому одним із компонентів регулюючої функції держави є захист інформації та поводження з різними категоріями відомостей, що віднесено до компетентності державних органів законами України «Про державну таємницю», «Про національну безпеку України».

Програмні документи також містять трактування поняття інформація. У «Стратегія кібербезпеки України» (2021 р.) інформація вживається в смисловому взаємозв'язку з «масивами», «ресурсами», «системами», «спеціальними операціями», «персональними даними», «інфраструктурою», «технологією», «захистом». Документ «Стратегія забезпечення

державної безпеки» (2022 р.) співвідносить його з поняттями «безпека», «вплив», «сфера», «операція», «технологія», «психологічні засоби», «обмін», «охорона», «захист».

За кордоном, наприклад, у США в документі «Стратегія національної кібербезпеки» (2023 р.) ототожнюється захист «інформації» із захистом «даних» чи захистом «знання» [National Cybersecurity Strategy, 2023].

За сучасних концептуальних підходів Європейської Комісії щодо вдосконалення інформаційної політики прикметним є визначення поняття *дезінформація* – «це, інформація, що очевидно неправда або така, яка вводить в оману:

створена, представлена і поширена з метою економічної вигоди або умисного введення в оману громадськості;

може заподіяти шкоду суспільству через загрозу демократичним політичним процесам й процесам вироблення політики, а також суспільним благам, як захист здоров'я громадян, довкілля та безпека».

Таким чином, за основу європейською інституцією при розробці інформаційної політики взято категорію «інформація», але очевидним є різнонаправленість трактування її змісту. Тому залишається необхідність узгодження термінології, розробки стратегії і механізмів протидії дезінформації, постановці чітких цілей, на що, зокрема, звертає увагу О. Звоздецька, досліджуючи проблеми й підходи Європейського Союзу.

Еволюція світоглядно-філософських та соціальних аспектів сутності феномену інформації. У науковому дискурсі державного управління визначено «інформацію світоглядну, методологічну» як концептуально-методологічну основу – складника інформаційно-психологічної зброї першого пріоритету у контексті засобів впливу за допомогою яких здійснюється нав'язування певного типу соціальної поведінки – «інформація хронологічного порядку проходження фактів та явищ, їхнього взаємозв'язку між собою».

Інший смисл терміну «інформація» у концептуалізації поняття «війна інформаційно-психологічна». Коли інструментом інформаційної протидії є дезінформація, за посередництвом якої на учасників планування у сфері

національної безпеки і оборони чиниться організований психологічний тиск супротивною державою або зовнішнім актором.

Вивчаючи соціальні функції інформації, В. Пожуєв виділяє такі особливості:

доступність – через доведення її до суб'єкта та циркулювання каналами, до яких він має доступ;

притягувати увагу – бути відміченою суб'єктом і виокремленою з усього потоку;

бути інтеріоризованою суб'єктом – однозначно витлумаченою за допомогою накопичувальної інформації про оточуючу дійсність, якою вже володіє суб'єкт.

Досліджуючи феномен «гібридна війна», М. Требін окреслює інформацію як один із основних видів зброї війни шостого покоління, що застосовується агресором на стадії інформаційної боротьби для свідомого руйнування духовного світу цілих націй чи народів сторони-жертви.

У контексті теорії симулякрів Ж. Бодріяра − компонентів віртуальної реальності у формі знаків й образів, що є фальсифікованими копіями конкретних явищ та об'єктів, завдяки медіа та мережевій комунікації, в публічному просторі утворюється симульована реальність відмінна від справжньої завдяки симулякрам третього покоління заснованим на інформації.

Можемо говорити про усталену тенденцію використання в гібридних війнах інформаційних повідомлень для формування віртуальних явищ.

До прикладу, в інформаційній боротьбі симулякри «денаціоналізація», «демілітаризація», «укронацисти», «бандерівці», що генеровані прокремлівськими акторами напередодні повномасштабного вторгнення в Україну, були направлені на підміну справжніх цілей верхівки рф й виправдання активної військової фази перетворенням її військових угруповань на «визволителів».

Метою такого моделювання повинно було стати розмивання феномену української державності, національної ідентичності задля створення соціального простору на основі антиукраїнської системи ментальності, ототожнення

мешканцями Сходу і Півдня України з ідеологією «руського міра».

Звертаючись до аспектів формування авторитету державного службовця, Т. Новаченко переконує, що завдяки розповсюдженню інформації створюється віртуальна реальність з іміджу та системи симулякрів, яка породжує асоціацію з потрібним образом. Звідси, до авторитетів з реального життя додаються їх віртуальні образи. Дослідниця впевнена, що авторитет будь-якого керівника або політика можливо редагувати через гру. Отже, ігроізація– це реалії сучасного суспільства, що торкнулися і державного управління.

Престиж, репутація й імідж керівника, як моделювання і підтримка віртуальної реальності створюють віртуальний авторитет, який позначається на суспільній думці». Основним інструментом виконання цих завдань є інформаційно-комунікаційні системи та технології.

Загальновідомо, що однією з рушійних сил політичної активності є резонансна інформація, на що, зокрема, звертає увагу І. Підкуркова. При цьому варто зазначити, що значуща інформація актуалізує психологічну потребу публічного актора діяти, формувати смисли на основі знання, ділитися домінуючим актором певними прерогативами з іншими стейкхолдерами або навпаки обмежувати їх.

Прикладом, який підтверджує сказане є, зокрема так звана політична «картельна угода» − підписаний у 2006 році «Універсал національної єдності». Його підписали очільники вітчизняних владних інститутів та представники окремих провладних політичних партій за свідомого самоусунення інших. Тому результат виявився нежиттєздатним, стагнаційним явищем у масштабі країни.

Більше того, він насправді, створив основу для подальшого розбалансування в суспільстві і державі, не зміг забезпечити належне функціонування системи державного управління, суттєво обмеживши повноваження владних інститутів.

Таким чином інформація завжди формує систему дії чи протидії, а її стабільність або стійкість залежить від зовнішніх й внутрішніх чинників, контекстів або змістів.

В цифрову епоху, як зазначає А. Демартино, спектр інформаційно-комунікативних технологій розширився за рахунок способів практичного використання знання, спрямованого на досягнення конкретної цілі шляхом взаємодії між політичними суб'єктами, якій властиві такі риси, як: практичність, цілеспрямованість, конкретність, чітка спеціалізація, партикулярність, наявність політичного суб'єкта та процесу взаємодії.

Таким чином, практичні державно-управлінські виміри прийняття рішень залежать від чисельних факторів саме інформаційного характеру, зокрема:

регламенту доступу й використання інформації;

підходів оцінювання даних і розв'язання проблеми;

політичних спрямувань ключових стейкхолдерів інформаційного простору чи сектора безпеки;

інтерпретації подій інформаційно-аналітичними, експертними, консалтинговими центрами та інших компонентів впливу на систему державного управління.

Не варто, звичайно, виключати й фактор трансформаційного характеру українського суспільства.

Таким чином, мають місце різнопланові підходи і парадигми до трактування національним законодавцем та в концептуальних документах феномену «інформація» залежно від прикладної сфери. Тому важливим є вироблення комплексного підходу для визначення та врахування особливостей ролі інформації в державному управлінні у сфері національної безпеки.

3.2. Роль інформації в суб'єкт-об'єктній взаємодії в управлінні та як його системоутворювальний фактор

Роль інформації в суб'єкт-об'єктній взаємодії в системі державного управління. Суб'єктно-об'єктна взаємодія є одним із наріжних каменів методології державного управління.

Сутність цієї методології у трьох аспектах – практика, наукові дослідження і освіта, а її роль полягає в забезпеченні пізнавальної, практичної або навчальної діяльності. Така її особливість зумовлена міждисциплінарним характером науки

державного управління і наявністю в останньої специфічних властивостей об'єкта та предмета.

Трактування поняття «об'єкт» пропонують В. Бакуменко і С. Кравченко, як: будь-яке явище, процес або предмет, на який спрямована практична або пізнавальна діяльність людей.

Очевидно, що в залежності від етапу розвитку державотворення або суспільної трансформації, під впливом тих чи інших чинників, до прикладу, «євроатлантичні устремління», «загроза втрати територіальної цілісності», «протидія дезінформації», «військова агресія рф проти України» тощо, це має відображення й на адаптуванні методології державного управління, зумовлює пошук ефективних рішень.

Як зазначалося, інформація − частина публічного інформаційного простору. Саме вона формує суспільне інформаційне середовище, яке знаходиться у постійному русі, є його базовим компонентом, отже, це феномен суспільний.

З боку практичної діяльності в державному управління, інформація являє собою об'єкт управлінського впливу для суб'єктів-органів влади в здійсненні різноманітних функцій.

Наприклад, формування та реалізація політики щодо забезпечення інформаційної безпеки, планування політики у сфері державної безпеки, забезпечення безпеки громадян та інші напрями державно-управлінської діяльності.

Водночас, слід враховувати, що інформація про окремі сфери національної безпеки ще не дає вичерпного уявлення про безпеку об'єкта загалом. Звідси – необхідність комплексної оцінки умов розвитку людини, суспільства, держави у контексті реалізації їхніх інтересів у різних сферах.

Під впливом різноманітних чинників, формується і методологічний зміст державного управління залученням та адаптацією методів інших сфер галузі науки, додаючи йому системного характеру.

Науковці підкреслюють, що саме системній методології, яка об'єднує пізнання, оцінювання та практику, належить зростаюча роль з набуттям властивості загального методологічного ядра державного управління. Тому системну методологію можна розглядати як об'єднуючу платформу дослідження різних аспектів державно-управлінської

діяльності, включаючи регулювання інформаційного середовища за допомогою ІКТ систем та технологій.

З точки зору властивості матерії, принцип системності проявляється через системність практичної і пізнавальної діяльності направленої на оточуючий людину світ.

В наукових колах прийняте визначення принципу системності, як здатність об'єкта бути системою завдяки наявності того чи іншого фактора, що цю систему утворює, а з-поміж його характеристик:

елементний склад;

структура зв'язків;

функції елементів і цілого;

єдність внутрішнього й зовнішнього середовища;

закони розвитку елементів і системи та інші.

Оскільки інформація як суспільний феномен, відтворюється у межах ієрархічної суспільної структури а, відповідно, структури системи держаного управління, у тому числі у сфері національної безпеки, то завдяки єдності і взаємодії елементів інформаційного середовища, вона також є системним явищем.

Свого часу, говорячи про управління інформаційним простором, видатний український вчений Г. Почепцов виокремив систему аксіом, яка складається з основних категорій:

об'єм (існування нескінченних можливостей розширення і наповнення новим змістом);

доступ (інформаційний простір вільний, а його обмеження потребують додаткових засобів);

управління (увага може приділятися лише конкретному елементу);

неоднорідність (елементи відрізняються один від одного);

взаємозалежність (елементи перебувають у різних зв'язках між собою).

Це додає широкого смислу природі інформація, оскільки системний підхід полягає в дослідженні інтеракції між різними елементами системи.

Можливості ж системного підходу в розкритті сутності предмета чи об'єкта є наслідком сукупності його методів та

напрямів наукового пізнання, принципів системного аналізу: елементаризму, загального зв'язку, розвитку, цілісності, системності, оптимальності, ієрархії, формалізації, нормативності, цілепокладання та інші.

Інформація як системоутворювальний фактор управлінської діяльності у сфері національної безпеки. Принципово важливим при дослідження будь-якої системи, явища, процесу тощо є виявлення його системоутворювального фактора. Це сприяє не лише ефекту пізнавального, практичного або освітнього, а й слугує засобом отримання повноцінного результату (знання).

До прикладу, у функціональних теоріях систем системоутворювальним фактором поведінських актів визначається мотивація, відповідно до пріоритетних потреб організму.

У соціальній системі, це – ціль, як об'єднуюча основа задля її формування, утримання рівноваги, забезпечення розвитку, збереження спадковості і пам'яті про код, а також реалізації інших завдань.

Значною мірою, на наш погляд, під цим кодом розуміється інформація, яка дозволяє ідентифікувати унікальні культурні особливості, а під державністю – певна організація матеріального і духовного буття народу як соціальної системи, яка складається із території, макросоціальної спільноти (нації), яка на ній проживає і вирізняється культурним кодом та створені нею державні інститути.

Співвідносячи сутність й властивість інформації з її проявами в управлінні у сфері національної безпеки, можемо стверджувати, що об'єднуючою основою, одним із визначальних структуроутворювальних факторів державного управління, системи забезпечення національної безпеки, є прагнення і ціль зберігати, накопичувати, охороняти, розподіляти, поширювати інформацію, а також здійснювати інші заходи поводження з нею для забезпечення безпеки життєдіяльності людини (індивіда), суспільства та держави.

Це означає, що «інформація» проявляє властивості системоутворювального фактора, який пов'язаний з

виникненням та розгортанням тієї чи іншої системи в усіх сферах державної, публічної, суспільної діяльності.

З іншого боку, з огляду на сутність загальної методології державного управління та основних положень теорії систем як її методологічного ядра можна стверджувати, що:

системний підхід як компонент методології державного управління, його універсальність й всебічність пізнання розгортання соціальної системи, є релевантним інструментарієм у дослідженні практичних проявів феномену інформація, з одного боку, в частині державного управління та державно-управлінської діяльності, з іншого – регулювання інформаційної політики, забезпечення інформаційної безпеки як складової національної безпеки. Застосування прийомів і методів системного підходу робить можливим також проведення ефективного навчання в освітній галузі державного управління, дослідження феномену інформація, прогнозування та моделювання його проявів у різних аспектах державно-управлінської діяльності;

наявність соціальної мережі взаємодії між безпосередньо елементами й усією системою в цілому, функціонування якої забезпечують ІКТ, ієрархічність і статусність системи в публічному просторі сприяє значною мірою досягненню ефективності управлінського впливу органами державного управління, як суб'єкта, регулюванням поводження з інформацією;

цільова діяльність органів влади на збереження, захист, вироблення, поширення, розподіл та інші види поводження з інформацією зумовлює основу для утворення системи. А, профіль такої системи, направленість, характеристики, інші атрибути – у залежності від фактора що її утворює;

системна методологія, як платформа-ядро державного управління, сприяє ефективному розподілу сфер поводження з інформацією, як системоутворювального фактора, розподілу функціональних зв'язків між ключовими стейкхолдерами сектора безпеки, інформаційного, медійного або іншого простору, визначенню їх функціональних обов'язків;

через утворення публічного простору формуються напрями суспільної трансформації залученням суб'єктів

правовідносин з числа інститутів громадянського суспільства та інших інституцій до вироблення чи реалізації управлінських рішень щодо досягненням консенсусу між державою і суспільством на основі інформації утому числій й щодо забезпечення національної безпеки.

Запитання та завдання для самоконтролю

1. Дайте загальну характеристику сучасного стану розкриття змісту концепту «інформація»
2. Дайте загальну характеристику сучасного стану розкриття змісту концепту «інформаційна безпека»
3. Чому інформації, якщо її розглядати крізь призму інформаційної безпеки має об'єктивно-суб'єктивну природу?
4. Чому інформація є атрибутом буття об'єктів соціальних взаємодій?
5. Розкрийте зміст органічного та атрибутивного підходів до розкриття сутності інформації

та внутрішній і зовнішній аспекти її існування як субстанції

6. Розкрийте зміст підходів щодо розкриття змісту інформації у контексті її властивостей та джерел
7. Чому достовірність інформації є однією з суб'єктивно-об'єктивних її характеристик

та вимог, що висуваються до неї?

8. Дайте загальну характеристику інформації як визначального джерела влади в сучасних суспільствах
9. Чому інформація є одним із визначальних чинників забезпечення державної безпеки?
10. Чому інформація є одним із визначальних чинників забезпечення соціального порядку?
11. Розкрите зміст поглядів Е.Тоффлера на інформацію як чинник модернізації моделей державного управління
12. Які основні передумови та цілі сучасних інформаційних війн.?
13. Розкрийте сучасну роль інформації в управлінні у сфері національної безпеки

14. Розкрийте роль інформаційної складової масової культури

15. Чому масова культура в сучасних умовах є одніє із загроз національній безпеці?

16. Розкрийте сутність проблеми осмислення сучасної ролі інформації в державному управлінні у сфері національної безпеки

17. Дайте загальну характеристику еволюції історико-правових аспектів сутності феномену інформації

18. Дайте загальну характеристику еволюції світоглядно-філософських аспектів сутності феномену інформації.

19. Дайте загальну характеристику еволюції соціальних аспектів сутності феномену інформації.

20. Чому державно-управлінські виміри прийняття рішень залежать від чисельних факторів інформаційного характеру?

21. Розкрийте роль інформації в суб'єкт-об'єктній взаємодії в системі державного управління

22. Які аксіоми маютьвраховувати при управління інформаційним простором згідно Г.Почепцова?

23. Чому інформація є системоутворювальний фактор управлінської діяльності у сфері національної безпеки?

Список рекомендованої літератури

1. Бухтатий О. Публічні комунікації демократичної держави: монографія. Дніпро: Журфонд, 2018. 297 с.

2. Державне управління : підручник : у 2 т. / Нац. акад. держ. упр. при Президентові України ; ред. кол. : Ю. В. Ковбасюк (голова), К. О. Ващенко (заст. голови), Ю. П. Сурмін (заст. голови) [та ін.]. - К. ; Дніпропетровськ: НАДУ, 2012. Т. 1. 564 с.

3. Державно-громадянська комунікація: шлях від кризи до взаємодії: монографія / Козаков В.М., Рашковська О.В., Ребкало В.А., Романенко Є.О., Чаплай І.В. К.: ДП "Вид. дім "Персонал", 2017. 288 с.

4. Доронін І.М. Національна безпека України в інформаційну епоху: теоретико-правове дослідження.

Дис…докт. юрид. наук: 12.00.01; Наук.-досл. інст. інформ. і права, Нац. акад. прав. наук України. Київ. 2020.539 с.

5. Драгомирецька Н.М., Кандагура К.С., Букач А.В. Комунікативна діяльність в державному управлінні: навч. посібник. Одеса: ОРІДУ НАДУ, 2017. 180 с.

6. Дрешпак В.М. Комунікації в публічному управлінні: навч. пос. Д. : ДРІДУ НАДУ, 2015. 168 с.

7. Глобальна та національна безпека: підручник / авт.кол.: В.І. Абрамов, Г.П. Ситник, В.Ф. Смолянюк та інш.; за заг.ред. Г.П. Ситника. К.: НАДУ, 2016. 784 с.

8. Глобалізаційні виклики сучасності: підручник /авт.кол. Л.Г. Комаха, І.В. Алексеєнко, В.Л. Гура та ін.; за заг.ред. Л.Г. Комахи.- К.: ВПЦ "Київський університет", 2022. 350 с.

9. Звоздецька О. Дезінформація як загроза національній безпеці Європейського Союзу: проблеми та підходи. *Історико-політичні проблеми сучасного світу: Збірник наукових статей.* Чернівці : Чернівецький національний університет, 2021. Т. 43. С. 30-39. DOI : https:// 10.31861/mhpi2021.43.30-39.

11. Інформаційна складова державної політики та управління : монографія / Соловйов С.Г., та ін. ; заг. ред. Грицяк Н.В. ; НАДУ. К.: К.І.С., 2015. 320 с.

12. Климанська Л. Д. Соціально-комунікативні технології в політиці: таємниці політичної «кухні». Львів: Видавництво Національного університету «Львівська політехніка», 2007. 332 с.

13. Маліновська О.Я. Використання сучасного зарубіжного досвіду комунікацій в системі публічного адміністрування // *Збалансоване природокористування* № 2. 2022. С.39-44

14. Ніколаєнко Н.О. Інформаційна безпека та політична комунікація: навч.-метод. посібник. Миколаїв: НУК, 2022. 121 с.

15. Орел М.Г. Теоретичні основи державного управління у сфері політичної безпеки: монографія. Київ: Поліграф плюс 2019. 320 с.

16. Основи теорії управління у сфері національної безпеки: курс лекцій / Г.П. Ситник. К: ТОВ "САК Лтд.", 2023. 174 с.

17. Пацурія Н. Упровадження технологій штучного інтелекту в забезпечення національної безпеки та обороноздатності України: правові проблеми і перспективи повоєнного періоду// *Теорія і практика інтелектуальної власності* . №3.2023. С.68-78

18. Почепцов Г.Г. Від покемонів до гібридних війн: нові комунікативні технології XXI століття. Київ: Києво-Могилянська академія, 2017. 260 с.

19. Почепцов Г.Г. Державна інформаційна політика в Україні: шляхи вдосконалення [Електронний ресурс]: підручник / Г.Г. Почепцов. – Режим доступу: http://pidruchniki.ws/149 40511/politologiya/derzhavna_ informatsiyna_politika_ ukrayini_ shlyahi_vdoskonalennya.

20. Про доступ до публічної інформації: закон України від 13.01.2011 № 2939-VI. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi

21.Про інформацію: закон України від 02.10.1992 № 2657-XII. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi

22.Публічне управління та адміністрування у сфері національної безпеки: (системні, політичні та економічні аспекти): словник-довідник / С.П. Завгородня, М.Г. Орел, Г.П. Ситник [уклад.] /за заг.ред. Д.В. Неліпи, Є.О. Романенка, Г.П. Ситника. Київ: Видавець Кравченко Я.О., 2020. 380 с.

23. Саврук М. Проблеми інформаційної політики України в контексті забезпечення інформаційної безпеки. *Вісник Львівського університету. Серія міжнародні відносини*. 2017. Випуск 43. С. 172-184.

24. Ситник Г.П., Орел М.Г. Публічне управління у сфері національної безпеки: підручник /за ред. Г.П. Ситника. - Київ: Видавець Кравченко Я.О., 2020. 360 с.

25. Ситник Г., Бондар В., Орел М. Системний підхід дослідження феномену інформація в державному управлінні // Вісник Київського національного університету імені Тараса Шевченка. - Державне управління. №4. 2023. С. С. 63-74

26. Ситник Г.П. Концептуалізація “інформаційної безпеки” у контексті властивостей інформації як специфічної субстанції // *Державне управління: удосконалення та розвиток*. 2020. № 3. URL: http://www.dy.nayka.com.ua/?op=1&z=1595.

27. Стратегія інформаційної безпеки. Указ Президент України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

28. Турчак А. Основні складові інформаційної безпеки держави. *Аспекти публічного управління*. Том 7. №5, 2019. С.44-56

29. Ярова Г.Д. Генезис наукових поглядів на комунікації у публічному управлінні // *Інвестиції: практика та досвід* № 11. 2021. С.103-107

РОЗДІЛ 2
ІНФОРМАЦІЙНО-АНАЛІТИЧНА ДІЯЛЬНІСТЬ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

ГЛАВА 4. ІНФОРМАЦІЙНО-АНАЛІТИЧНА ДІЯЛЬНІСТЬ ЯК СКЛАДОВА УПРАВЛІННЯ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

4.1. Інформаційно-аналітична діяльність та взаємозалежність управлінської інформації і управлінських функцій

Поняття, мета та сутнісні риси інформаційно-аналітичної діяльності. Інформаційно-аналітична діяльність у сфері національної безпеки це вид управлінської роботи. Вона зорієнтована на системний аналіз безпекових аспектів тих чи інших сфер життєдіяльності людини (індивіда), соціальних груп, суспільства та соціальних інститутів (наприклад – інститутів держави).

Головною метою інформаційно-аналітичної діяльності у сфері національної безпеки є виявлення тенденцій, закономірностей та особливостей розвитку об’єктів (процесів, систем, явищ), підготовка пропозицій керівництву щодо вирішення виявлених проблем (управлінських альтернатив), оцінка можливих наслідків реалізації тих чи інших управлінських рішень.

Щоб виявити сутнісні риси інформаційно-аналітичної діяльності,необхідно вивчити складові цього поняття.

Поняття інформація означає «роз'яснення, виклад, уявлення», а загальна теорія інформації сформувалася наприкінці XIX-початку XX століть. В той час слово інформація почало вживатися як термін, що позначав «завдання вільної преси, яке полягало інформуванні читачів про реальний стан справ. При цьому акцентувалась увага на тому, що преса повинна постачати відомості, а не нав’язувати ідеї та думки.

У середині 50-х роках XX ст., родоначальник кібернетики Н. Вінер сформулював базовий принцип єдності інформації та

управління. Він використав поняття «інформація» для забезпечення змісту, отриманого із зовнішнього світу в процесі пристосування до нього людини. Проте Н. Вінер вважав що його розуміння інформації окреслює лише ту форму інформації, яка є результатом взаємодії людини з середовищем і є відображенням об'єктивного розмаїття останньої в людській психіці.

Як ми зазначали, «інформація» як більшість первинних понять типу «матерія», «простір», «час» невизначена повною мірою. Водночас вона невід'ємний атрибут будь-якої діяльності, що вказує на характер мети, способи визначення найкоротшого шляху до неї, методи подолання цього шляху тощо. Тому безперервна циркуляція інформації між керуючої та керованої підсистемами (суб'єктом та об'єктом), між окремими їх складовими частинами (компонентами) є необхідною, невід'ємною частиною (атрибутом) управління та всіх його функцій. І саме ця обставина визначає місце та роль інформації, інформаційно-аналітичної діяльності.

Взаємозалежність управлінської інформації та управлінських функцій. При управлінні суспільством під інформацією розуміють повідомлення, що містять відомості про навколишній світ, про внутрішній стан системи та зовнішні умови, які керуюча система використовує у здійсненні управлінських процесів.

Кожна з функцій управління здійснюється лише на основі інформації. Тому інформація є постійно діючим фактором, роль і значення якого в кожному конкретному випадку визначаються метою, змістом тієї чи іншої функції управління.

При цьому будь-яке управлінське рішення являє собою перетворену інформацію, яка безпосередньо необхідна для формування та реалізації управлінських впливів та передається по каналах прямого та зворотного зв'язку. І саме ця обставина визначає місце та роль ІКТ та інформаційних систем в управлінських процесах у сфері національної безпеки.

Таким чином, управлінська інформація безпосередньо пов'язана з функціями, які поетапно виконує управлінська система, серед яких:

збір директивної інформації, та інформації про стан організації та основних факторів зовнішнього середовища;

переробка отриманої інформації (аналіз, формалізація, обробка, оцінка достовірності тощо), розробка альтернативних варіантів управлінського рішення (основне завдання цього етапу полягає в тому, щоб «стиснути» інформацію, привести її до вигляду, зручного для ухвалення рішення;

ухвалення управлінського рішення (головним продуктом цього етапу є інформація, яка відображена у рішенні та спрямована на об'єкт управління);

передача необхідної інформації до об'єкта управління та здійснення заходів, що забезпечують адекватне її сприйняття всіма, на кого спрямовано управлінський вплив;

організація зворотного зв'язку (потоків облікової, звітної, іншої інформації про характер соціальних процесів, що протікають);

коригування прийнятих рішень відповідно до ситуації, що змінилася в керованій підсистемі і зовнішньому середовищі та інше.

4.2. Класифікація управлінської інформації та вимоги до соціальної інформації

Класифікація, типи та види управлінської інформації. Різноманіття інформації можна поділити на потоки інформації всередині системи та на потоки, що циркулює між системою та зовнішнім середовищем.

Інформація всередині системи створює два типи потоків:

потоки, що циркулюють каналами прямого зв'язку – від суб'єкта до об'єкта (пряма інформація);

потоки, що циркулюють каналами зворотного зв'язку – від об'єкта до суб'єкта (зворотна інформація).

Належна організація прямої інформації забезпечує своєчасне та якісне надходження на об'єкт управління вихідних, коригувальних, контролюючих команд із боку суб'єкта, а зворотної інформації – надходження суб'єкту даних про стан об'єкта і досягненні поставленої ним мети.

Таким чином, завдяки обміну інформацією між компонентами системи та в цілому з навколишнім середовищем, і може здійснюватися їхня взаємодія, внаслідок чого зберігається стійкість, цілісність системи.

Інформацію у системі управління класифікують за різними ознаками:

за якістю інформації: актуальна, достатня, доступна, аутентична тощо;

за джерелами надходження: норми нормативно-правових актів, що уповноважують суб'єкти управління на прийняття певних управлінських рішень;

обов'язкові вказівки вищих органів управління;

факти, що виявляються у процесах контролю, які відображають стан керованих об'єктів;

додаткова інформація (про проблемні, конфліктні, експериментальні та інші складні ситуації, що потребують оперативного та активного втручання суб'єкта управління).

Водночас інформацію поділяють на чотири види, виходячи з її функціональної призначеності: вихідна, регулююча, оперативна та контрольно-облікова.

1. *Вихідна інформація* необхідна для вироблення та прийняття управлінських рішень, самих рішень або управлінських команд, що визначають організацію керуючих та керованих систем. Щоб ухвалити те чи інше рішення, необхідно попередньо отримати *достовірну* інформацію про стан проблеми, яку передбачається вирішити. Тільки на основі глибокого, всебічного *аналітичного* вивчення вихідних даних можна прийняти обґрунтоване управлінське рішення

2. *Регулююча інформація* представлена різного роду параметрами, нормативами, законами, інструкціями, технологічними картами. Така інформація є приписною, але вона у свою чергу передбачає інформацію, що інформує (дескриптивну). Тільки на основі аналізу та переробки цієї інформації можливі переробка та використання інформації, так би мовити, наказового характеру.

3. *Оперативна інформація* надходить у процесі функціонування системи та характеризує її повсякденний стан. Така інформація допомагає суб'єкту управління впорядкувати

управлінський цикл, визначити послідовність операцій у часі та в просторі, вибрати та закріпити структуру суб'єкта та об'єкта управління, розподілити функції між ланками, визначити їх права та обов'язки. У ході реалізації цієї функції управління здійснюється і організація самої інформації, її відбір, взаємодія між її різними потоками та видами, її систематизація та інше.

4. *Контрольно-облікова інформація* характеризує перебіг та результати управлінської діяльності в системі. Цей вид інформації є відомостями, повідомленнями, вираженими, як правило, у кількісних показниках про наявні ресурси та про результати виконання рішень. Облікова інформація, у свою чергу, поділяється на підвиди – статистичну, бухгалтерську, оперативно-технічну. Контрольна інформація нерозривно пов'язана з обліковою. Вона відображає ступінь відповідності процесів і результатів функціонування системи вимогам припису, що полягає в рішеннях: програмах, планах, законах, нормах, стандартах.

Таким чином, управлінська інформація – це базис, який лежить в основі вироблення, прийняття, реалізації управлінських рішень і дозволяє впорядкувати взаємодію об'єкта і суб'єкта управління, сформувати прямі та зворотні зв'язки.

Сутність соціальної інформації та вимоги до неї. Розкриття сутності інформаційно-аналітичної діяльності в соціальних системах потребує визначення поняття «соціальна інформація».

Як правило, поняття «соціальна інформація» визначається як повідомлення, яке може внести зміну до свідомості та поведінки людей, впливає на систему цінностей і шкалу оцінок, що даються громадянам, як лише частина змісту суспільної свідомості. Ця інформація зафіксована в книгах, документах, статтях, радіо- та телепередачах, лекціях, усних повідомленнях та інших носіях. Тому соціальна інформація є сукупністю відомостей, об'єктивно необхідних для функціонування соціального організму, тобто це інформація, що циркулює в суспільстві та впливає на нього.

За змістом соціальна інформація поділяється на наукову, ідеологічну, технічну, економічну, політичну та інші. Тому вона

є багаторівневе знання та найскладнішим видом інформації властивим лише людині.

Таким чином, соціальна інформація – це особливий вид інформації, що з'явився в результаті розвитку свідомості людини та який відображає в узагальненому вигляді суспільні відносини людей (соціальні взаємодії).

Кардинальне ускладнення систем управління у суспільстві призвело до того, що передусім актуалізувалась необхідність вирішення проблеми отримання якісної соціальної інформації (її актуальності, достовірності, повноти тощо) та необхідність своєчасної і всебічної її переробки (аналізу).

Процес поширення інформації в суспільстві покликаний обслуговувати інтереси складних систем (соціальної, політичної, економічної та інших), що складаються з великої кількості компонентів, які потребують забезпечення належного зв'язку та управління.

Поки що відсутнє однозначне трактування змісту поняття «соціальна інформація». Водночас у будь-якому випадку соціальна інформація є певною системою даних (відомостей), які виступають одночасно метою та детермінантами соціальних перетворень тією мірою, в якій вони (відомості) відповідають очікуванням суб'єктам соціальних взаємодій дії та містять необхідний і достатній матеріал для реалізації їх потреб.

З огляду на це, враховуючи наведену вище характеристику управлінської інформації, можна сформулювати загальні вимоги, яким має відповідати соціальна інформація.

По-перше, вона має бути доступною, тобто має бути доведена до суб'єктів соціальних взаємодій, у зв'язку з чим соціальна інформація має циркулювати по тих каналах, до яких суб'єкт має доступ.

По-друге, вона має бути відзначена суб'єктом і виділена їм із усього потоку доступної йому інформації, тобто соціальна інформація має привертати увагу.

По-третє, соціальна інформація повинна спонукати суб'єкта до соціальної дії, тобто повинна містити (у явній чи неявній формі) спонукальний мотив.

Варто акцентувати увагу на тому, що остання вимога є визначальною. Це зумовлено тим, що соціальна інформація з необхідністю та достатністю реалізується лише у процесі перетворюючої діяльності суб'єкта. Але водночас реалізація цих функцій інформації не веде до соціальних перетворень, якщо відсутня мотив (ідея) цих перетворень.

4.3. Особливості аналітичної діяльності в управлінні та його інформаційно-аналітичне забезпечення

Особливості аналітичної діяльності в управлінських процесах. У сучасному світі інформаційно-аналітична діяльність є невід'ємною частиною ефективних соціально-інформаційних та інформаційно-комунікаційних технологій управління, засобом досягнення належного рівня керованості соціальними системами. Тому після аналізу місця та ролі інформації та соціальної інформації в управлінні соціальними системами (процесами) необхідно здійснити аналіз другої складової поняття «інформаційно-аналітична діяльність», а саме ролі аналітичної діяльності в управлінських процесах.

Ще до початку 90-х років минулого століття аналітична діяльність вивчалася, як правило, у рамках вирішення практичних завдань щодо пошуку оптимальних управлінських рішень в межах дисципліни «дослідження операцій». Вказана дисципліна займається розробкою й застосуванням методів знаходження оптимальних рішень на основі математичного моделювання у різних сферах життєдіяльності суспільства та держави. Ці дослідження з пов'язані з системним аналізом, математичним програмуванням, теорією оптимальних рішень і передбачають використання математичного апарату.

Свою ефективність дослідження операцій показали у роки другої світової війни при планування бойових дій. Так, фахівці з дослідження операцій працювали в командуванні бомбардувальної авіації США. Ними досліджувалися численні фактори, що впливають на ефективність бомбардування. Були вироблені рекомендації, що призвели до чотириразового підвищення ефективності бомбардування.

Так, залучення до командування фахівців з дослідження операцій дозволило встановити такі маршрути патрулювання й такий розклад польотів, при яких імовірність залишити об'єкт непоміченим була зведена до мінімуму. Отримані рекомендації були застосовані для організації патрулювання над південною частиною Атлантичного океану з метою перехоплення німецьких кораблів з військовими матеріалами. З п'яти ворожих кораблів, що прорвали блокаду, три були перехоплені на шляху з Японії в Німеччину, один був виявлений і знищений у Біскайській затоці і лише одному вдалося зникнути завдяки ретельному маскуванню.

По закінченні другої світової війни групи фахівців з дослідження операцій продовжили свою роботу в збройних силах США і Великої Британії. Публікація ряду результатів у відкритій пресі викликала сплеск суспільного інтересу до цього напрямку. Виникає тенденція до застосування методів дослідження операцій у комерційній діяльності, з метою реорганізації виробництва, перекладу промисловості на мирні рейки. Дослідження операцій стало застосовуватися при плануванні і проведенні деяких державних, соціальних і економічних заходів. Так, наприклад, дослідження, проведені для міністерства продовольства, дозволили прогнозувати вплив політики урядових цін на сімейний бюджет. Лідерство в області застосування наукових методів керування належало авіаційній промисловості, що не могла не йти в ногу зі зростаючими вимогами військових. В 50-ті-60-ті роки на Заході створюються суспільства та центри дослідження операцій, ряд університетів США включає цю дисципліну у свої навчальні плани.

Методи дослідження операцій не являють собою єдиного універсального апарату, придатного для вироблення рішень на всі випадки життя. Дослідження операцій— це набір різних математичних методів, об'єднаних спільним завданням обґрунтування найкращих рішень. Кожен з цих методів має свою область застосування. Методи дослідження операцій можуть бути віднесені до чотирьох основних груп: аналітичні, статистичні, математичного програмування, теоретико-ігрові.

Аналітичні методи характерні тим, що встановлюються аналітичні, формульні залежності між умовами розв'язуваної

задачі та її результатами. До цих методів належать теорія ймовірностей, теорія марковських процесів, теорія масового обслуговування, динаміка середніх.

Теорія ймовірностей — наука про закономірності у випадкових явищах. З її допомогою виробляються рішення, що залежать від умов випадкового характеру.

Теорія марковських випадкових процесів розроблена для опису операцій, що розвиваються випадковим чином в часі.

Теорія масового обслуговування розглядає масові повторювані процеси.

Метод динаміки середніх застосовується в тих випадках, коли можна скласти залежності між умовами операції і її результатом виходячи із середніх характеристик зазначених умов.

Статистичні методи засновані на зборі, обробці та аналізі статистичних матеріалів, отриманих як в результаті фактично дій, так і вироблених штучно шляхом статистичного моделювання на ЕОМ. До цих методів належать послідовний аналіз і метод статистичних випробувань.

Послідовний аналіз дає можливість ухвалювати рішення на основі низки гіпотез, кожна з яких відразу ж послідовно перевіряється, наприклад під час перевірки якості партії виробів.

Метод статистичних випробувань (Монте -Карло) полягає в тому, що хід операцій програється, мовби копіюється на ЕОМ, з усіма притаманними операції випадковостями.

Математичне програмування є низкою методів, призначених для найкращого розподілу наявних обмежених ресурсів, а також для складання раціонального плану операції. Математичне програмування підрозділяється на лінійне, нелінійне і динамічне. Сюди ж зазвичай відносять і методи *мережевого (сіткового) планування*.

Лінійне програмування застосовується в тих випадках, коли умови ведення операцій описуються системою лінійних (1-го ступеня) рівнянь або нерівностей. У разі, якщо зазначені залежності носять нелінійний характер (2-й і більші ступені), застосовується метод нелінійного програмування.

Динамічне програмування служить для вибору найкращого плану виконання багатоетапних дій, коли результат кожного наступного етапу залежить від попереднього.

Мереживе (сіткове) планування призначене для складання та реалізації раціонального плану ведення операції, що передбачає розв'язання задачі в найкоротший термін і з найкращими результатами. Призначені для обґрунтування рішень в умовах невизначеності (неповноти, неясності) даних обстановки.

До теоретико-ігрових методів належать *теорія ігор і теорія статистичних рішень.* Теорія ігор застосовується в тих випадках, коли невизначеність обстановки викликана свідомими, зловмисними діями конфліктуючої сторони. Теорія статистичних рішень застосовується тоді, коли невизначеність обстановки викликана об'єктивними обставинами, які або невідомі, або носять випадковий характер.

В цілому дослідження операцій не розглядались як самостійна галузь наукових знань. Проте в останні десятиліття у розвинутих країнах почали застосовувати нові соціально-інформаційні технології та інформаційно-комунікаційні технології. Вони різко збільшили інтенсивність інформаційних потоків та кількість інформаційних сплесків. Головним наслідком став *новий інформаційний режим*. Це режим супроводжується глобалізацією інформаційної взаємодії та взаємозалежності, підвищенням ролі та значення соціально-інформаційних технологій управління в соціумі.

Необхідність здійснювати цілеспрямовану політику, ефективно діяти за умов нового інформаційного режиму зажадала виходу на якісно інший рівень аналітичної діяльності розвинених західних країнах, створення відповідних інформаційних систем та технологій, а в Україні призвела до усвідомлення важливості цієї діяльності.

Широка громадськість мала можливість спостерігати застосування аналітики, аналітичного супроводу у політичній, економічній та конкурентній боротьбі, у процедурах лобіювання чиїхось інтересів при прийнятті рішень у найвищих сферах вітчизняної політики, у масових рекламних кампаніях, у кампаніях з маніпуляції суспільною думкою, коли стикалися

думки різних заангажованих аналітиків, у великомасштабних та локальних інформаційних конфліктах, дезінформаційних акціях тощо, які набували обрисів та характеру інформаційної війни за владу та ресурси.

Факти негативного прояву аналітичної діяльності особливо гостро сприймаються широкими масами. При цьому очевидно, що слабкість інститутів громадянського суспільства, відсутність незалежних каналів висвітлення альтернативної думки з боку громадянського суспільства сприяли негативному впливу заангажованих аналітиків на суспільство загалом.

Аналітична діяльність виконує насамперед завдання змістовного перетворення інформації. Функціонально вона перетинається у цьому плані з науковою діяльністю, метою якої є виробництво нового знання, та управлінською діяльністю, метою якої є розробка варіантів рішень, сценаріїв та прийняття відповідних рішень. Тому кінцевим результатом аналітичної діяльності є, як правило, новий інформаційний продукт.

Інформаційно-аналітичне забезпечення управлінської діяльності. Визначена сутність інформаційно-аналітичної діяльності через визначення місця та роль інформації та аналітики в управлінні свідчить, що інформаційно-аналітична діяльність передує виконанню всіх основних функцій управління, які черпають у його результатах необхідну інформацію. Тобто інформація та аналіз будучи нерозривно пов'язані між собою та будучи невід'ємною частиною управління, формують самостійний вид діяльності – інформаційно-аналітичне забезпечення управління.

Сьогодні в різних країнах, передусім у провідних, відбувається активний процес становлення інформаційної аналітики. Він супроводжується такими процесами, як інституціоналізація (формування організаційно-правових засад), професіоналізація (підготовка відповідних кадрів) та соціалізація (виокремлення інформаційної аналітики в окремий вид забезпечення управлінської діяльності). Ці процеси призвели до створення певних основ інформаційно-аналітичної діяльності, але поки що не сформували цілісну систему її функціонування в різних сферах життя суспільства. Йдеться про систему яка б могла забезпечувати належну якість

управлінських рішень на різних ієрархічних рівнях управління та етапах їх прийняття. Прийняття таких рішень особливо важливо у сфері національної безпеки та в умовах кризових ситуацій, оскільки ці рішення, як правило, мають доленосний (визначальний) характер длябезпеки життєдіяльності людини (індивіда) та соціальних інститутів, у тому числі політичної системи.

При цьому зростає як позитивний, так і негативний вплив результатів інформаційної аналітики на життя соціуму. Це свідчить про необхідність подальшої розробки теорії інформаційно-аналітичної діяльності та створення відповідних служб та центрів аналізу інформації (інформаційно-аналітичних, ситуаційних та інших центрів).

4.4. Зміст та основні завдання інформаційного та інформаційно-аналітичного забезпечення у сфері національної безпеки

Інформаційне забезпечення у сфері національної безпеки – це діяльність з надання потрібної інформації для управління із заданою періодичністю. Тобто це певні заходи для створення інформаційного середовища управління.

Зміст інформаційного забезпечення у сфері національної безпеки полягає у:

задоволенні інформаційних потреб органів управління;

формуванні, розміщенні, наповненні, підтримці, актуалізації та використанні інформаційних ресурсів організації, на яку покладаються виконання відповідних безпекових завдань;

створенні та розвитку інформаційних систем обробки та передачі інформації.

Тому у процесі інформаційного забезпечення у сфері національної безпеки вирішуються низка завдань, зокрема щодо:

відбору первинних відомостей та джерел необхідної інформації;

систематизації та класифікації наявної інформації;

безперервного процесу збору, переробки та поширення інформації до відповідних адресатів;

забезпечення доступу до інформаційних ресурсів (як правило, за чітко унормованою процедурою);

приведення інформації до визначеного керівними документами єдиного формату;

фільтрації, агрегування та актуалізації (своєчасного оновлення) інформації.

Інформаційне забезпечення дозволяє обробляти інформацію, використовуючи при цьому всі можливі технічні засоби, здійснювати сумісність локальних продуктів, зменшувати дублювання інформаційної діяльності. Тобто в основі інформаційного забезпечення техніко-технологічний, кібернетичний підхід до обробки інформації, який практично реалізовуються у спеціально створюваних інформаційних системах, які використовують сучасні інформаційні технології та ЕОМ.

В основі інформаційно-аналітичного забезпечення у сфері національної безпеки аналітична, а не технічна обробка інформації, тобто синтез інформації та аналізу.

Інформаційно-аналітичне забезпечення в інтересах управлінської діяльності може розглядатися у різних аспектах, зокрема як:

особлива галузь людської діяльності, покликана забезпечити інформаційні потреби суб'єктів управління за допомогою аналітичних технологій та отримання якісно нового знання;

основа в соціальному управлінні, а саме: діяльність, направлена на систематичне отримання об'єктивної, оптимальної, інформації про актуальні, соціально значущі процеси в суспільстві, діагностику та прогнозування їх розвитку, для прийняття ефективних управлінських рішень;

як системна єдність процесів збору, обробки та аналізу інформації, що здійснюються в інтересах встановлення поточного стану та тенденцій зміни суб'єкта та об'єкта управління, середовища їх взаємодії, а також в інтересах синтезу прогностичних моделей та прогнозів зміни ситуації в системі, утвореної сукупністю суб'єкта та об'єкта управління і,

таким чином, як фактор легітимності та спосіб підвищення ефективності управління.

Досягнення інформаційної аналітики у сфері збору та обробки даних дозволяють прогнозувати в національному масштабі оперативне реагування на виклики та загрози національним інтересам.

Водночас домінуванням техніко-технологічного підходу до управління, який з появою сучасних ІКТ перейшов на новий рівень, може призвести до небезпеки нерозуміння важливості ролі інформаційно-аналітичних ресурсів.

Зосередження уваги на самій постановці проблеми, розробці систем підтримки прийняття рішень перетворює процес прийняття рішень на виконавчому рівні на самоціль. Ціль управління як функції політичної влади розмивається, процес відривається від змісту і починає функціонувати сам по собі. Тому процес управління перетворюється на своєрідний ланцюжок слабко пов'язаних з реальним життям нормативно-правових актів, що призводять до непередбачених соціальних наслідків. Необхідна переорієнтація процесу створення системи підтримки ухвалення рішення на процес функціонування інформаційно-аналітичного забезпечення влади.

В цілому недооцінка статусу інформаційно-аналітичних ресурсів влади як сегменту ринку інформації, інформаційних та телекомунікаційних технологій та послуг веде до відставання органів влади від новостворених економічних структур у цій сфері.

Варто пам’ятати, що навіть знання про наявність необхідної інформації не гарантує її отримання, бо відносини між джерелами та споживачами інформації можуть бути не регламентовані належним чином.

Варто також акцентувати увагу на тому, що в органах державної влади сьогодні відбувається певний перекіс у бік використання інформаційного забезпечення управління. Одна з причин полягає в тому, що більшість коштів, які направляються на інформатизацію, витрачається на придбання техніки без інтелектуальних програмних засобів обробки інформації. За такого підходу в органах управління, оснащених сучасними комп'ютерами, не створюється якісно нова інформація –

інформація для прийняття рішення, а технічні ресурси використовуються вкрай неефективно.

Загальновідомо, що ефективність державного управління, у тому числі й у сфері національної безпеки повинна будуватися на зміцненні постійного та рівноправного діалогу органів влади та суспільства, стимулюванні залучення громадян у процес управління, узгодженні діяльності влади з суспільними інтересами. Тому слід враховувати, що інформаційно-аналітична діяльність органів державної влади носить двоєдиний характер. Вона включає не тільки вплив органів влади на інститути громадянського суспільства, а й громадськості на владу.

Враховуючи вищевикладене, можна розділити функції інформаційно-аналітичного забезпечення у сфері національної безпеки на дві групи:

внутрішню – інформаційно-аналітичний супровід прийняття управлінських рішень в системі забезпечення національної безпеки;

зовнішню – інформаційно-аналітичне забезпечення взаємодії суб'єктів системи забезпечення національної безпеки із суспільством.

До внутрішньої групи функцій, що забезпечують інформаційно-аналітичний супровід діяльності органу управління, пов'язаної з прийняттям конкретних управлінських рішень, слід віднести.

забезпечення внутрішніх комунікацій органу управління, організація доступу до зовнішніх та внутрішніх інформаційно-аналітичних продуктів;

забезпечення необхідного рівня якості прийнятих рішень за рахунок: збору, аналітичної обробки та надання органу управління в різних режимах фактографічної інформації про поточну, бажану та прогнозовану ситуацію в об'єкті управління та в зовнішньому середовищі;

збирання та надання органу управління в різних режимах документів науково-методичного, аналітичного, юридичного характеру та доступу до спеціально організованих фондів вхідних, внутрішніх та вихідних документів;

забезпечення необхідного рівня якості прийнятих рішень за рахунок поглиблення процедур аналізу та прогнозування ситуацій щодо об'єкта управління, а також за рахунок оцінки наслідків прийнятих рішень, прогнозування їх розвитку у вигляді: «підготовки змістовної частини управлінських рішень та їх документального оформлення; аналізу обґрунтованості та юридичної правомірності прийнятих рішень; проведення погоджувальних процедур і процесів групового прийняття рішень

До зовнішньої групи функцій, що забезпечують взаємодію суб'єктів системи забезпечення національної безпеки у процесі її забезпечення слід віднести ряд специфічних соціальних функцій: демократизації державного управління; сприяння розвитку інститутів громадянського суспільства; організації соціальної взаємодії органів виконавчої влади та громадянського суспільства; встановлення соціальної злагоди у суспільстві; формування соціально-ідеологічних установок громадянського суспільства.

Перелічені соціальні функції інформаційно-аналітичного забезпечення управління у сфері національної безпеки взаємообумовлені причинно-наслідковими зв'язками, одну мету не можна досягти без іншої. Але ключовим моментом є забезпечення належної взаємодії громадянського суспільства та держави. Взаємодія інститутів громадянського суспільства та органів державної влади пов'язана з вирішенням важливої проблеми у сфері національної безпеки, а саме пошуком шляхів досягнення політичної та громадянської злагоди, подолання кризи у відносинах між державою та суспільством, необхідністю формування більш ефективного механізму взаємовідносин законодавчих та виконавчих органів влади, розвитку державних та громадських засад в управлінні державою.

Тому сутність інформаційно-аналітичного забезпечення управління у сфері національної безпеки полягає у наданні органам влади необхідної інформації, яка правильно орієнтувала б їх при підготовці та прийнятті рішень; в об'єктивному виявленні ставлення громадськості до прийнятих рішень (зворотній зв'язок); широкому інформуванні населення

про основні напрямки діяльності органів влади, про плани та перспективи цієї роботи; у виявленні громадської думки про найбільш важливі проблеми, які необхідно вирішувати органам влади у сфері національної безпеки.

ГЛАВА 5. ІКТ ТА ПРОБЛЕМИ ЇХ РОЗВИТКУ У КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

5.1. Взаємозв'язок інформації та інформаційних технологій та етапи їх розвитку

Взаємозвязок інформації та інформаційних технологій. На етапі переходу до інформаційного суспільства ступінь розвитку інформаційного простору та інформаційних технологій є чинником становлення активного та свідомого громадянина та конкурентоспроможності держави. Тому постіндустріальне суспільство є передусім інформаційним, в якому здійснюється інформатизація всіх сфер життєдіяльності суспільства та держави.

Поняття інформація є досить абстрактне. Воно може мати різні значення залежно від контексту. Походить від латинського слова «informatio», яке має декілька значень: роз'яснення; виклад фактів, подій; витлумачення; представлення, поняття; ознайомлення, просвіта.

У будь-якому випадку, інформація – це нові відомості, які прийняті, зрозумілі і оцінені її користувачем як корисні. Тобто інформація – це нові знання, які отримує споживач (суб'єкт) у результаті сприйняття і переробки певних відомостей.

Важливим є також поняття «дані». Походить від лат. *data*, множина від лат. *datum* від лат. *dare* – давати, щось дане, наприклад:

відомості, показники, необхідні для ознайомлення з ким, чим-небудь, для характеристики когось, чогось або для прийняття певних висновків, рішень;

здібності, якості, необхідні для чого-небудь;

форма представлення знань. Тексти, таблиці, інструкції, відомості про факти, явища і таке інше, представлені у

буквено-цифровій, числовій, текстовій, звуковій або графічній формі.

Дані можуть зберігатися на різних носіях, в тому числі в ЕОМ та пересилатися і піддаватися обробці. Їх носіями даних може бути папір, магнітний диск тощо. У ході інформаційного процесу дані перетворюються із одного виду в інший за допомогою різних методів. Обробка даних вимагає здійснення багатьох операцій. Серед них можна виділити такі операції:

збирання даних – це накопичення для забезпечення достатньої повноти для прийняття рішення;

формалізація даних – приведення даних, що надходять від різних джерел до однакової форми;

фільтрація даних – відсіювання "зайвих" даних, у яких нема необхідності для прийняття рішення;

сортування даних – упорядкування даних за заданою ознакою, що дозволяє підвищити доступність даних;

архівація даних – організація зберігання даних, що дозволяє зменшити витрати для зберігання даних і підвищує надійність інформаційного процесу;

захист даних – заходи, що спрямовані на запобігання втрат, відтворення та модифікацію даних;

перетворення даних – переведення даних із однієї форми в іншу або із однієї структури в іншу, яке часто пов'язане із зміною типу носія.

Слово *технологія* в перекладі з грецької – наука, сукупність методів та прийомів обробки матеріалів або сировини, переробки їх у предмети споживання.

Сучасне розуміння цього слова включає не тільки сукупність процесів матеріального виробництва і сфери послуг, а й перетворення та використання матерії (матеріалів), енергії, інформації, наукових та інженерних знань для вирішення практичних завдань в інтересах людини й суспільства.

Інформаційні технології (ІТ) – сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, опрацювання, зберігання, розповсюдження, показу і використання інформації в інтересах її користувачів. Цим терміном позначають всі

технології, що використовуються для спілкування та роботи з інформацією.

За Дж. Велінгтоном, інформаційні технології – це системи, створені для виробництва, передачі, відбору, трансформації (обробки) і використання інформації у вигляді звуку, тексту, графічного зображення і цифрової інформації.

Інформаційні технології використовуються для великих систем обробки даних, обчислення на персональному комп'ютері, науці і освіті, управлінні, автоматизованому проектуванні істворенні систем з штучним інтелектом.

Інформаційні технології – сучасні технологічні системи величезного стратегічного значення (політичного, оборонного, економічного, соціального і культурного). ІКТ відноситься не лише до сфери високотехнічних процесів і біотехніки, але і до області лінгвістики, економіки, освіти, впливаючи, таким чином, на наше життя в цілому.

Бурхливий розвиток інформаційних технологій, конвергенція комп'ютерних систем, комунікацій різних видів, індустрії розваги, виробництва побутової електроніки призводять до необхідності переглянути уявлення про інформаційну індустрію, її роль і місце в суспільстві.

Етапи розвитку інформаційних технологій. Якщо в якості ознаки інформаційних технологій вибрати інструменти, за допомогою яких проводиться обробка інформації (інструментарій технології), то можна виділити наступні етапи її розвитку :

перший етап (до другої половини XIX ст.) - «Ручна» інформаційна технологія, інструментарій якої складали: перо, чорнильниця, книга. Комунікації здійснювалися ручним способом шляхом передачі поштою листів, пакетів. Основна мета технології - представлення інформації в потрібній формі.

другий етап (з кінця XIX ст.) - «Механічна» технологія, оснащена більш досконалими засобами доставки пошти, інструментарій якої складали: друкарська машинка, телефон, диктофон. Основна мета технології - представлення інформації в потрібній формі більш зручними засобами;

третій етап (40 - 60-і рр.. XX ст.) - «Електрична» технологія, інструментарій якої складали: великі ЕОМ і

відповідне програмне забезпечення, електричні друкарські машинки, ксерокси, портативні диктофони. Основна мета технології - починає переміщатися з форми представлення інформації на формування її змісту;

четвертий етап (з початку 70-х рр..) - «Електронна» технологія, основним інструментарієм якої стають великі ЕОМ і створені на їхній базі автоматизовані системи управління (АСУ) і інформаційно-пошукові системи, оснащені широким спектром базових і спеціалізованих програмних комплексів. Центр ваги технології ще більш зміщується на формування змістовної сторони інформації для управлінського середовища різних сфер суспільного життя, особливо на організацію аналітичної роботи;

п'ятий етап (з середини 80-х рр.) - «Комп'ютерна» («нова») технологія, основним інструментарієм якої є персональний комп'ютер із широким спектром стандартних програмних продуктів різного призначення. На цьому етапі відбувається процес персоналізації АСК, що проявляється у створенні систем підтримки прийняття рішень певними спеціалістами. Подібні системи мають умонтовані елементи аналізу та штучного інтелекту для різних рівнів управління, реалізуються на персональному комп'ютері і використовують телекомунікації. У зв'язку з переходом на мікропроцесорну базу змінам піддаються і технічні засоби побутового, культурного та іншого призначень;

шостий етап (поточний) - «мережева технологія» (іноді її вважають частиною комп'ютерних технологій). Починають широко використовуватися в різних галузях глобальні і локальні комп'ютерні мережі. Їй пророкують в майбутньому бурхливе зростання, обумовлене популярністю її засновника - глобальної комп'ютерної мережі Internet.

З появою персональних комп'ютерів з'явився термін "нові інформаційні технології". Під ними розуміють впровадження орієнтовані на розвиток творчого потенціалу людини з метою підвищення ефективності його використання, завдяки застосуванню сучасних технічних засобів. Використовувані способи і засоби пов'язані з комп'ютером, тому їх іще називають комп'ютерні технології.

Таким чином, інформаційна технологія – це технологія обробки даних (інформаційного ресурсу), яка складається з сукупності технологічних елементів: збирання, накопичення, пошуку, обробки, передачі даних користувачам на основі сучасних технічних засобів.

5.2. Структура ІКТ та інформатизація суспільства

ІКТ є одним з важливих чинників стимулювання економічного зростання та розвитку громадянського суспільства, зайнятості населення, розширення конкуренції і, як наслідок, сприяння подоланню "цифрового розриву".

Концепція інформаційних технологій була додана до елементу комунікації і виникла у 1980-ті роки. Наразі ІКТ включають апаратні засоби (комп'ютери, сервери, тощо) та програмне забезпечення (операційні системи, мережеві протоколи, пошукові системи, тощо). Тобто ІКТ – це засоби пов'язані зі створенням, збереженням, передачею, обробкою і управлінням інформації. Термін ІКТ включає в себе всі технології, що використовуються для спілкування та роботи з інформацією.

У сучасному світі ІКТ є важливою і невіддільною частиною держави, бізнесу та приватного життя, а термін ІКТ використовується для позначення об'єднання (конвергенції) аудіовізуальних та телефонних мереж з комп'ютерними мережами через один кабель або з'єднувальну систему.

Є великі економічні стимули при об'єднанні аудіовізуальних, телефонних та електромереж з системою комп'ютерної мережі використовуючи одну єдину систему кабелів, сигнал розподілу та управління (економія коштів шляхом вилучення телефонної мережі). Це своєю чергою стимулювало зростання організацій, які використовували термін ІКТ у своїх назвах, щоб вказати на їхню спеціалізацію в процесах об'єднання різних мережевих систем.

ІКТ часто використовується як синонім до інформаційних технологій (ІТ), хоча ІКТ це загальніший термін, оскільки ІКТ складаються з ІТ, а також телекомунікацій, медіа-трансляцій,

усіх видів аудіо і відеообробки, передачі, мережевих функцій управління та моніторингу.

Термін ІКТ підкреслює роль уніфікованих технологій та інтеграцію телекомунікацій (телефонних ліній та бездротових з'єднань), комп'ютерів, програмного забезпечення, накопичувальних та аудіовізуальних систем, які дозволяють користувачам створювати, одержувати доступ, зберігати, передавати та змінювати інформацію.

Таким чином, ІКТ – це сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, обробки, зберігання, розповсюдження, демонстрації та використання даних в інтересах їх користувачів.

Важливою складовою сучасних ІКТ є *обчислювальна техніка* – це сукупність технічних засобів (комп'ютерів, пристроїв, приладів), призначених для автоматизації процесів обробки даних, розв'язування задач, що потребують великого обсягу обчислень, обробки даних експериментів і т. ін.

Поняття ІКТ не є однозначним. Узагалі ІКТ можна визначити як сукупність різноманітних технологічних інструментів і ресурсів, які використовуються для забезпечення процесу комунікації та створення, поширення, збереження та управління інформацією.

Так, І. Захарова розуміє під ІКТ "конкретний спосіб роботи з інформацією: це і сукупність знань про способи та засоби роботи з інформаційними ресурсами, і спосіб та засоби збору, обробки та передавання інформації для набуття нових відомостей про об'єкт, що вивчається".

Зазвичай використовують типізацію засобів ІКТ за технічними ознаками – *програмні та апаратні.*

В. Трайнев до складу ІКТ відносить сукупність методів та програмно- технічних засобів, що об'єднанні в технологічний ланцюг, який забезпечує збір, обробку, збереження та відображення інформації з метою зниження трудомісткості її використання, а також для підвищення її надійності й оперативності.

При розробці та використанні ІКТ використовують поняття *інформаційний ресурс.* Вказані ресурси - це особливий вид ресурсу, який будується на ідеях і знаннях,

накопичених в результаті науково-технологічної діяльності людей, зокрема аналітичної, у деякій предметній галузі, та поданий у формі, придатній для накопичення, реалізації і відтворення.

Розвиток ІКТ часто розглядають у контексті та як складову *інформатизації суспільства.*

Під інформатизацією суспільства розуміють глобальний соціальний процес. Його особливість полягає в тому, що домінуючим видом діяльності в сфері суспільного виробництва є збирання, нагромадження, продукування, оброблення, зберігання, передавання та використання інформації. Ці процеси здійснюються на основі сучасних засобів процесорної та обчислювальної техніки, а також на базі різноманітних засобів інформаційного обміну.

Сьогодні належна інформатизація суспільства забезпечує, зокрема:

активне використання інтелектуального потенціалу, що постійно розширюється, сконцентрованого в друкованому фонді, науковому, виробничому та іншому видах діяльності його членів;

інтеграцію інформаційних технологій з науковим, виробничим, ініціюючим розвитком усіх сфер суспільного виробництва, інтелектуалізацію трудової діяльності;

високий рівень інформаційного обслуговування, доступність будь якого члена суспільства до джерел достовірної інформації, візуалізацію представленої інформації, правдивість використаних даних.

Інформатизація суспільства пов’язана з розвитком комп’ютерної техніки, програмного забезпечення, Інтернету, мультимедійних технологій.

Тобто глобальне впровадження комп'ютерних ІКТ у всі сфери діяльності, формування нових комунікацій стало першим кроком до формування інформаційного суспільства.

Проблема інформатизації суспільства часто розглядається як технологічна. І дійсно, її матеріальною основою служить глобальний перехід до безпаперової інформатики, коли основна маса даних, циркулюючих в суспільстві, зберігатиметься і оброблятиметься в комп’ютерних системах і передаватиметься

по автоматизованих каналах супутникового або телекабельного зв'язку, сполучає окремі комп'ютери і автоматизовані робочі місця в інформаційні мережі, забезпечуючи звернення до баз даних, знаходиться практично у будь-який точці земної кулі.

У основі цього підходу лежить ряд фундаментальних винаходів і відкриттів: персональні комп'ютери, оптичні диски на десятки і сотні гігабайт, що дозволяють в компактному виді зберігати вміст цілих бібліотек, оптико-волоконні канали зв'язку, відеотекстові системи зв'язку, методи представлення даних і знань.

Уся ця техніка забезпечує можливість створення в недалекому майбутньому високоавтоматизованого інформаційного середовища, що дозволяє отримати доступ до будь-якого знання, наданого у вигляді інформації. Фактично це означає, що інформаційне середовище дає глобальне рішення проблеми доступу до знання, отриманого у будь-який момент часу у будь-якому місці. Вже з цього виходить, що проблема інформатизації є не чисто технічною, але значною мірою соціокультурною.

Радикально міняється і далі мінятиметься потік інформації. Якісно трансформується мислення, свідомість, діяльність, міжособові і групові стосунки, що формуються в умовах інформаційного насиченого середовища.

Покоління, що зростає в тісному спілкуванні з комп'ютерами, електронними іграми, мобільним зв'язком, відрізняється по світогляду в психологічному, моральному і духовному плані. Мова йде не лише про навички володіння обчислювальною технікою, але і про зміни фундаментальних духовно-культурних структур, понять і представлень. Інакше організовується свій зовнішній світ, розвиваються інтелектуальні здібності не просто швидше і різнобічніше, але і в іншому соціально-тимчасовому вимірі.

Але треба відмітити наступне: сучасні технології приносять у світ постійно зростаючі об'єми інформації, а багато інтелектуальних досягнень від інформації практично не залежать. Тут, знову ж таки, виникає проблема співвідношення інформації і знання.

Розвиток автоматизованого інформаційного середовища призводить до радикальних змін в соціально-економічній структурі суспільства. Дозволяє під іншим ракурсом досліджувати безпекові характеристики (параметри) на функціонування та розвитку соціальних систем. Передусім динаміку кризових ситуацій, які постійно виникають у цих системах та її елементах (політичній, економічній та інших). Тому інформаційні технології сьогодні займають центральне місце в оновленні (трансформації) безпекової складової усіх сфер та видів діяльності індивида (людини), суспільства та інститутів держави.

Таким чином, виникнення та розвиток інформаційного суспільств передбачає широке застосування ІКТ у різних сферах суспільного життя,

5.3. Компоненти створення та функціонування ІКТ та виклики, які є наслідком їх розвитку

Компоненти створення та функціонування ІКТ. Фахівці, зокрема, А. Зубов виокремлюють такі компоненти створення та функціонування ІКТ:

теоретичні засади створення та функціонування ІКТ;

методи вирішення завдань, які використовують в ІКТ;

засоби вирішення завдань в ІКТ.

Теоретичні засади створення та функціонування ІКТ складаються із найважливіших понять й законів інформатики, а саме:

об’єкта та предмета інформатики;

поняття інформації, її властивостей та особливостей, до яких відносять цінність, повноту, актуальність, компактність, достовірність та логічність;

різноманітні класифікації інформації;

основні інформаційні процеси, типи інформаційних ресурсів, види інформаційної діяльності;

принципи функціонування комп’ютерної техніки, алгоритми інформаційного моделювання, використання ІКТ.

Методи вирішення завдань, які використовують в ІКТ включають методи моделювання, системний аналіз, системне

проектування, методи передачі, збору, продукування, накопичення, збереження, обробки, передачі та захисту інформації.

Засоби вирішення завдань в ІКТ поділяють на:

апаратні: персональний комп'ютер і його основні складові, локальні та глобальні мережі, сучасне периферійне обладнання;

програмні: системні, прикладні, інструментальні.

Можливості та проблеми (виклики), які є наслідком розвитку ІКТ. Головним чинником, що визначає важливість і доцільність вдосконалення ІКТ є потреба відповісти на основні виклики людству у XXI столітті:

необхідність переходу суспільства до нової стратегії розвитку на основі знань і високоефективних інформаційно-комунікаційних технологій;

фундаментальна залежність цивілізації від здібностей і якостей особистості, що формуються освітою;

можливість успішного розвитку суспільства на засадах ефективного використання ІКТ;

щонайтісніший зв'язок між рівнем добробуту нації, національною безпекою і застосуванням ІКТ.

В цілому ІКТ мають значний вплив на суспільство, який стає все більш помітним. Деякі з головних аспектів впливу ІКТ на суспільство стосуються створення небачених раніше можливостей, зокрема:

у зміні способу життя людей, змінюючи їх підходи до різних аспектів життя (наприклад, деякі люди віддають перевагу дистанційній роботі, що дозволяє їм працювати з будь-якої точки світу, тобто територіально вони не так привязані з державою, а інші можуть використовувати ІКТ для здійснення покупок онлайн або для постійного зв'язку з рідними та друзями, які знаходяться в інших країнах;

у бізнесі (наприклад, використання електронних таблиць може спростити процес обліку фінансів та збільшити точність цих даних, а використання електронної пошти та месенджерів може спростити комунікацію між співробітниками та партнерами);

в освіті (наприклад, використання онлайн-курсів може допомогти студентам отримати доступ до матеріалів з будь-якого місця та у будь-який час, електронних дошок та інших ІКТ може допомогти педагогам створювати більш динамічні та інтерактивні навчальні заняття);

у сфері розваг (наприклад, використання стрімінгових платформ для перегляду відео дозволяє людям отримувати доступ до більш широкого вибору контенту та дозволяє їм переглядати його у зручний для них час).

Водночас розвиток ІКТ породжує низку проблем для людини (індивіда) та функціонування соціальних систем, наслідки яких поки що важко оцінити. Серед вказаних проблем зокрема, наступні.

1. Проблеми безпекового хараактеру. Вони є одним із найбільших недоліків використання ІКТ. Сьогодні все більше людей та різних організацій користується ІКТ для збору, обробки, зберігання та передачі інформації. Доситьчасто вона має виключно конфіденційний характер. Водночас хакерські атаки, віруси та інші загрози можуть призвести до втрати даних та інших серйозних наслідків стратегічного характеру для безпеки життєдільності соціальних систем, у тому числі структур сектору безпекита оборони

2. Проблеми пов'язані зі здоров'ям людей. Все більше з'являється досліджень, які свідчать, що ІКТ можуть досить негативно впливати на здоров'я людей. Наприклад, довгі години, проведені за комп'ютером, можуть призвести до значних проблем зі здоров'ям спини та очей. Крім того, надмірне використання соціальних мереж та інших ІКТ може призвести до погіршення психічного здоров'я та соціальної ізоляції.

3. Поглиблення соціальної нерівності та соціальної відокремленості Використання ІКТ в цілому сьогодні призводять до нерівності в доступі до життєво важливої інформації та можливостей, а відтак і до поглиблення соціальної нерівності, яка набуває глобального характеру. Наприклад, люди з низьким рівнем доходу або з віддалених регіонів в окремих державах можуть мати обмежений доступ до ІКТ та відповідних можливостей, а держави з низьким рівнем розвитку

ІКТ будуть все більше відставати від країн у яких уже закладені підвалини постіндустріального (інформаціного) суспільства,тобто у яких домінує так звана «економіка знань», яка грунтується саме на сучасних інформаціних технологіях. Це призводить до поглиблення нерівності та соціальної відокремленості як окремих людей та соціальних груп, так і цілих регіонів.

Таким чином, незважаючи на те, що роль ІКТ у житті людей постійно зростає, оскільки вони роблять більш насиченими соціальні взаємодії та дозволяють отримувати доступ до різноманітної інформації, водночас зростають ризики для безпеки людини та соціальних інститутів, зокрема повязані з кібербезпекою та конфіденційністю даних. Тому важливо розуміти, як використовувати ІКТ ефективно та безпечно, щоб максимально скористатися їх можливостями, тобто дотримуватися певних правил кібербезпеки.

5.4. Класифікація новітніх ІКТ у контексті забезпечення безпеки та стандарти їх розвитку

Класифікація новітніх ІКТ у контексті забезпечення безпеки. У тій чи іншій мірі можна говорити про існування ІКТ, починаючи із Стародавнього світу, на кожному етапі людського існування. Але, якщо раніше ІКТ виконували допоміжну функцію, наприклад, виступали інструментом в електоральних кампаніях, пропаганді чи державному управлінні, то в сучасних умовах вони проникають у всі сфери суспільного життя. Це призводить до виникнення комунікативних стратегій інформаційного суспільства та, відповідно, інформаційно-комунікативних систем.

Говорячи про новітні ІКТ, варто зауважити час їхнього виникнення та використання. Тобто, мається на увазі сучасність, а точніше – цифрова епоха. Тобто конкретний набір ІКТ зумовлюється певною інформаційно-комунікаційною системою Тому «новітність» є виключно характеристикою часу.

Отже, новітня ІКТ – це притаманний цифровій епосі спосіб практичного використання знання, спрямований на досягнення конкретної мети.

Щодо класифікації новітніх ІКТ, то за логікою має бути прив'язка до цифрової епохи. Тобто, мається на увазі, що та чи інша ІКТ, щоб бути зарахованою до новітніх, повинна виникнути саме в окреслений період. Однак це не зовсім так. Може йти мова і про трансформацію ІКТ технологій попередніх періодів.

Наприклад, український дослідник Г. Почепцов у цілій низці публікацій розглядає пропаганду та її прояви як різновид новітньої ІКТ. Так, у її межах, вчений виокремлює наступні технології управління інформаційним полем:

руйнування інформаційного монополізму, перерозподіл інформаційної ваги гравців (у цьому випадку коректніше говорити «суб'єктів інформаційно-комунікативної системи»);

створення керованих масових єдностей;

керування сприйняттям;

управління героїкою;

управління ворогами;

маніпуляція з джерелом;

управління парадоксальністю;

управління рамками;

управління каналом комунікації;

управління розважальністю;

управління сакральністю;

управління історією;

управління за допомогою великих масивів інформації.

У цьому контексті одразу вбачається негативна спрямованість кожної з вище названих технологій пропаганди, оскільки кожна з них передбачає використання проти ворога. Але це лише одна сторона ІКТ.

До того ж, пропаганда не завжди має негативний контекст.

Слід розуміти, що поставлена мета не завжди матиме деструктивний або конструктивний характер. Наприклад, застосування тієї чи іншої ІКТ зумовлюється наявною ситуацією й може виконувати роль підтримки.

Повертаючись до наведеного поділу, варто зробити висновок, що загалом згадані Г. Почепцовим технології можна звести до наступних трьох груп:

спрямовані на зміну суб'єктів та/або їхнього сприйняття і способів взаємодії;

спрямовані на зміну засобів комунікації;

спрямовані на зміну інформаційного поля (простору).

Говорячи про останню групу, яка, за великим рахунком, повинна бути найскладнішою у своїй реалізації, варто навести аксіоми управління інформаційним простором.

Г. Почепцов виокремлює наступні:

аксіома об'єму – існують нескінченні можливості розширення і наповнення інформаційного простору новим змістом;

аксіома доступу – інформаційний простір вільний, його обмеження потребує залучення додаткових засобів; -

аксіома управління – увага може приділятися лише конкретному сегменту інформаційного простору;

аксіома неоднорідності – елементи інформаційного простору відрізняються один від одного;

аксіома взаємозалежності – сегменти інформаційного простору перебувають у різних зв'язках між собою.

Перелік не є повним, але він дозволяє коректно класифікувати новітні ІКТ. Отже новітні ІКТ можна класифікувати за спрямованістю.

Відповідно, маємо:

технології зміни засобів комунікації;

технології зміни суб'єктів комунікації та/або їхнього сприйняття;

технології зміни інформаційного поля (простору) – причому варто уточнити, що тут слід вести мову лише про окремі сегменти.

Це дозволяє говорити про чітку спеціалізацію новітніх ІКТ.

Далі новітні ІКТ слід класифікувати за цілями, які прагне реалізувати суб'єкт використання.

Отже, можна виокремити:

технології підтримки (нейтральний підхід) – йдеться про забезпечення статус-кво у конкретному політичному процесі;

технології забезпечення домінування (деструктивний підхід) – мається на увазі отримання перемоги над ворогом, його

деморалізація і т. д. У такому контексті говорять про гібридні, психологічні, інформаційні війни, де, безумовно, мають місце ІКТ;

технології забезпечення порядку (конструктивний підхід) – така назва є доволі широкою, – основними ознаками яких є збереження стабільності власних позицій у процесі комунікації або ліквідація наслідків негативного впливу супротивника.

Отже, як висновок, слід зазначити, що ці дві класифікації найбільш загально окреслюють сутність новітніх. Від тих, що належать до попереднього періоду, їх відрізняє значно ширший спектр діяльності, можливість використання тих чи інших ресурсів та характер мети, покладеної в її застосування.

Якщо, наприклад, у Новий час ІКТ могли послуговуватися виключно в негативному контексті (дискредитація та деморалізація ворога), а також вони асоціювалися переважно з військовою сферою, то в Новітню епоху спектр їхньої дії значно розширюється. Те ж стосується доступних засобів для їхнього використання.

Стандарти у сфері розвитку ІКТ. Стандарти є дуже важливими для ІКТ, оскільки вони визначають зрозумілу мову технологій. Це особливо актуально, оскільки ключовою ідеєю ІКТ є те, що пристрої зберігання інформації можуть безпроблемно комунікувати через медіа спосіб з мережами зв'язку та обчислювальними системами.

Відкриті стандарти та стандарти організацій, такі як Асоціація телекомунікаційної промисловості в Сполучених Штатах і ETSI в Європі відіграють особливу роль.

Основними організаціями, які розробляють та сприяють впровадженню стандартів в галузі комп'ютерних мереж є:

Міжнародний телекомунікаційний союз (МТС) (ITU — International Telecommunication Union).

Стандарти МТС поділяються на серії. Стандарти кожної серії присвячені одній тематиці й позначаються великою літерою латинського алфавіту. Після літери ставиться крапка і номер стандарту.

Наприклад, літерою V позначаються стандарти щодо передавання даних телефонними каналами, літерою X —

стандарти щодо мереж передавання даних, літерою Q — стандарти щодо телефонної комутації та сигналізації.

Технічний комітет 97 — комітет міжнародної організації зі стандартизації (ISO — International Organization for Standardization). Технічний комітет розробляє стандарти щодо опрацювання інформації за допомогою ЕОМ.

Стандарти цієї організації позначаються чотиризначним числом та суфіксом ISO. Наприклад, стандарт, який стосується протокольного стека TCP/IP має позначення 7498 ISO.

Комісія з питань діяльності Internet (IAB — Internet Activities Board) розробляє стандарти щодо діяльності Internet

Дотримання стандартів, які розроблені цими організаціями, обов'язкове під час проєктування, створення та експлуатації будь-яких комп'ютерних мереж.

Основним нині діючим проектним документом з розвитку інформаційної сфери ЄС є ініціатива Європейської Комісії «Цифровий порядок денний для Європи» («Digital Agenda for Europe»), ухвалена в рамках прийнятої Європейською Радою навесні 2010 р. стратегії «Europe 2020».

Ініціатива спрямована на досягнення двоєдиної мети: забезпечення глобальної конкурентоспроможності ЄС через розвиток та імплементацію ІКТ, а також вихід на новий рівень використання цифрових технологій в усіх сферах і прошарках європейського соціуму.

Для стратегічного проектування і планування інформаційної сфери в керівних органах ЄС характерні такі риси:

тісна взаємопов’язаність і чітка ієрархічність проектних документів, принцип поетапної спеціалізації цілей та завдань (багато локальних автономних стратегій в одній великій);

широке застосування програмно-цільового методу, максимальна конкретизація завдань, термінів їх виконання, там де це можливо – визначення відповідального суб’єкта;

оперативне та адекватне реагування на зміну ситуації, здатність швидко внести необхідні корективи у вже затверджені плани та стратегії;

опора на постійний моніторинг ситуації та стратегічні комунікації, потужне експертно-аналітичне супроводження нормопроектної діяльності.

Як і у випадку з іншими колективними документами, межі та механізми кореляції «Цифрового порядку денного для Європи» з національними законодавствами і проектами країн-членів ЄС ґрунтується на acquis communautaire Союзу й усталених правових практиках.

Зазвичай загальноєвропейські стратегії формуються з урахуванням інтересів та особливостей всіх держав-членів ЄС. Зобов'язання національних урядів щодо їх виконання зводяться до необхідності дотримання стандартів, приписів та рішень, що поширюються на весь ЄС.

5.5. Проблема захисту ІКТ від кіберзагроз та проблемні питання їх розвитку в Україні

Характеристика проблеми захисту ІКТ від кіберзагроз. Створення безпечного *кіберпростору* є одним із напрямів інформаційної політики. В Окінавській хартії глобального інформаційного суспільства, прийнятій лідерами країн вісімки у японському м. Окінава у 2000 р., кіберпростір розглядається як частина глобального інформаційного простору, пов'язана з комп'ютерною інфраструктурою, насамперед з Інтернетом.

Д. Дубов характеризує кіберпростір як середовище, створене організованою сукупністю інформаційних процесів на підставі об'єднаних загальними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем незалежно від форми власності.

Кіберпростір держави перебуває під різноманітними кіберзагрозами, серед яких вплив на:

стан електронних інформаційних ресурсів та на можливість доступу до інформації;

функціонування об'єктів критичної інфраструктури;

складові частини інформаційно-комунікаційної інфраструктури;

морально-психологічний стан суб'єктів кіберпростору.

Тож поняття кібербезпека позначає стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та / або телекомунікаційних мереж, за якого мінімізується можливість завдати їм шкоди. Вказана шкода може бути через:

неповноту, невчасність та невірогідність інформації, що використовується;

негативний інформаційний вплив;

негативні наслідки функціонування інформаційних технологій;

несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації.

Останнє стосується не лише технічних питань і технологічного складника, а й людського чинника – ворожих інсайдерських дій чи людський помилок, а також проблем владних відносин на національному та міжнародному рівнях.

Можливість країни впливати на кіберпростір характеризують поняттям *кіберпотужність.* Вона, зокрема залежить від: можливості інтернету та інформаційних технологій, можливості інтернет-ринку та ІТ-індустрії. Використовується й термін *кіберсила,* під якою розуміється потужність, що залежить від інформаційних ресурсів, які характеризують кіберпростір. Кіберсила країни вимірюється через такі параметри: рівень залежності від інформаційних атак та захисту в кіберпросторі.

Подію, яка може порушити кібербезпеку (конфіденційність, цілісність та доступність інформації у кіберпросторі), називають *кіберінцидентом.*

Кіберзагрози охоплюють різноманітні впливи агресора, яким можуть бути окремі держави, групи та особи, на різні сфери життєдіяльності суспільства та держави: економічну, політичну, науково-технічну, оборонно-промисловий і транспортний комплекси, інфраструктуру електронних комунікацій, управління у сфері національної безпеки та інші.

Кіберзлочинність не обмежується збиранням, зберігання, використанням, знищенням, поширенням персональних даних, незаконними фінансовими операціями, крадіжками та шахрайствами в мережі Інтернет. Вона сьогодні є глобальною

транснаціональною проблемою. При цьому *кібератака* розглядається як сукупність дій противника або ворожої групи, яка намагається досягти певної негативної для об'єкта атаки цілі чи ефекту з використанням комп'ютерної техніки зокрема чи можливостей кіберпростору в цілому, найчастіше – з використанням спеціально розроблених для таких завдань засобів.

Сукупність кібератак, що перевищують за своїм загальним негативним впливом певне порогове значення, можуть розглядатися як початок *кібервійни*. Вказані атаки можуть здійснюватися дилетантами, хакерами, інсайдерами з метою особистого збагачення чи вигоди, а також спонсоруватися державою з метою шпигунства чи в умовах ведення інформаційної війни.

М. Каветлі пропонує таку *типологію кіберконфліктів*:

кібервандалізм (включає зміни чи знищення змісту, наприклад, веб-сайту, вимкнення чи перевантаження сервера, є найпоширенішою формою кіберконфлікту, що має значний суспільний резонанс, однак наслідки таких інцидентів обмежені в часі та відносно незначні);

інтернет-злочини (діяльність переважно з метою отримання прямого фінансового зиску, може включати як злочини з комп'ютерної техніки, так і суто комп'ютерні злочини);

кібершпигунство (головною жертвою найчастіше стає корпоративний сектор. За окремими підрахунками, втрати компаній від такої діяльності перевищують 1 трлн доларів США на рік. Останнім часом частішають атаки і на Урядові мережі, в яких міститься конфіденційна інформація;

кібертероризм (потенційно масштаби збитків від кібертеракту оцінюються надзвичайно високо);

кібервійна.

Інформаційні ресурси різних країн все частіше стають стають об'єктами кібератак. Починаючи з 2014 року, кіберзагрози займають 1-2 місця серед потенційних загроз,

Загрози кібербезпеці актуалізуються через дію таких чинників:

невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;

недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;

безсистемність заходів кіберзахисту критичної інформаційної інфраструктури;

недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів;

недостатня ефективність суб'єктів сектору безпеки і оборони у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;

недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

Пріоритети України в сфері кібербезпеки. Серед пріоритетів України в сфері кібербезпеки, зокрема:

розвиток інформаційної інфраструктури держави;

розвиток мережі реагування на комп'ютерні надзвичайні події;

розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів;

забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак;

створення системи підготовки кадрів у сфері кібербезпеки
для потреб органів сектору безпеки і оборони;

розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, для посилення спроможностей України у сфері кібербезпеки.

З огляду на викладене, розвиток безпечного, стабільного і надійного національного кіберпростору має полягати, зокрема, у таких діях:

вироблення і оперативна адаптація державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягненні сумісності з відповідними стандартами ЄС та НАТО;

створення вітчизняної нормативно-правової та термінологічної баз у цій сфері, гармонізація нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО;

формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту;

розвиток технологій кіберзахисту засобів рухомого зв'язку, забезпечення апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку;

підвищення цифрової грамотності громадян та культури безпекової поведінки в кіберпросторі, набуття комплексних знань, навичок і здібностей, необхідних для підтримки кібербезпеки, впровадження державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, підтримка міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, поглиблення співпраці України з ЄС та НАТО для посилення спроможностей України у сфері кібербезпеки, участь у заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідою ОБСЄ.

З огляду на викладене принципово важливим питанням є формування ефективної національної системи кібербезпеки. Вона має забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та / або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури.

Проблемні питання розвитку ІКТ в Україні. В цілому, незважаючи на наявність значного потенціалу щодо впровадження сучасних ІКТ в усі сфери життєдіяльності країни, вагомого суспільного запиту на таке впровадження, стан розбудови інформаційного суспільства та сфери ІКТ в Україні порівняно із світовими тенденціями є недостатнім і не відповідає стратегічним цілям розвитку України. Йдеться, зокрема про наступне.

1. Існують суттєві проблеми з формуванням та реалізацією ефективної державної політики, зокрема щодо розвитку інформаційного суспільства та подолання цифрової нерівність у доступі громадян України до електронних комунікацій та інформаційних ресурсів, через що повільно зростає рівень комп'ютерної грамотності населення;

2. Недостатній рівень впровадження та використання можливостей ІКТ у сферах освіти, науки, культури, охорони здоров'я, в агропромисловому комплексі та інших секторах економіки.

3. Організацію здійснення громадського контролю на засадах широкого використання ІКТ та мережі Інтернет.

4. Створення належних умов для ведення ІКТ-бізнесу, зокрема недостатньо врегульовані відносини для забезпечення економічної конкуренції на ринках деяких телекомунікаційних послуг та відсутні ефективні механізми нагляду у сфері телекомунікацій, спрямовані на запобігання порушенням та зниження потенційно можливого тиску на суб'єкти господарювання, зменшення кількості перевірок таких суб'єктів.

5. Реалізації сучасних завдань безпеки та оборони держави з широким залученням підприємств ІКТ-галузі, наукових установ, закладів освіти та громадських організацій, що забезпечують впровадження новітніх ІКТ, зокрема інформаційної безпеки та кібербезпеки;

6. Визнання на державному рівні міжнародних сертифікатів у сфері управління інформаційною безпекою, кібербезпекою та інформаційними технологіями;

7. Унеможливлення зловживань та дотримання прав людини при перехопленні інформації силовими структурами;

8. Розбудову сучасної нормативно-правової бази реформування ІКТ-галузі та розвитку інформаційного простору, багато положень якої не відповідають вимогам сьогодення та потребують удосконалення;

9. Забезпечення прискорення гармонізації національного законодавства з нормами законодавства ЄС, зокрема з питань інформаційного суспільства, надання електронних послуг, розвитку телекомунікацій, захисту інтелектуальної власності тощо;

10. Відсутність єдиного центрального органу виконавчої влади, відповідального за формування та/або реалізацію державної політики розвитку інформаційного суспільства, сфери телекомунікацій, програмування, забезпечення інформаційної безпеки та кібербезпеки, впровадження технологій електронного урядування, електронного документообігу, електронного підпису, що зумовлює:

невизначеність та відсутність єдиної державної політики у цих сферах;

недостатній рівень координації діяльності органів державної влади та органів місцевого самоврядування у сфері ІКТ та зв'язку;

незабезпечення взаємосумісності різних інформаційних систем, що створювалися в різний час, за різними принципами, на різних технологічних платформах;

11. Відсутність передбачених на законодавчому рівні дієвих механізмів захисту прав споживачів телекомунікаційних послуг у разі припинення діяльності операторів, провайдерів телекомунікацій.

Таким чином першочерговими для України сьогодні залишається оптимізація досліджень і розробок в ІТ-сфері, підготовка ІТ-кадрів, створення привабливих умов для інвестицій і розвиток державно-приватного партнерства.

Необхідним є також глибоке оновлення нормативно-правового і проектного забезпечення розвитку інформаційного суспільства. Доцільним є запровадження конвергентної моделі управління інформаційною сферою з визначенням єдиного державного органу в межах компетенції та відповідальності якого заходиться весь комплекс питань, пов'язаних з розвитком ІКТ.

ГЛАВА 6. КРИЗОВІ СИТУАЦІЇ У СОЦІАЛЬНИХ СИСТЕМАХ

6.1. Співвідношення кризових та надзвичайних ситуацій та світоглядний аспект природи кризових ситуацій соціального характеру

Проблема з'ясування співвідношення кризових та надзвичайних ситуацій. Той чи інший нестабільний стан (кризова ситуація) є невід'ємним атрибутом соціальної системи і породжує певні виклики та загрози її функціонуванню. Кризові ситуації операціоналізуються через поняття «протиріччя» в основі яких зміна якісно-кількісних характеристик буття соціальної системи у руслі формування нової соціальної реальності.

Кризові ситуації соціального характеру розвиваються у часі та просторі, що дозволяє виділити їх певні стадії, у тому числі ті, на яких можуть виникнути надзвичайні ситуації. Їх характерною особливістю є те, що управління в таких ситуаціях не тотожне кризовому управлінню, оскільки, не кожна криза пов'язана із загрозами фізичній безпеці громадян чи втрати матеріальних ресурсів.

Наслідки надзвичайних ситуацій завжди негативні, на відміну від кризових ситуацій, із амбівалентності властивостей яких ці наслідки можуть бути, як негативні, так і позитивні, незважаючи на те, що між кризовими та надзвичайними ситуації існує прямий і зворотній зв'язок.

Аналіз наукового доробку та законодавства дозволив дійти висновку, що кризова ситуація, критична ситуація, криза, надзвичайна ситуація, є визначальними властивостями вказаних систем та наслідком дії взаємопов'язаних факторів через що деякі поняття вживаються як синоніми. Це свідчить про необхідність більш чіткого з'ясування співвідношення. понять «кризова ситуація», «критична ситуація», «криза», «надзвичайна ситуація».

Як відомо, рух об'єктів матеріального світу в часі і просторі лежать в основі їх розвитку, є внутрішньою необхідністю їх існування. Вона зумовлена перманентною

потребою у якісно-кількісній зміні змісту й форми вказаних об'єктів. Тому в соціальних системах нестабільний стан, який прийнято називати кризовою ситуацією потребує адекватного реагування з боку суб'єктів управління у сфері національної безпеки. Інакше ці ситуації можуть трансформуватися у надзвичайні ситуації і, як наслідок, введення надзвичайного чи воєнного стану.

Водночас сьогодні лише незначна кількість фахівців досліджують управлінські аспекти сутності кризових ситуацій соціального характеру та їх трансформації у відповідні надзвичайні ситуації.

Законодавство України виокремлює вказані ситуації як окремий вид. Це мало б активізувати науковий дискурс, розкриття взаємозумовленості кризових та надзвичайних ситуацій у контексті управління у сфері національної безпеки. Проте, варто зауважити, що під поняттями кризові ситуації часто розуміють не тільки все, що виходить за межі нормальних (безпекових) умов життєдіяльності суспільства та держави, а й ототожнюють їх, наприклад, з кризами, катастрофами, критичними ситуаціями. Це породжує невизначеність при інформаційно-аналітичному супроводженні розробки, прийняття та реалізації управлінських рішень у сфері національної безпеки.

На цей час проблематиці забезпечення ефективності управління в кризових ситуаціях присвячено значний обсяг наукової літератури. Для сучасного періоду дослідження цього явища характерним є намагання створити деяку інтегральну концепцію кризового управління, а наявні його стратегії передбачають, що можна виділити певні стадії й визначити відповідні управлінські завдання щодо її врегулювання.

Водночас науковці традиційно акцентують увагу на надзвичайних ситуаціях, які виникають через аварії, катастрофи, стихійні лиха тощо, а роботи, в яких досліджуються кризові ситуації, які спричинені соціальними явищами в соціальній системі (масовими заворушеннями, реформами, політичною дестабілізацією тощо), майже відсутні.

Як ми зазначали, кризові ситуації є визначальною властивістю соціальної системи і є наслідком дії багатьох

взаємопов'язаних зовнішніх та внутрішніх факторів. Це породжує термінологічну плутанину з близькими за значенням термінами, такими, зокрема, як "соціальна криза", "критична ситуація", "надзвичайна ситуація", які широко використовують у науковому дискурсі та нормативно-правових актах.

Виконаний аналіз дозволяє дійти висновку, що ці поняття часто не розмежовують, вживають як синоніми, ототожнюють, тому важливим є розкриття взаємозумовленості кризових та надзвичайних ситуацій у контексті управління у сфері національної безпеки.

Таким чином, принципово важливим для фахівців-управлінців у сфері національної безпеки є розуміння динаміки розвитку кризових ситуацій і на цій основі співвідношення з іншими близькими до нього поняттями, передусім поняттям "надзвичайні ситуації" та, відповідно, їх інформаційного змісту.

Світоглядний аспект природи кризових ситуацій соціального характеру. Розвиток соціальної системи зумовлений впливом зовнішніх і внутрішніх факторів, які генерують у ній стан нестійкості. Він руйнує процеси її функціонування, але водночас створює й необхідні умови для більш стійкого та якісного їх здійснення у майбутньому.

При цьому існує дві взаємопов'язані, але протилежні тенденції, які є основою буття (існування) будь-якої соціальної системи:

стійкість, яка забезпечує збереження набутих системою якісних характеристик

мінливість характеристик системи, як результат реагування на вказані фактори.

Ці тенденції зумовлюють наявність двох взаємозумовлених етапів (стадій) буття соціальної системи, які змінюють один одного: *стабільний стан* й *кризові ситуації* в межах яких відбуваються кризи, як переламні моменти у функціонуванні системи.

Розвиток кризових ситуацій генерує ті чи інші небезпеки для соціальної системи. Вони заперечують в той чи інший період буття системи її природну визначеність, незважаючи на те, що ці ситуації є невід'ємною властивістю систем.

Можливість заперечення визначеності (сутності) системи згідно діалектичному закону "заперечення-заперечення" міститься у самій системі, що зумовлено єдністю її сталості й змінності, спрямованістю й формами її розвитку.

Принципово важливим є й те, що якісно-кількісні характеристики тих чи інших соціальних явищ, які є небезпеками для соціальної системи, завжди мають об'єктивно-суб'єктивну природу. Тому завжди існує ймовірність неадекватної оцінки безпеки соціальної системи, коли вона починає діяти виходячи з власних уявлень про небезпеку.

Таким чином, відмінною особливістю кризових ситуацій в соціальних системах, є наявність певного потенціалу небезпеки для людини (індивіду) суспільства та державних інститутів. Тому важливими питаннями є з'ясування змісту, форми, причин й динаміки (стадій) кризових ситуацій, як передумови ефективного управління в цих ситуаціях, особливо коли ці ситуації спонукають до введення надзвичайного або воєнного стану. Очевидно, що вирішення цього питання потребує ґрунтовної та оперативної оцінки значних масивів інформації, яка циркулює в інформаційно-комунікативних (інформаційних) системах і стосується життєдіяльності тієї чи іншої соціальної системи.

Таким чином створення передумов ефективного управління у кризових ситуаціях зумовлює необхідність більш детального розкриття взаємозумовленості соціальних криз, кризових та надзвичайних ситуацій та підстав для введення надзвичайного та воєнного стану.

6.2. Нормативно-правове трактування кризових ситуацій та поняття "криза", як вимір буття соціальної системи

Нормативно-правове трактування сутності кризових ситуацій. Згідно ст. 3. Закону України "Про Раду національної безпеки і оборони України" до її функцій належить "координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в умовах воєнного або надзвичайного стану та при виникненні

кризових ситуацій, що загрожують національній безпеці України". Водночас згідно примітки до ст. 4. закону "кризовою ситуацією вважається крайнє загострення протиріч, гостра дестабілізація становища в будь-якій сфері діяльності, регіоні, країні".

Таким чином, у даному випадку кризова ситуація передбачає крайнє загострення протиріч, а умови, тобто перебіг подій за такої ситуації, вирізняються від умов коли вводиться воєнний або надзвичайний стан. При цьому зміст поняття "кризова ситуація" операціоналізується через поняття "протиріччя".

З іншого боку, ті чи інші протиріччя, які виникають у соціальній системі призводять до конфлікту, під яким розуміється зіткнення інтересів, мотивів, тенденцій, суб'єктів суспільного життя. Тому природа вказаних конфліктів соціальна, а їх сутність та динаміка зумовлена соціальними взаємодіями.

Як зазначає А.Дондюк "елементи системи знаходяться в конфлікті з іншими за умови, що "відкрите виявлення" інтересів, мотивів, цілей одних елементів активізує дії протилежних інтересів, мотивів системи, його зародження можливе, коли в її межах на одному рівні знаходяться неідентичні в своїх виявах елементи, а сама динаміка конфлікту відбувається або в напрямі до утиску одного з його суб'єктів, або поступової саморуйнації системи або ж повільного його "згасання", що створює ситуацію взаємодоповнюваності тенденцій, інтересів тощо".

Очевидно, що вказані конфлікти можуть виникати у різних сферах суспільного життя, тобто є різні види таких конфліктів. Так, розповсюдженими є політичні конфлікти, "як відкрите суперництво, протистояння, протиборство суспільних суб'єктів з приводу відносин політичної влади і політичного управління в ситуації кризового загострення протиріччя чи протиріч відносин цих суб'єктів, а його виявами є насильство: спроба примусу або завдання шкоди, що відбувається всупереч інтересам і волі сторони або сторін, проти якої або яких вони спрямовані".

З огляду на викладене доцільним є аналіз трактування змісту "кризова ситуація" наведеного в п. 4 Державного стандарту, де вона визначається як "ситуація, в якій з'являється набір травматичних подій, обставин, з яких людина не може вийти, не змінивши їх. Кількість можливих варіантів змінювати ці обставини незначна, будь-яка спроба змін обставин традиційними чи звичайними способами може призвести до погіршення ситуації, до зменшення можливостей та ще більшого обмеження дій".

Аналіз наведеного змісту кризової ситуації дозволяє дійти висновку, що у даному випадку вона ототожнюється з критичною ситуацією, оскільки йдеться про обставини, які створюють загрозу задоволення фундаментальних потреб людини і водночас проблему, якої вона не може уникнути (не може вирішити) в короткий час звичним способом.

Існують чотири категорії, які використовують при інтерпретації змісту поняття "критична ситуація": стрес, фрустрація, конфлікт, криза. Водночас, на думку Ф.Василюка, дослідники будь-яку критичну ситуацію підводять під улюблену категорію, що призводить до термінологічної плутанини при трактуванні змісту цього поняття, особливо з огляду на те, що й стосовно розуміння цих категорій у них відсутня методологічна визначеність, наприклад, в змісті поняття "стрес" уживаються абсолютно різнорідні явища: реакція на холод, радість успіху, приниження тощо.

В кінцевому підсумку він також доходить висновку, з яким важко не погодитися, що кожному з понять, що фіксують ідею критичної ситуації, відповідає своє категоріальне поле, яке відображає особливий вимір життєдіяльності людини, що володіє власними закономірностями та характерними для неї умовами життєдіяльності, типом активності і специфічною внутрішньою необхідністю, що має враховуватися при його використанні.

Поняття "криза", як особливий вимір характеристик буття соціальної системи. З огляду на викладене вище важливим є окреслення не тільки змісту поняття "конфлікт", а й поняття "криза", як особливого виміру характеристик буття людини та

соціальних утворень (соціальних систем), яке володіє власними закономірностями та характерними для нього умовами.

Загальновідомо, що проблематика кризи, як занепаду, загострення протиріч, переломний момент тощо, завжди була в колі уваги гуманітарної думки.

Так, під кризою в соціальних науках розуміється гостра форма прояву соціальних протиріч, що робить неможливим стабільний, стійкий розвиток суспільства в цілому або його життєво-важливих підсистем. Тому логічною є, наприклад, думка М.Кармазіної, щодо сутності політичної кризи. Вказана криза, вважає вона "є етапом у розвитку політичного об'єкта, який характеризується порушенням рівноваги однієї чи кількох базових підсистем у процесі їхнього функціонування, тому змінюється сутність об'єкта, порушується регулярність політичної взаємодії, тому така криза може проявлятися в зміні не тільки стану об'єкта, а й його характеристик".

Звичайно, політична нестабільність не завжди має наслідком політичну кризу. Її розгортанню/запобіганню (подоланню) може сприяти чи перешкоджати негативний/позитивний потенціал політичного об'єкта, його неспроможність/спроможність протистояти деструктивним викликам шляхом неприйняття/реалізації ефективних політичних рішень. Тому криза може завершитися як подоланням, так і політичним конфліктом між політичними суб'єктами, у т. ч. у формі перевороту, революції, громадянської війни тощо.

З огляду на це, варто погодитися із І.Забеліною, що політичні кризи є вкрай небезпечними, оскільки вони є результатом нестабільного розвитку політичної системи або тупикового стану політичних відносин, найвищий прояв політичних протиріч. Тому її наслідками можуть бути руйнування всієї системи управління і соціальна катастрофа. Це актуалізує пошук шляхів діагностики політичних криз.

С.Ставченко, розглядаючи можливі індикатори кризових явищ як інструментів діагностики політичної кризи, вважає, що "у діагностиці політичної кризи досить перспективним убачається виділення трьох типів індикативних показників аналізу кризи залежно від стадії кризи, а саме:

індикатори передкризового стану;
індикатори актуалізації політичної кризи;
індикатори післякризового періоду".

Є всі підстави погодитися з нею, що для *прогнозування та превентивного управління* політичною кризою найбільш перспективними виявляються аналіз та діагностика індикаторів передкризового стану політичної системи, а з позицій *політичного управління* в кризовій ситуації – аналіз можливостей ескалації кризових явищ та "керованості" параметрами політичної системи.

Очевидно також, що управління в умовах *післякризового* періоду має здійснюватися з урахуванням результатів аналізу *наслідків* кризової ситуації.

Таким чином, С.Ставченко передкризовий стан не ідентифікує як кризову ситуацію, а останню фактично інтерпретує як кризу.

Заслуговує на увагу і думка Е. Короткова, що криза державного управління це "особливий переломний стан у розвитку і функціонуванні політичної системи суспільства, державно-владних структур, що визначається нестабільністю, розбалансованістю діяльності політичних інститутів, зниженням рівня керованості соціально-економічними процесами, загостренням політичних конфліктів, наростанням критичної активності мас".

Варто також зазначити, що в теорії міжнародних відносин криза розглядається як одна зі стадій конфлікту, тому в основному проблеми їх врегулювання розглядаються через призму врегулювання конфлікту в цілому.

Трансформація кризової ситуації, яка виникає між учасниками воєнно-політичних відносин, метою яких є досягнення власних інтересів у тому числі із застосуванням воєнних інструментів, у політичну кризу, а останньої у воєнну, як правило, є наслідком їх неспроможності вирішити протиріччя, які виникли у контексті їх політичних, воєнних та інших намірів. Настання воєнної кризи завжди свідчать про високу ймовірність виникнення воєнного конфлікту, під яким розуміється "форма розв'язання міждержавних або внутрішньодержавних суперечностей із двостороннім

застосуванням воєнної сили, основними видами якого є війна та збройний конфлікт".

Таким чином, криза є визначальною властивістю будь-якої соціальної системи і є наслідком дії багатьох взаємопов'язаних факторів. Це породжує певні дискусії при класифікації криз та термінологічну плутанину з близькими за значенням термінами, такими, зокрема, як "надзвичайна ситуація", "кризовий стан", "катастрофа". Вони часто вживаються як синоніми, але співвідношення цих понять до кінця не розроблено, тому потребує більш чіткого їх поділу.

Так, А.Терент'єва зауважує, що дефініції "кризова ситуація" та "надзвичайна ситуація" дуже часто використовують як синоніми, проте їх слід розрізняти, незважаючи на те, що вказані ситуації мають спільні характеристики в управлінському сенсі, включаючи необхідність в координації комплексу оперативних заходів і комунікацій. Проте у подальшому вона майже не розрізняє не тільки ці поняття, а й поняття "криза" стверджуючи, що "надзвичайна ситуація може стати кризою у випадку, якщо виникає відчуття того, що держава не здатна керувати ситуацією та що кризи не обов'язково становлять серйозну загрозу життю і здоров'ю громадян, й тому прийняття управлінських рішень з метою нейтралізації кризових ситуацій може лежати поза межами повноважень центральних органів виконавчої влади, уповноважених з цих питань".

6.3. Характерні риси кризової ситуації, як об'єкта управління та їх стадії

Характерні риси кризової ситуації, як об'єкта управління. На думку Є.Гризунової характерні риси кризової ситуації, як об'єкту управління мають об'єктивну і суб'єктивну складові, передусім:

наявність загрози;
невизначеність;
ескалація подій;
втрата контролю;
наростання втручання зовнішніх сил;
паніка.

Вона ж акцентує увагу на тому, що як соціальне явище кризи має ряд амбівалентних властивостей, а саме вони:

творчо-руйнівні (залежно від результату можуть як спровокувати руйнівні наслідки, так і сприяти позитивним змінам);

континуально-дискретні (є переломним моментом у розвитку системи і багатоетапним керованим процесом);

об'єктивно-суб'єктивні (об'єктивне порушення в системі і суб'єктивне усвідомлення ситуації як кризової).

Це означає, що кризові ситуації при належному управлінні є сприятливою можливістю для оновлення та консолідації тієї чи іншої організації, зокрема держави.

Наведені Є.Гризуновою характеристики та властивості кризових ситуацій є досить вичерпними, але вона чомусь ототожнює поняття "кризова ситуація" і "криза".

Кризові ситуації є динамічними у часі і просторі, що дозволяє виділити їх певні стадії, у тому числі ті, на яких можуть виникнути кризи, як надзвичайні ситуації, наслідки яких завжди мають негативний характер.

Дійсно, згідно ст.1 Закону України "Про правовий режим надзвичайного стану": 'Надзвичайний стан – це особливий правовий режим, який може тимчасово вводитися в Україні чи в окремих її місцевостях при виникненні надзвичайних ситуацій техногенного або природного характеру…. або при спробі захоплення державної влади чи зміни конституційного ладу України шляхом насильства". Тобто можливому введенню надзвичайного стану передує виникнення певної надзвичайної ситуації.

Стосовно неї ст.4 цього Закону дає пояснення: "надзвичайний стан вводиться лише за наявності *реальної загрози* безпеці громадян або конституційному ладові, усунення якої іншими способами є неможливим".

Таким чином, для того, щоб події не виходили з-під контролю під час виникнення надзвичайних ситуацій виникає необхідність застосовування специфічних організаційно-правових форм забезпечення національної безпеки і нормалізації ситуації, зокрема, введення надзвичайного стану.

Водночас, згідно ст.2 Кодексу цивільного захисту "надзвичайна ситуація – обстановка на окремій території чи суб'єкті господарювання на ній або водному об'єкті, яка характеризується порушенням нормальних умов життєдіяльності населення, спричинена катастрофою, аварією, пожежею, стихійним лихом, епідемією, епізоотією, епіфітотією, застосуванням засобів ураження або іншою небезпечною подією, що призвела (може призвести) до виникнення загрози життю або здоров'ю населення, великої кількості загиблих і постраждалих, завдання значних матеріальних збитків, а також до неможливості проживання населення на такій території чи об'єкті, провадження на ній господарської діяльності".

Варто також зазначити, що ст. 5 вказаного Кодексу одним із видів надзвичайних ситуацій визначає соціальні, але не дає їх визначення.

Таким чином, якщо слідувати офіційній нормативній термінології, то об'єктами соціологічного аналізу можуть виступати лише кризи і надзвичайні ситуації. При цьому існує система управління в умовах надзвичайних ситуацій, значна кількість наукових досліджень з цього приводу.

Водночас очевидно, що управління в умовах надзвичайних ситуацій не тотожне кризовому управлінню ("управлінню кризою"), оскільки не всяка криза пов'язана із загрозами життю і фізичній безпеці громадян чи втрати матеріальних ресурсів. Тобто у даному випадку йдеться про різні соціальні явища, які можуть в деяких випадках розвиватися паралельно і взаємопов'язано. Тому ухвалення управлінських рішень з метою нейтралізації негативних наслідків кризових ситуацій виходить далеко за межі повноважень Державної служби з надзвичайних ситуацій, на які передусім покладаються завдання щодо ліквідації наслідків надзвичайних ситуацій.

Крім того, надзвичайні ситуації завжди характеризуються певним збитком (шкодою), тобто їх наслідки завжди негативні, а наслідки кризових ситуацій, через амбівалентності їх властивостей, можуть мати водночас негативні та позитивні наслідки. Водночас між вказаними ситуаціями існує прямий та зворотній зв'язок.

Передумовою надзвичайних ситуацій є надзвичайні події та катастрофи, які можуть бути наслідками соціальних криз (масові безпорядки, погроми тощо) і, навпаки, соціальні кризи можуть бути наслідками неадекватного реагування на надзвичайні ситуації з боку органів державного управління.

Принципово важливим є й те, що останнім часом надзвичайні ситуації усе частіше виникають через використання державами для досягнення своїх стратегічних цілей так званих "несилових" методів розв'язання політичних, економічних та інших суперечностей, які виникають між ними.

Основою цих методів є ІКТ навмисного (штучного) "збурювання" (загострення) політичних, економічних, культурологічних та інших суперечностей, що призводять до виникнення кризових ситуацій, наслідком яких є відповідні кризи, що переростають у надзвичайні ситуації.

Стадії кризових ситуації. Розглядаючи кризові ситуації, які виникають у соціальних системах (кризові ситуації соціального характеру) у контексті зростання небезпек людині (індивіду), суспільству та державним інститутам можна виділити чотири стадії (етапи) їх розвитку.

Початкова стадія, на якій виникають політичні, економічні та інші явні або приховані протиріччя між суб'єктами соціальних взаємодій (суспільних відносин), які призводять до напруженості у відносинах між ними, тобто виникає підґрунтя для виникнення кризової ситуації та відбувається накопичення певних викликів для життєдіяльності вказаних суб'єктів;

Стадія «статус-кво», на якій протиріччя між суб'єктами соціальних взаємодій й, відповідно, зростання напруженості у стосунках між ними стають очевидними, тобто кризова ситуація набуває чітких обрисів з огляду на цілі (наміри) її учасників, їх дії та ресурси тощо та завершується накопичення потенційних загроз для життєдіяльності цих суб'єктів.

У даному випадку використання терміну «статус-кво» підкреслює те, що на цьому етапі подальший розвиток ситуації суб'єкти суспільних відносин вбачають взаємно небажаним, оскільки результат при будь-яких змінах може бути для них досить ризикованим через накопичені потенційні загрози для їх

життєдіяльності, проте вони визнають (очікують), що з часом, може статися якась зміна, що створить можливість досягти їх цілей (намірів).

Стадія настання критичної ситуації, для якої характерним є, як правило, стрімке та значне загострення протиріч між суб'єктами соціальних взаємодій, й, відповідно, зростання напруженості у стосунках між ними через що вони зіштовхуються з неможливістю задоволення життєво важливих для них потреб (мотивів, намірів, цінностей тощо), тобто потенційні загрози для них трансформуються у реальні. Це свідчить про настання надзвичайної ситуації, якщо розглядати ситуацію через призму небезпек людині (індивіду), суспільству чи інститутів держави у тій чи іншій сфері їх життєдіяльності (політичній, економічній тощо).

Стадія трансформації для якої характерним є затухання (ліквідація, врегулювання, вирішення тощо) протиріч між суб'єктами соціальних взаємодій, й, відповідно, напруженості у стосунках між ними, як наслідок прийняття тих чи інших політичних та державно-управлінських рішень та їх імплементація з метою формування нової соціальної реальності щодо механізмів соціальних взаємодій (нових або радикально реформованих суспільно-політичних систем і механізмів).

Отже, кінцевим результатом розвитку кризової ситуації є формування якісно нової соціальної реальності, а основним критерієм ідентифікації стадій розвитку кризових ситуацій доцільно обирати небезпеки національній безпеці за схемою: виклик – потенційна загроза – реальна загроза, які мають ймовірнісну природу, що передбачає їх оцінювання з використанням концепту "ризик".

З огляду на поліцентричну та багатофакторну природу кризових ситуацій соціального характеру, оцінка цих ризиків має відбуватися на всіх етапах кризового управління. При цьому на стадії "критична ситуація" характеристики надзвичайної ситуації мають враховувати й міру соціальних девіацій і дисфункцій.

Крім того, на всіх стадіях мають аналізуватися та враховуватися недоліки в управлінні, яким належить значна роль у провокуванні соціальних кризових ситуацій.

Таким чином, характеристики кризової ситуації соціального характеру у контексті її розвитку не обов'язково пов'язані з реальними загрозами безпеці громадян або конституційному ладові. Тому ототожнення понять кризова ситуація та надзвичайна ситуація з методологічної точки зору є помилкою, а з практичної – небезпечно, оскільки може призвести до неадекватних управлінських рішень в тих чи інших ситуаціях й відповідних наслідків для національної безпеки.

Очевидно, що можливі різні типи та підтипи кризових та надзвичайних ситуацій, що зумовлено впливом різних і часто суперечливих факторів на їх зародження та динаміку розвитку.

Водночас реальне буття (існування) людини (індивіда), соціальних утворень, інститутів держави та зумовлені ним соціальні взаємодії набагато складніше будь-яких схем. Упроцесі цих взаємодій має місце співробітництво, зіткнення цінностей, мотивів поведінки, інтересів, протиборство, суперництво тощо. Все це призводять до тих чи інших конфліктів, які не виникають спонтанно, є проявом соціальної напруженості, а відтак "локомотивом" кризових ситуацій, що виникають в соціальних системах.

Варто також зазначити, що з огляду на викладене поняття "кризове управління" ("управління кризою"), є більш коректне, ніж домінуюче на вітчизняних теренах поняття "антикризове управління".

Врешті-решт, як стверджують деякі дослідники "Будь-яка держава як "жива" система має здатність "хворіти". Хвороба проявляється в нестабільності, проблемах, кризах і конфліктах. На стадії розвитку держави виникають патології, що відрізняються від родових, до захисту від яких система управління не готова.

Що ж до України, то як зазначав Ю.Сурмін, найпоширенішими її хворобами є:

"корупція органів та посадових осіб державного управління та місцевого самоврядування;

розбалансованість системи управління;

порушення прав і свобод громадян;

підміна управлінської діяльності піарівською грою політиків;

неадекватність управлінської діяльності цілям, завданням, ресурсам, ситуації, інформації, її ціннісні провали",

Безумовно, що вказані "хвороби" держави є одним із головних джерел небезпек для буття людини (індивіда) та соціальних утворень.

Таким чином, кризові ситуації є невід'ємним атрибутом соціальної системи, операціоналізуються через поняття "протиріччя", сприяють зміні якісно-кількісних характеристик буття соціальної системи у руслі формування нової соціальної реальності.

Аналіз наукового доробку та законодавства дозволив дійти висновку, що кризова ситуація, критична ситуація, криза, надзвичайна ситуація, є визначальними властивістю вказаних систем та наслідком дії взаємопов'язаних факторів зважаючи на що деякі поняття вживаються як синоніми, що свідчить про необхідність більш чіткого з'ясування їх співвідношення.

Кризові ситуації соціального характеру розвиваються у часі та просторі, що дозволяє виділити їх певні стадії, у тому числі ті, на яких можуть виникнути надзвичайні ситуації, характерною особливістю яких є те, що управління в таких ситуаціях не тотожне кризовому управлінню, оскільки,

по-перше, не всяка криза пов'язана із загрозами фізичній безпеці громадян чи втрати матеріальних ресурсів;

по-друге, наслідки надзвичайних ситуацій завжди негативні, а кризових ситуацій через амбівалентності їх властивостей, можуть мати негативні та позитивні наслідки. Крім того, між вказаними ситуаціями існує прямий та зворотній зв'язок.

Тому важливим є організація (створення) ефективної системи моніторингу кризових ситуацій основою яких мають бути сучасні ІКТ.

Розгляд соціальних кризових ситуації у контексті зростання небезпек людині (індивіду), суспільству та державним інститутам та з огляду на характер соціальних взаємодій цих суб'єктів дозволив виокремити чотири стадії їх розвитку:

початкова, на якій виникають протиріччя між суб'єктами та відбувається накопичення певних викликів для їх життєдіяльності;

статус-кво – кризова ситуація набуває чітких обрисів з огляду на цілі (наміри) суб'єктів та завершується накопичення потенційних загроз для їх життєдіяльності;

критична ситуація – стрімко зростає напруженість у стосунках між суб'єктами, а потенційні загрози для них трансформуються у реальні, що свідчить про настання надзвичайної ситуації;

трансформації – затухання протиріч між суб'єктами та формування нової соціальної реальності щодо механізмів соціальних взаємодій.

Визначальними рисами та причинами сучасних кризових ситуації сьогодні, зокрема, є: зростання ролі масових комунікацій та нових технологій в генеруванні кризових ситуацій, що зумовлює необхідність розробки нестандартних управлінських рішень, не обов'язково пов'язаних з реальними загрозами безпеці громадян або конституційному ладові, тому ототожнення цього поняття з поняттям надзвичайна ситуація є методологічною помилкою.

Запитання та завдання для самоконтролю

1. Розкрийте зміст поняття «інформаційно-аналітична діяльність» та її складові
2. Якою є мета інформаційно-аналітичної діяльності та її сутнісні риси у сфері національноїбезпеки?
3. Розкрийте взаємозалежність управлінської інформації та управлінських функцій
4. Які створює два типи потоків утворює інформація всередині соціальної системи?
5. За якими ознаками класифікують інформацію в системі управління
6. Дайте загальну характеристику типів інформації в управлінських системах
7. Розкрийте сутність соціальної інформації та вимоги до неї

8. Розкрийте особливості аналітичної діяльності в управлінських процесах

9. Розкрийте зміст основних груп методів дослідження операцій як технології інформаційного забезпечення управлінських рішень

10. Чому інформаційно-аналітичне забезпечення є самостійним видом діяльності в управлінській сфері?

11. Розкрийте зміст інформаційного забезпечення у сфері національної безпеки та його завдань

12. Чому домінуванням техніко-технологічного підходу до управління може призвести до небезпеки нерозуміння важливості ролі інформаційно-аналітичних ресурсів?

13. Розкрийте зміст внутрішньої та зовнішньої функцій інформаційно-аналітичного забезпечення у сфері національної безпеки

14. Рокрийте взаємозвязок інформації та інформаційних технологій

15. Розкрийте зміст етапів розвитку інформаційних технологій

16. Розкрите зміст поняття ІКТта їх структуру

17. Які можливості надає інформатизація суспільства?

18. Які компоненти створення та функціонування сучасних ІКТ виокремлюють фахівці?

19. Які можливості створюють для суспільства створює розвиток ІКТ?

20. Які проблеми (виклики) для суспільства породжує розвиток ІКТ?

21. Дайте загальну характеристику класифікації новітніх ІКТ у контексті забезпечення безпеки

22. У чому полягає важливість стандартів у сфері розвитку ІКТ з огляду на міжнародний досвід?

23. Дайте загальну характеристику проблеми захисту ІКТ від кіберзагроз

24. Які пріоритети України в сфері кібербезпеки?

25. Розкрийте зміст проблемних питань розвитку ІКТ в Україні

26. Розкрийте зміст проблема з’ясування співвідношення кризових та надзвичайних ситуацій

27. Розкрите світоглядний аспект природи кризових ситуацій соціального характеру

28. Дайте характеристику нормативно-правового трактування сутності кризових ситуацій.

29. Чому поняття “криза”є особливим виміром характеристик буття соціальної системи?

30. Опишість характерні риси кризової ситуації, як об’єкта управління.

31. Розкрийте зміст стадій кризових ситуацій в соціальних системах

32. Чому важливим є належний інформаційний моніторинг стадій кризових ситуацій?

Список рекомендованої літератури

1. Варенко В.М. Інформаційно-аналітична діяльність: навч. посіб. К.: Університет «Україна», 2014. 417 с.

2. Данильчук Л. Сутність і зміст поняття «інформаційно-комунікаційні технології». *Педагогіка і психологія професійної освіти*. 2012. № 4. С. 123-130

3**.** Державне управління : підручник : у 2 т. / Нац. акад. держ. упр. при Президентові України ; ред. кол. : Ю.В. Ковбасюк (голова), К.О. Ващенко (заст. голови), Ю.П. Сурмін (заст. голови) [та ін.]. - К. ; Дніпропетровськ: НАДУ, 2012. Т. 1. 564 с.

4. Демартино А.П. Поняття і класифікація новітніх інформаційно-комунікативних технологій // *Науковий часопис НПУ імені М. П. Драгоманова* Випуск 24.2018.С.94-99

5. Державно-громадянська комунікація: шлях від кризи до взаємодії: монографія / Козаков В.М., Рашковська О.В., Ребкало В.А., Романенко Є.О., Чаплай І.В. К.: ДП “Вид. дім “Персонал”, 2017. 288 с.

6. Доронін І.М. Національна безпека України в інформаційну епоху: теоретико-правове дослідження. Дис…докт. юрид. наук: 12.00.01; Наук.-досл. інст. інформ. і права, Нац. акад. прав. наук України. Київ. 2020.539 с.

7. Драгомирецка Н.М. Сучасні тенденції комунікацій у сучасному світі. *Публічне урядування* : збірник. 2015. N 1. Київ: ДП «Видавничий дім «Персонал», 2015. С. 85-97.

8. Драгомирецька Н.М., Кандагура К.С., Букач А.В. Комунікативна діяльність в державному управлінні: навч. посібник. Одеса: ОРІДУ НАДУ, 2017. 180 с.

9. Дрешпак В.М. Комунікації в публічному управлінні: навч. пос. Д. : ДРІДУ НАДУ, 2015. 168 с.

10. Глобальна та національна безпека: підручник / авт.кол.: В.І. Абрамов, Г.П. Ситник, В.Ф. Смолянюк та інш.; за заг.ред. Г.П. Ситника. К.: НАДУ, 2016. 784 с.

11. Глобалізаційні виклики сучасності: підручник /авт.кол. Л.Г. Комаха, І.В. Алексеєнко, В.Л. Гура та ін.; за заг.ред. Л.Г. Комахи.- К.: ВПЦ "Київський університет", 2022. 350 с.

12. Гнатенко В. Застосування інформаційно-комунікаційних технологій у забезпеченні економічної безпеки держави // *Літопис Волині*. *Всеукраїнський науковий часопис*. № 22. 2020. С.88-92

13. Інформаційна складова державної політики та управління : монографія / Соловйов С.Г., та ін. ; заг. ред. Грицяк Н.В. ; НАДУ. К.: К.І.С., 2015. 320 с.

14. Кириченко Г.В. Інформаційно-комунікаційні механізми як інновації в системі формування позитивного іміджу органів державної влади. *Вчені записки Таврійського Національного Університету імені В.І. Вернадського. Серія: державне управління* Т. 30 (69). № 6. 2020. С. 46-54.

15. Клубань О.М., Курбан О.В., Любовець Г.В., Король В.Г., Савчук Р.П. Сучасні комунікаційно-контентні процеси в безпековій сфері:навч. посібник. Київ: ВІКНУ, 2016. 170 с.

16. Кочубей Л. Особливості сучасних інформаційно-комунікативних технологій в Україні. *Наукові записки*. Вип. 3 (89). 2018. С. 44-70.

17. Климанська Л.Д. Соціально-комунікативні технології в політиці: таємниці політичної «кухні». Львів: Видавництво Національного університету «Львівська політехніка», 2007. 332 с.

18. Маліновська О.Я. Використання сучасного зарубіжного досвіду комунікацій в системі публічного адміністрування // *Збалансоване природокористування* № 2. 2022. С.39-44

19. Ніколаєнко Н.О. Інформаційна безпека та політична комунікація: навч.-метод. посібник. Миколаїв: НУК, 2022. 121 с.

20. Олешко А.А. Інформаційно-комунікаційні технології та людський розвиток // *Інвестиції: практика та досвід* № 16. 2019. С.16-19

21. Орел М.Г. Теоретичні основи державного управління у сфері політичної безпеки: монографія. Київ: Поліграф плюс 2019. 320 с.

22. Основи теорії управління у сфері національної безпеки: курс лекцій / Г.П. Ситник. К: ТОВ "САК Лтд.", 2023. 174 с.

23. Островська Н.В. Прикладні соціально-комунікаційні технології: навч. посібник. Запоріжжя. ЗНТУ, 2017. 110 с.

24. Пацурія Н. Упровадження технологій штучного інтелекту в забезпечення національної безпеки та обороноздатності України: правові проблеми і перспективи повоєнного періоду// *Теорія і практика інтелектуальної власності* . №3.2023. С.68-78

25. Про доступ до публічної інформації: закон України від 13.01.2011 № 2939-VI. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi

26.Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Постанова Кабінет Міністрів України від 29 березня 2006 р. n 373 із змінами, внесеними згідно з Постановою КМ N 645 (645-2022-п) від 03.06.2022 URL: https://zakon.rada.gov.ua/laws/show/373-2006-п#Text

27. Про захист інформації в інформаційно-телекомунікаційних системах: закон України від 05.07.1994 № 80/94-ВР // Законодавство України. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi

28. Про інформацію: закон України від 02.10.1992 № 2657-XII. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi

29.Публічне управління та адміністрування у сфері національної безпеки: (системні, політичні та економічні аспекти): словник-довідник / С.П. Завгородня, М.Г. Орел, Г.П. Ситник [уклад.] /за заг.ред. Д.В. Неліпи, Є.О. Романенка, Г.П. Ситника. Київ: Видавець Кравченко Я.О., 2020. 380 с.

30. Редька І. Інформаційні технології. Основні якості сучасних інформаційних технологій. *Матеріали Всеукраїнської науково-практичної конференції «Соціальні комунікації і нові комунікативні технології*». Запоріжжя, 2017. С. 20-25.

31. Ситник Г.П., Орел М.Г. Публічне управління у сфері національної безпеки: підручник /за ред. Г.П. Ситника. - Київ: Видавець Кравченко Я.О., 2020. 360 с.

32. Ситник Г.П., Борисов А.В. Політичний досвід розвинених країн світу щодо інформаційно-аналітичного забезпечення системи цивільної безпеки // *Національні інтереси України*. 2024. № 2(2) .С.124-133. – URL: https://doi.org/10.52058/3041-1793-2024-2(2)-123-132

33. Ситник Г.П. Інформаційна компонента критичних (надзвичайних) ситуацій у контексті забезпечення державної безпеки. *Науковий вісник: Державне управління*. 2020. №2(4). С.327-339

34. Ситник Г.П., Клименко Н.Г. , Гореліков І.О. Державна політика забезпечення інформаційної безпеки та кібербезпеки, як її складової: проблеми та шляхи їх вирішення // «*Державне управління: удосконалення та розвиток*». 2024. No 5. – URL: https://nayka.com.ua/index.php/dy/article/view/3678

35. Соколов В.А. Інституалізація аналітичної діяльності в системі забезпечення національної безпеки на основі застосування зарубіжного та вітчизняного досвіду. Дис. … канд. наук з держ.упр.: 25.00.01; Харківський рег. інст. держ. управ. НАДУ. Харків, 2020. 375 с.

36. Стратегія інформаційної безпеки. Указ Президент України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

37. Толстой В.В., Петречук Л.М., Іващенко Ю.С., Гуляєва О.А., О.В. Соболенко. Сучасні інформаційно-

комунікаційні технології: навч. посібник. Дніпро: Нац.металур.акад. України, 2019. 230 с.

38. Швачич Г.Г., Толстой В.В., Петречук Л.М., Іващенко Ю.С., Гуляєва О.А., Соболенко О.В. Сучасні інформаційно-комунікаційні технології: навч. посібник. Дніпро: НМетАУ, 2017. 230 с.

РОЗДІЛ 3
ПРАКТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ ІКТ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

ГЛАВА 7. ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ПРИ ПРИЙНЯТТІ РІШЕНЬ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

7.1. Переваги автоматизації процесів прийняття рішень та компоненти інформаційної системи управління

Переваги та передумови автоматизації процесів прийняття рішень. Розробка ефективних управлінських рішень потребує застосування сучасних інформаційних технологій, що забезпечують повноту, своєчасність інформаційного відображення процесів, можливість їхнього моделювання, аналізу, прогнозування.

Переваги автоматизації процесів прийняття рішень полягаютьу наступному.

Підвищення швидкості прийняття рішень:

скорочення часу на збір та аналіз інформації;

швидке реагування на зміни.

Покращення якості рішень:

змінення впливу людського фактору та суб'єктивності;

використання складних аналітичних моделей для обробки даних.

Оптимізація використання ресурсів:

ефективний розподіл людських та матеріальних ресурсів;

зниження операційних витрат.

Підвищення продуктивності праці:

автоматизація рутинних завдань;

вивільнення часу співробітників для стратегічних завдань.

Покращення координації та комунікації:

забезпечення єдиного інформаційного простору для всіх підрозділів;

полегшення обміну даними між рівнями управління.

Підвищення конкурентоспроможності:

швидка адаптація до змін у відповідній сфері;

можливість прийняття проактивних рішень на основі прогнозів.

Поліпшення контролю та звітності:

можливість відстеження ключових показників ефективності в реальному часі:

Автоматизація процесів звітності та аудиту.

Компоненти інформаційної системи управління. Інформаційна система (ІС) – це набір процедур, таких як процес, збирання й переробка інформації для підтримки планування, прийняття рішень, координації та контролю. ІС містить вхідну (дані, інструкції тощо) й вихідну інформацію (звіти, розрахунки тощо), а також може мати механізм зворотного зв'язку, що контролює операції.

Серед компонентів вказаної системи виокремлюють наступні.

Апаратне забезпечення:

сервери та робочі станції;

мережеве обладнання;

пристрої введення/виведення даних.

Програмне забезпечення:

операційні системи;

системи управління базами даних;

прикладне програмне забезпечення для аналізу та обробки даних.

База даних:

централизованное сховище данных;

системи управління великими даними (Big Data)

Мережева інфраструктура:

локальні та глобальні мережі;

системи захисту інформації.

Аналітичні інструменти:

системи бізнес-аналітики (BI);

інструменти прогнозування та моделювання.

Інтерфейс користувача:

графічні інтерфейси для різних категорій користувачів;

системи візуалізації даних та звітності.

Системи підтримки прийняття рішень:

експертні системи;

системи штучного інтелекту та машинного навчання.

Модулі інтеграції:

інтерфейси для взаємодії з іншими інформаційними системами;

API для обміну даними із зовнішніми джерелами.

Системи безпеки та контролю доступу:

механізми аутентифікації та авторизації;

системи моніторингу та аудиту.

Ефективне впровадження та використання цих компонентів дозволяє організаціям максимально використовувати переваги автоматизації процесів прийняття рішень, підвищуючи свою ефективність та конкурентоспроможність на ринку.

Ключову позицію в інформаційній системі посідає *система обробки даних*. Спочатку дані вводяться в інформаційну систему, далі вони проходять різні форми обробки і трансформуються у ”вихідну” інформацію: звіти, аналітичні матеріали, розрахунки й інші матеріали для прийняття управлінських рішень і контролю виконання поставлених завдань.

Розглянемо складник програмного забезпечення детальніше.

Програмне забезпечення– це набір програм, документів, процедур, повсякденних операцій комп’ютерної системи, що дають змогу технічним засобам виконувати різні операції. Найважливішими класами програмного забезпечення є системне і спеціальне (прикладне), у вигляді пакетів прикладних програм (ППП), що дають можливість організаціям здійснювати управління і мати доступ до необхідних даних.

Пакети прикладних програм (ППП) – це сукупність взаємопов’язаних прикладних програм для виконання типових роз- рахунків у досить формалізованих галузях знань: дослідження проблеми, аналіз даних, моделювання, документування й оформлення результатів.

ППП мають задовольняти загальні вимоги:

простота освоєння і використання;

відповідність високим вимогам до введення, перетворення і зберігання даних;

широкий набір засобів графічного зображення даних і результатів їхньої обробки;

можливість залучення таблиць і графіків до звіту;

великий набір методів аналізу даних;

докладність документації.

До *проблемно-орієнтованих ППП*, зокрема, належать такі програмні продукти.

1. *Текстові процесори* – програми для роботи з документами (текстами), що дають змогу компонувати, форматувати, редагувати тексти під час створення користувачем документа.

2. *Настільні видавничі системи* (НВС) – програми для професійної видавничої діяльності, які дають змогу здійснювати електронну верстку основних типів документів, наприклад, об'ємного каталогу або торговельної заявки.

3. *Графічні редактори* – пакети для обробки графічної інформації, а саме растрової графіки та зображень і векторної графіки.

4. *Електронні таблиці* (табличні процесори) – програми для обробки даних таблиці.

5. *Організатори робіт* – пакети програм, призначені для автоматизації процедур планування використання різних ресурсів.

6. *Програми розпізнавання символів* призначені для перекладу графічного зображення літер і цифр у ASCII.

7. *Фінансові програми*, які використовуються для ведення фінансів, автоматизації бухгалтерського обліку організацій, економічного прогнозування розвитку організацій, аналізу інвестиційних проєктів, розробки техніко-економічного обґрунтування фінансових угод.

8. *Аналітико-статистичні програми*, котрі використовуються для аналізу даних, можна умовно поділити на математичні і статистичні. У табличних процесорах часто зустрічаються засоби описової статистики, методи регресійного аналізу, засоби аналізу часових рядів, згладжування і прогнозування.

Статистична обробка даних є основою створення математичної моделі розв'язуваної задачі. Статистичні пакети можна поділити на спеціалізовані (містять методи, що використовуються в конкретній сфері) та загального призначення (універсальні). До групи пакетів загального призначення належать системи StatGraphics, Stadia, Statistica, SPSS. Програма MS Excel дає змогу розв'язувати задачі математичного програмування, прогнозування даних, проводити кореляційно-регресійний аналіз моделей, застосовувати статистичні функції, здійснювати пошук оптимальних рішень. Це забезпечує високий рівень автоматизації розрахунків, комплексності, графічного моделювання й організації ресурсів під час прийняття управлінських рішень.

7.2. Класифікація інформаційних систем

Існують різноманітні підходи до класифікації інформаційних систем. Переважно їх класифікують за такими *ознаками*.

1. Функції та рівні управління: розрізняють *корпоративні* (інтегровані) й *локальні* ІС. Корпоративна ІС автоматизує всі функції управління на всіх його рівнях. Така ІС багатокористувацька. Локальна ІС автоматизує окремі функції управління на окремих його рівнях, така ІС переважно однокористувацька.

2. Організаційна структура: ІС для департаментів (однієї функціональної сфери); міжорганізаційні ІС; ІС організації.

3. Функціональні сфери: фінансові та бухгалтерські ІС; банківські ІС; ІС маркетингу; виробничі ІС; ІС управління персоналом тощо.

4. Особливості потреб різних організаційних рівнів і функціональних сфер менеджменту: процесійні ІС; офісно-автоматизаційні; управлінські системи; системи підтримки рішення; системи підтримки виконання рішень.

Процесійна система – інформаційна система, яка виконує щоденні поточні операції, потрібні для розвитку бізнесу, й забезпечує пряму підтримку на операційному рівні організації.

Офісна автоматизаційна система має полегшити зв'язок і підвищити продуктивність менеджерів через систему селекторної інформації (електронний календар, телеконференція тощо).

Управлінська система – інформаційна система, що постачає поточну інформацію, необхідну зазвичай менеджерам середнього і нижчого рівнів. Система орієнтована на фактичні, операційні напрями діяльності й важлива під час планування, прийняття рішень, контролю.

Система підтримки рішень – інформаційна система, яка підтримує процес прийняття управлінських рішень у ситуаціях, які не досить добре структуровані. Такі системи загалом не називають оптимальне рішення, але сприяють скеруванню процесу прийняття рішень у правильне русло.

Спеціалізованим типом інформаційної системи, який дедалі частіше використовують, є *експертна система* (інтенсивно-наукова), що застосовує реальні знання експерта для розв'язання спеціальних проблем, а також намагається об'єднати знання великої групи експертів.

Системи підтримки виконання рішень – інформаційні системи, що підтримують виконання рішень та ефективне функціонування організацій на вищих рівнях. Такі системи розроблені недавно, їх інколи називають виконавчо-інформаційними.

5. Характер обробки інформації. На різних рівнях управління (оперативний, тактичний, стратегічний) виділяють такі типи ІС: системи обробки даних (EDP); інформаційна система управління (MIS); система підтримки прийняття рішень (DSS).

Системи обробки даних призначені для обліку й *оперативного регулювання операцій*: підготовки стандартних документів (рахунків, накладних, платіжних доручень тощо), реєстрації й обробки подій, приймання та видачі матеріальних цінностей на складі, ведення табеля обліку робочого часу тощо. Ці завдання мають регулярний характер, реалізуються безпосередніми виконавцями.

Інформаційні системи управління орієнтовані на *тактичний рівень управління*: середньострокове планування,

аналіз й організацію робіт упродовж кількох тижнів (місяців), наприклад, аналіз і планування поставок, збуту, складання виробничих програм. Ці завдання характеризуються регламентованим формуванням кінцевих документів, призначені для керівників різних служб підприємств.

Системи підтримки прийняття рішень (СППР) використовуються здебільшого на вищому рівні управління, що має стратегічне довгострокове значення упродовж року або кількох років (формування стратегічних цілей, планування залучення ресурсів, джерел фінансування тощо). СППР можуть реалізовуватися і на тактичному рівні, наприклад, під час вибору постачальників. Завдання СППР мають зазвичай нерегулярний характер, вони мають такі недоліки, як суперечливість, нечіткість наявної інформації, слабка формалізованість.

Ідеальною вважається ІС, що містить усі три типи названих інформаційних систем.

В цілому ж відповідно до рівнів управління виокремлюють:

на стратегічному – системи підтримки виконання рішень;

на управлінському – інформаційні системи управління; системи підтримки прийняття рішень;

на рівні знань – системи знань; системи автоматизації діловодства;

на експлуатаційному – системи діалогової обробки запитів. Експлуатаційний персонал управління досить добре розв'язує структуровані проблеми.

Системи стратегічного рівня являють собою інструмент допомоги керівникам вищого рівня і готують стратегічні дослідження та довготривалі прогнози. Стратегічні аналітики зазвичай мають справу із неструктурованими проблемами.

Системи рівня знань забезпечують автоматизацію розробки нових видів продукції, створення та підтримку електронних архівів, збирання інформації, нових знань з електронних сховищ даних. Системи тактичного рівня призначені для забезпечення контролю, аналізу, управління, прийняття рішень й адміністративних дій менеджерів середньої

ланки. Ці системи часто відповідають на запитання “що..., якщо ... ?”.

Отже, інформаційні системи в організаціях розроблені для допомоги менеджерам реалізувати функції маркетингу, виробництва, обліку, управління персоналом на кожному рівні.

Найбільш важливі, напевно, управлінські інформаційні системи (MIS) та системи забезпечення прийняття рішення (DSS). У MIS дані збираються, обробляються й подаються менеджерові таким чином, щоб забезпечити оперативне управління. Приклади інформації, яка формується в базах даних: ціни, вихід продукції, швидкість, кількість розпоряджень, наявність ресурсів і потоки робочої сили.

DSS відрізняються від MIS тим, що менеджер зазвичай є внутрішнім компонентом DSS, а не зовнішнім, як у MIS. Тобто менеджер взаємодіє з комп’ютерною інформаційною системою так, щоб отримати рішення в ітеративному процесі. Інформаційні потоки взаємодії менеджера та комп’ютерної системи DSS називаються аналізом “що ..., якщо .... ?”. Комп’ютер генерує результати на економіко-математичній моделі, а менеджер його запитує: “Що трапиться, коли що-небудь зміниться в моделі?”.

Розвиток систем DSS – це експертні системи (комп’ютерні програми, що містять бази знань з окремих проблем і механізми взаємодії елементів цих баз), по суті, це інтелектуальні DSS. Експертні системи є консультантами під час прийняття рішень, оскільки містять факти, знання і правила, які взаємодіють у проблемній сфері.

7.3. Інформаційні системи підтримки прийняття управлінських рішень

Системи підтримки прийняття рішень (СППР) – це спеціалізовані автоматизовані системи, які допомагають керівникам та управлінцям приймати ефективні рішення на основі аналізу великих обсягів даних.

Ці системи забезпечують виконання декілька ключових функцій, а саме:

збір та обробка даних з різних джерел;

аналіз інформації та виявлення схованих (неочевидних) закономірностей;

моделювання можливих сценаріїв розвитку ситуації;

візуалізація результатів аналізу;

підготовка рекомендацій та щодо управлінських рішень.

Інформаційні системи підтримки прийняття управлінських рішень (ІСППУР) складаються з кількох основних блоків, кожен з яких виконує конкретні функції. Розглянемо докладніше ці ключові компоненти.

1. *Блок збору та зберігання даних:*

база даних, яка забезпечсує централізоване сховище для зберігання великих обсягів структурованої інформації;

система управління базами даних (СУБД), яка забезпечує ефективний доступ до даних та їх обробку;

інтерфейси для імпорту даних, які дозволяють отримувати інформацію з різних джерел (внутрішніх та зовнішніх).

2. *Блок аналізу та обробки інформації:*

аналітичні інструменти, які включають алгоритми для статистичного аналізу, прогнозування, оптимізації та моделювання;

модулі інтелектуального аналізу даних, які використовують методи машинного навчання та штучного інтелекту для виявлення прихованих закономірностей;

система управління моделями, яка дозволяє створювати, захищати та використовувати різні аналітичні моделі.

3. Блок генерації рішень:

експертні системи, які використовують базу знань та правила для формування рекомендацій;

модулі оптимізації, які допомагають знайти оптимальні рішення в складних ситуаціях;

системи підтримки групових рішень, які забезпечують спільне прийняття рішень.

4. *Блок візуалізації та представлення результатів*:

інструменти візуалізації, які створюють графіки, діаграми та інші видимі представлення даних;

генератори звітів, які формують структуровані звіти на основі аналізу результатів;

інтерактивні табло, яке надає оперативний доступ до ключових показників.

5. *Блок користувацького інтерфейсу*:

графічний інтерфейс користувача, який забезпечує зручну взаємодію користувача з системою;

модулі налаштування, які дозволяють адаптувати систему під конкретні потреби користувача;

система допомоги та навчання, яка надає підтримку користувачам у роботі з системою.

6. *Блок безпеки та адміністрування*:

система контролю доступу, яка забезпечує захист даних та розмежування прав користувачів;

модулі аудиту, які відстежують дії користувачів та зміни в системі;

інструменти резервного копіювання, які гарантують збереження даних та можливість відновлення.

Ці блоки взаємодіють між собою, створюючи комплексну систему, яка керівникам аналізує проблеми, розглядає альтернативи та приймає обґрунтовані рішення.

Ефективність ІСППУР залежить від правильної інтеграції всіх цих компонентів та їх адаптації до конкретних потреб організації.

Переваги використання ІСППУР полягають у наступному.

підвищення швидкості та якості прийняття рішень;

можливість обробки великих масивів даних;

виявлення неочевидних взаємозв'язків між факторами;

зниження впливу людського фактору на прийняття рішення;

оптимізація бізнес-процесів підприємства.

Інформаційні системи підтримки прийняття рішень широкого використання в різних сферах:

В екологічній безпеці - для прогнозування та запобігання екологічним загрозам

В медицині - для діагностики захворювань та призначення лікування

В управлінні підприємствами - для оптимізації бізнес-процесів та кадрових рішень

У фінансовій сфері - для аналізу ринків та управління ризиками

Отже, інформаційні системи підтримки прийняття управлінських рішень є потужним інструментом, який керівникам приймає обґрунтовані рішення на основі комплексного аналізу даних, що особливо важливо в умовах сучасної інформаційної економіки.

СППР складається з двох основних підсистем – це люди, що приймають рішення, і комп'ютерна система.

Систематику СППР можна побудувати за функціональними галузями (маркетинг, планування, інвестиції тощо), в яких підтримується прийняття рішень, за рівнями інформаційного забезпечення (тактичний, операційний, стратегічний, рівень середньої ланки управління) тощо.

Розглянемо дві найвідоміші таксономії (класифікації) СППР.

Класифікація СППР Альтера, розроблена на основі емпіричних досліджень 56 різних СППР, виділяє два типи систем.

1. *Системи, орієнтовані на дані (вибирають інформацію)*:

накопичування файлів;

аналізу даних;

аналізу інформації.

2. *Системи, орієнтовані на моделі (дають змогу підтримувати прийняття рішень)*:

розрахункові або облікові та фінансові моделі;

репрезентативні або образні;

оптимізаційні;

рекомендаційні.

Класифікація СППР Пауера передбачає виокремлення п'яти категорій СППР (орієнтовані на дані СППР , орієнтовані на моделі, на знання СППР, на документи СППР, на комунікації та групові СППР і три групи, які ґрунтуються на вторинних ознаках (інтерорганізаційні та інтра- організаційні СППР, функціонально-специфічні СППР і СППР загального призначення, СППР).

Різноманіття нових інструментів (методи штучного інтелекту, системи інтелектуального аналізу даних, оперативна аналітична обробка – OLAP і технології (World Wide Web, Інтернет, інтернет-мережі) здатне розширити можливості СППР і змінити форми розвитку.

Основними технологіями аналітичного моделювання для підтримки прийняття управлінських рішень є:

1. *Факторний аналіз ("причина-наслідок")* – зміна значення одних змінних (факторів) або їхніх зв'язків (формул) для дослідження простору зміни значень інших, залежних, змінних.

2. *Оптимізаційний аналіз* – отримання найкращого значення цільової функції з урахуванням накладених обмежень шляхом підбору значень змінних.

3. *Кореляційно-регресивний аналіз* – визначення виду зв'язків між залежними змінними і факторами.

4. *Аналіз тенденцій* – прогнозування динаміки розвитку об'єкта управління шляхом побудови трендів – відрізків числових рядів.

Системи підтримки прийняття рішень набули широкого застосування в різних країнах, причому їхня кількість постійно зростає. Орієнтовані на операційне управління СППР застосовуються в маркетингу (для прогнозування й аналізу збуту, дослідження ринку і цін), для виконання науково-дослідних і конструкторських робіт, в управлінні кадрами, виробництвом тощо.

Найбільша частка комп'ютерної підтримки різних функцій припадає на стратегічне планування, управління і розвиток підприємств, операційне управління й розподіл ресурсів.

Таким чином, автоматизація розробки управлінського рішення являє собою комплексний процес, в якому задіяні людські та матеріальні ресурси, програмне і технічне забезпечення, методи і процедури пошуку, обробки, передачі даних.

Інформаційна система управління – це сукупність інформації, економіко-математичних методів і моделей, технічних, про- грамних, інших технологічних засобів і

фахівців, призначена для обробки інформації та прийняття управлінських рішень у функціональних сферах, таких як бухгалтерський облік, фінанси, управління трудовими ресурсами, маркетинг і управління виробництвом.

Системи підтримки прийняття рішень утворюють підмножину автоматизованих інформаційних систем: СППР, експертні та керуючі інформаційні системи. Для прийняття управлінських рішень найбільш важливі управлінські інформаційні системи (MIS), системи забезпечення прийняття рішення (DSS).

Систематика СППР може бути побудована за функціональними галузями (маркетинг, планування, інвестиції), в яких надається підтримка прийняття рішень, за рівнями інформаційного забезпечення (тактичний, операційний, стратегічний, рівень середньої ланки управління тощо).

ГЛАВА 8. ПРОКСІ-ВІЙНИ ЯК ПРОСТІР ВИКОРИСТАННЯ СУЧАСНИХ ІКТ

8.1. Проксі-війни: поняття, причини, історія ведення

Сутність проксі-війни. Оксфордський словник політики та міжнародних відносин дає таке визначення поняття проксі-війна. Проксі-війни — це конфлікти, у яких третя сторона опосередковано втручається у вже існуючу війну, щоб вплинути на стратегічний результат на користь обраної сторони конфлікту. Іншою мовою, це збройний конфлікт, що ведеться між двома воюючими сторонами, у якому принаймні одна з воюючих сторін, будь то держава чи недержавний актор підтримується зовнішньою сторонньою силою. Проксі-війни є заміною для держав і недержавних акторів, які прагнуть досягти власних стратегічних цілей, але водночас уникають прямої, дорогої та кровопролитної війни. Такі відповіді ґрунтуються на внутрішньому сприйнятті ризику, зокрема того, що пряме втручання в конфлікт було б невиправданим, занадто дорогим (політично, фінансово чи матеріально), його можна було б уникнути, нелегітимним або нездійсненним

У терміні проксі-війна воююча сторона, яка має зовнішню підтримку, є проксі; обидві воюючі сторони у проксі-війні можуть вважатися проксі, якщо обидва отримують іноземну військову допомогу від третьої країни. Американські дослідники Кендіс Рондо та Девід Стерман у роботі «Проксі-війна XXI століття: протистояння стратегічним інноваціям у багатогополярному світі» розглядають проксі-війну як «спонсорство третьою стороною звичайних або нерегулярних збройних сил, які не мають офіційного статусі у законодавстві країни, на території якої розгортаються дії проксі-війни». Проксі-війна це військовий конфлікт, у якому є третя сторона, яка прямо чи опосередковано підтримує одного чи кількох державних чи недержавних комбатантів у спробі вплинути на результат конфлікту й таким чином просуває власні стратегічні інтереси чи підриває інтереси своїх опонентів. Треті сторони у проксі- війні як правило не беруть участі у фактичних бойових діях. Проксі-війни дозволяють великим державам уникати прямої конфронтації одна з одною, оскільки вони змагаються за вплив і ресурси. Прямі засоби підтримки третіми сторонами військового конфлікту складаються з військової допомоги та навчання, економічної допомоги, а іноді й обмежених військових операцій. Непрямі засоби підтримки включають блокади, санкції, торгове ембарго та інші стратегії, спрямовані на перешкоду однієї з сторони конфлікту.

Причини та мотиви проксі-війн. Причини та мотиви цих типів воєн різноманітні та складні, часто включають геополітичне суперництво, економічні інтереси та ідеологічні розбіжності між націями. Деякі поширені причини проксі-війн включають:

1. *Геополітичне суперництво* – багато проксі-війн велися за контроль над такими ресурсами, як нафта, вода та земля. Ці суперечки щодо ресурсів часто виникають через масштабні геополітичні суперництва між націями, такі як холодна війна між Сполученими Штатами та Радянським Союзом. У цих випадках проксі-війни використовувалися як спосіб отримати вплив і владу в регіонах, де вже існувала напруга між двома супердержавами.

2. *Економічні інтереси.* Проксі-війни також можуть підживлюватися економічними інтересами, особливо пов'язаними з торгівлею та фінансами. Наприклад, деякі проксі-війни велися за доступ до ринків або контроль над певними галузями промисловості. У цих випадках країни можуть використовувати армії-проксі для боротьби від свого імені, щоб захистити свої економічні інтереси.

3. *Ідеологічні розбіжності.* Нарешті, проксі-війни також можна вести через ідеологічні розбіжності між націями. Це може включати релігійні розбіжності, як-от конфлікт Ісламської держави із західними державами, або політичні розбіжності, як-от проксі-війни епохи холодної війни між комуністичними та некомуністичними державами. У цих випадках проксі-війни служать для держав способом просування власної ідеології та поширення її по всьому світу.

Проксі-війни мають довгу історію у світових військових протистояннях. Національні держави та імперії використовували їх як військову та зовнішньополітичну стратегію, щоб впливати на сусідні держави чи навіть підкоряти їх. Візантійська імперія (330–1453), наприклад, розпалювала проксі-війни, навмисно розпалюючи ворожнечу між різними групами всередині конкуруючих націй. Потім вона підтримала найсильнішу сторону, коли вибухали громадянські війни. Під час Першої світової війни Британія та Франція використовували подібну стратегію, підтримуючи Арабське повстання (1916–18) проти Османської імперії. Так само Громадянська війна в Іспанії (1936–39) була проксі-конфліктом між республіканськими силами, підтримуваними Радянським Союзом, і націоналістичними силами, підтримуваними нацистською Німеччиною та фашистською Італією.

Оскільки ядерні арсенали Сполучених Штатів і Радянського Союзу зростали протягом 1950-х і 60-х років, інтенсивна конкуренція між двома країнами породила думку про те, що прямий військовий конфлікт призведе до глобального знищення. Проксі-війни стали більш прийнятним способом боротьби двох наддержав за світовий вплив. Під час холодної війни Сполучені Штати, Радянський Союз і Китай вели кілька проксі-війн, включаючи громадянську війну в Анголі (1975–

2002). Війна у В'єтнамі (1954–75) була великою проксі-війною для радянсько-китайської коаліції, яка підтримувала Північний В'єтнам і В'єтконг. Виведення американських військ і поразка Південного В'єтнаму досягли мети коаліції щодо обмеження американського впливу в регіоні та посилення власного. Не стали виключенням і Корейська війна 1950—1953 років, війни за деколонізацію в Африці та Азії, повстанські рухи і громадянські війни в Латинській Америці тощо.

У 1980-х роках, після того, як Радянський Союз вторгся в Афганістан для встановлення нового афганського комуністичного уряду, Сполучені Штати виступили третьою стороною у війні, у якій протистояли афганські та радянські війська проти афганських моджахедів, які отримували зброю та інше військове обладнання від уряду США.

Проксі-війни тривають і у XXI столітті. Приклади: громадянська війна в Ємені, що почалася в 2014 році, включала велике зіткнення між войовничим рухом хуситів, підтримуваним Іраном, і урядовими силами Ємену, підтримуваними Саудівською Аравією та її союзниками. Сирійський конфлікт, спровокований місцевим повстанням у 2011 році, швидко перетворився на яскраву ілюстрацію проксі-війни, яка залучає глобальні сили та посилює її складність. Росія та Сполучені Штати зіграли ключову роль у війні, при цьому Росія підтримувала режим Асада проти повстанських сил разом з Іраном, а США підтримували різні опозиційні групи, які прагнуть повалити сирійський уряд, разом з іншими, такими як ЄС і Туреччина. Конфлікт триває і до сьогодення.

Сучасна російсько-українська війна також має елементи проксі-війн. В 2014 році російські війська перетнувши український кордон в Криму в військовій формі де не було шевронів та розпізнавальних знаків, що могли ідентифікувати їх як регулярну російську армію. Після розгортання війни Сполучені Штати та їхні союзники по НАТО (Організація Північноатлантичного договору) виступили в ролі третьої сторони, яка підтримувала Україну, надаючи матеріальну та військову допомогу уряду України вводячи економічні санкції проти Росії, тоді як Китай, Іран, Північна Корея виступали в ролі третьої сторони і підтримали Росію. Сучасна західна преса вже

називає війну в Україні першим глобальним конфліктом нової холодної війни. Два величезні альянси опосередковано, але зіткнулися на полі бою в Європі.

Типи проксі-війн. До винаходження ядерної зброї воєнні конфлікти відбувалися між державами з рішучими політичними цілями за допомогою великих армій. Цілі формулювала правляча еліта, яка уособлювала державу. У класичній війні держава вчиняла дії в усіх сферах, хоча головним акцентом були військові дії.

У середині XX ст. наймогутнішим державам вдалося створити технології виробництва ядерної зброї. Це зробило занадто безпосереднє протиборство між ними, втім не змінило їх цілей і не усунуло суперечностей. Водночас було винайдено нову концепцію геополітичного домінування – ведення воєнних конфліктів "чужими руками".

Згідно з концепцією, світові держави протистоять не прямо, а через проектування воєнних конфліктів між сателітами: політично підпорядкованими державами, різнорідними внутрішніми збройними формуваннями, тобто силами, які мають політичні цілі і засоби збройного насильства. У проксі-війні сателіти ведуть воєнні дії і застосовують звичайні, неядерні засоби збройного насильства. Держави-домінанти беруть обмежену участь у конфлікті, забезпечуючи сателітам допомогу, наприклад, постачання зброї. Тому їх дії переміщуються у невоєнну сферу. Такий тип конфлікту потребує від держави-домінанта значних витрат, оскільки сателітам, які правило, є слабкі держави, важко вести війну за рахунок власних ресурсів.

Переваги проксі-війн для держав-домінантів: знижений ризик ядерної війни та ударів у відповідь, відсутність втрат серед свого населення та інші. У разі програшу вона зазнає збитків, але не критичних для існування.

У проксі-війнах протиборство між впливовими державами не зникає, вони продовжують формулювати цілі війни. Пріоритетними сферами протиборства стають економічна, політична, інформаційна та інші невоєнні сфери. Тому проксі-війна є повністю гібридною, оскільки поєднує різні за природою та характером цілі і засоби їх досягнення.

Гібридні війни. Розвиток технологій і засобів збройної боротьби сповільнив для провідних держав можливість домінування в озброєннях. Так, паралельно з розвитком літальних апаратів триває розвиток засобів ППО та вдосконалюється ядерний потенціал. Водночас, спроможність держави вести війну визначається й іншими складовими воєнної могутності, а глобалізація привела до критичної взаємозалежності економік та інформаційних просторів держав. Тому економічні, фінансові та інформаційні інструменти протиборства набули спроможності завдавати збитків, сумірних зі збитками від застосування воєнної сили. За таких умов воєнні дії відсунулися на другій план, а воєнні конфлікти почали називати *гібридними війнами*.

У гібридних війнах правлячі еліти держав продовжують формулювати її цілі, але у воєнних діях переважають спецоперації, тобто дії з обмеженими локальними цілями. Для "ураження" противника змінено інструменти. Зазнали змін і політичні цілі війни. Раніше "класичними" цілями були анексія або зміна уряду. Нині цілями стали примушення противника до підпорядкування або поставлення під контроль його правлячої еліти.

Термін "гібридна війна" виник у документах з безпеки США і Великої Британії на початку XXI. Згідно з ними гібридна війна – це "використання воєнних і невоєнних інструментів в інтегрованій кампанії, спрямованій на:

досягнення раптовості, захоплення ініціативи та отримання психологічних переваг для використання в дипломатичних діях;

масштабні і стрімкі інформаційні, електронні і кібернетичні операції;

прикриття воєнних і розвідувальних дій у поєднанні з економічним тиском.

Таким чином, гібридна війна означає підпорядкування певної території за допомогою інформаційних, електронних, кібернетичних операцій у поєднанні з діями збройних сил, спецслужб та економічним тиском, тобто поєднанні воєнних та невоєнних інструментів.

Зрештою усі воєнні конфлікти є гібридними, оскільки протиборство триває із застосуванням усього спектру наявних інструментів.

Мережеві війни. Після того, як внаслідок екстенсивного розвитку інформаційні засоби стали доступними в будь-якому куточку світу, почалася епоха "мережених" війн, що було якісним стрибком у використанні інформаційних інструментів для досягнення воєнно-політичних цілей.

Термін запропонували корпорація RAND на основі застосування ідей і методів ведення війни в кібернетичному просторі для вирішення завдань, які раніше вирішувались за допомогою воєнної сили. Головним мотивом дослідників RAND було зменшення інтенсивності воєнних дій, потрібної для досягнення політичних цілей.

Застосування інструментарію мережевих війн спрямоване на населення противника для його дезорієнтування і зміну світогляду: населення не змушують до підпорядкування, воно само підпорядковується. Усі інструменти працюють на цю мету. Перевагу надають інформаційно-психологічним інструментам.

Винахідники нової війни виокремили два її типи:

перший тип – ненасильницький – боротьба за права людини з метою переходу від авторитаризму до демократії, відкритого суспільства, середовище якого найбільш придатне для зовнішнього впливу;

другий тип – насильницький – боротьба терористичних, етнічних, націоналістичних формувань проти держави, тобто підрив державної влади.

У мережевій війні держава-агресор залучає переважно внутрішні суб'єкти (партії, недержавні організації тощо), але не відкидає і зовнішніх (держав-сателітів, міжнародних терористичних організацій).

Війну назвали мережевою, бо мережа є формою організації множини суб'єктів, яка ґрунтується на *децентралізованому прихованому проникненні* і подальшому впливі на державні структури з метою мінімізації суверенітету суб'єкта-жертви. Мережа охоплює противника зсередини та з усіх боків.

Виховання споживчих настроїв, піднесення споживання в ранг філософії життя створює підґрунтя для підвищення ефективності інформаційно-психологічних впливів. Використовують і корупцію, яка розкладає еліту держави, державну владу і суспільство, розбещує молодь тощо. Спектр інструментів у мережевій війні розширюється необмежено, не відкидаються дії, пов'язані із застосуванням воєнної сили і насильства, зокрема партизанські війни, диверсії, провокації, заколоти тощо.

Різноманіття можливих інструментів призводить до того, що держава-агресор оточує противника великою кількістю нібито не пов'язаних між собою дій: провокацій, дезінформацій, дипломатичних демаршів, дій різноманітних фондів, комітетів, авторитетних лідерів, рухів, телеканалів, Інтернет-сайтів тощо.

Насправді ж дії є добре узгодженими на основі єдиної *стратегічної концепції*. Це збільшує силу впливу за рахунок координації, сприяє забезпеченню раптовості дій і складностіорганізації протидії, оскільки протистояти системним впливам з усіх боків може лише добре інтелектуально підготовлена державницька еліта.

Важливо, що в умовах мережевих війн збройні сили не спроможні діяти ефективно. Вони не мають правових основ та інструментів, адекватних особливостям дій противника. На цей час практично всі держави не має єдиного інституту для протиборства у мережевій війні. На практиці лише РНБ або аналогічні органи координують дії різнорідних державних органів.

Таким чином, головна відмінність мережевих війн полягає у *подрібненні* суб'єкту впливу на кілька суб'єктів, що можуть бути внутрішніми, не обов'язково володіти засобами збройного насильства і розуміти істинні цілі своїх дій.

Класичним прикладом мережевої війни є війна в Лівії (2010 р.), коли як суб'єкти впливу на уряд Каддафі були використані неурядові організації, кочівники, впливові клани, загони спецпризначення, ВПС країн – членів НАТО та їх потужні інформаційні ресурси.

Приватизовані війни. Концепція мережевих війн відображає характер сучасних війн. Втім еволюція способів протиборства триває. Розмивання суб'єкта впливу на противника у мережевій війні все ж не повністю відображає сутність сучасних війн. Що ж змінюється?

Як і в гібридній війні, застосовується весь спектр інструментів впливів. Як і у проксі-війні, впливові держави намагаються не вступати у безпосереднє протиборство, а використовувати підпорядковані сили. Як у мережевій війні, розмивається суб'єкт впливу на противника, використовуються внутрішні суб'єкти. Проте можна виділити нові риси:

через світову фінансово-економічну кризу фінансування підпорядкованих сателітів у значних обсягах стало проблематичним;

поширилася практика застосування тероризму як інструменту досягнення воєнно-політичних цілей (при цьому не відбувається вчинення окремих терактів, а проводяться цілісні терористичні кампанії, створюються терористичні держави як стійкі політичні утворення з ідеологією держави;

майже повністю заблоковано міжнародні інститути, призначені для стримування агресії і вирішення конфліктів, їх перетворено на один з політико-дипломатичних інструментів;

у провідних державах світу поширилася практика формування політичної еліти через делегування представників великих корпорацій, що призводить до витіснення національних інтересів інтересами бізнесу, при цьому бізнес-групи часто залишаються невидимими для покарання;

поширилася практика залучення до участі у конфліктах суб'єктів, які важко ототожнити з державою – приватних військових компаній, незаконних збройних формувань, які керуються приховано і зовсім не переймаються міжнародним гуманітарним правом у власних діях.

Ці риси відображають зміни характеру війни, які й можна назвати "приватизацією війни".

Якщо в мережевій війні розмито структуру суб'єкта впливу на противника, то у приватизованій, крім того, розмито структуру держави-агресора, тобто *справжній агресор* приховує власну суб'єктність, підставляючи замість себе державу. Як

інститут влади держава втрачає виключне право на формування і реалізацію воєнної політики, стаючи сателітом інших сил (недержавних бізнес-об'єднань, олігархату, тощо).

8.2. Гібридна війна як простір невизначеності та інформаційний аспект кризових ситуацій

Гібридна війна як простір невизначеності. Концепція гібридної війни не є чимось абсолютно новим, являючи собою поєднання конвенційних та неконвенційних/нерегулярних методів ведення війни, що виходять за межі поля битв та охоплюють економічні, дипломатичні, інформаційні (у тому числі психологічні, кібер та дезінформаційні) та політичні способи протистояння. Ця концепція ґрунтується на здатності надавати цілеспрямований вплив на віддалені об'єкти та процеси нетрадиційними військовими засобами, особливо на процеси та об'єкти, що є критично важливими для функціонування державних інституцій та збройних сил. Як асиметричний підхід, гібридна війна спрямована на досягнення широкомасштабних наслідків з використанням відповідних засобів, наприклад, перешкоджання військовим операціям противника або запобігання одержанню політичної підтримки населення. В цілому, при гібридних конфліктах має місце координація так званих м'яких дій з використанням більш цілісної стратегії, яка варіює в плані інтенсивності на різних етапах (ініціювання, гостра фаза, рішення) і яка спрямована на дестабілізацію внутрішніх та зовнішніх процесів держави. Кінцевою метою є підрив цієї держави шляхом стимулювання дестабілізації економіки, розчарування та невдоволення населення, міжнаціональні та міжконфесійні конфлікти всередині держави, створення умов для контрольованої та неконтрольованої міграції, придушення цивільного опору та підриву критичної інфраструктури. До цього додається використання певних розвідувальних інструментів, операцій сил особливого призначення, конвенційних збройних сил та нерегулярних комбатантів (терористів, злочинців, найманців, рухів опору, партизанів тощо).

Західно-європейська наукова традиція зосереджена на уявленні про гібридну війну, як вона описана в «Доктрині Герасимова», тобто. як про маскування, проведення операцій нижче за поріг відкритої конвенційної війни при збереженні здатності правдоподібно заперечувати свою участь

Застосування засобів гібридної війни спрямовано на найбільш критичні вразливості у матеріальних системах – комунікаціях, інфраструктурі чи транспорті. Все частіше державні та недержавні актори здійснюють напади на вразливі точки, що існують в соціальних системах, а також використовують соціальне невдоволення існуючих проблем в суспільстві, наприклад, корупції для створення внутрішньополітичної нестабільності в країні. Ці істотні стратегічні слабкості дали можливість більшого успіху тим, хто використовує методи інформаційної чи асиметричної війни.

Інформаційний аспект кризових ситуацій. Кризові ситуації виникають, коли зовнішні сили (агресія та/або природні катастрофи) використовують уразливості та вражають критичні системи в цільовому регіоні або цільовій групі. Ці кризи можуть бути результатом інформаційних чи кібер дій в умовах гібридного конфлікту, результатом здійснення інформаційних, психологічних та кібер загроз (напр. терористичних, військових, дипломатичних, політичних тощо), спрямованих проти критичної інфраструктури держави чи системи управління та командування збройними силами. Втрата чи інтенсивна деградація управлінських функцій систем противника здійснюється до повного збою цільової системи.

Ефективні заходи у кризових ситуаціях у кібер просторі відповідно до досвіду АТО/ООС можуть бути реалізовані при умові:

систематичного розвитку форм, методів та засобів оперативного виявлення, захисту та здійснення активних контрзаходів проти інформаційних загроз у кіберпросторі

наукового дослідження та розвитку потенціалу для розробки спеціального програмного забезпечення та апаратних засобів для інформаційної діяльності у кіберпросторі

розвитку професійної військової освіти та підвищенні кваліфікації, заснованої на бойовому досвіді та практичних кейсах у цій сфері;

проведення, комп'ютерних військових ігор та консультацій на національному та міжнародному рівнях;

удосконалення підготовки та освіти військових та цивільних фахівців у сфері інформаційної та кібер безпеки.

Досвід показує, що ефективне використання методів гібридної війни призводить загалом до непередбачуваних схем криз та реакцій. На практиці гібридна війна не має чітко запрограмованих результатів та послідовності подій, і тому ті, кому доводиться реагувати на таку стратегію, повинні вміти адаптуватися до динамічного та швидко мінливого середовища.

Технологічний дизайн відомих систем контрзаходів у кризових ситуаціях, повинен бути спрямований на формування статично надмірної структури цільової системи. Розподіл завдань між усіма компонентами кібератак на систему часто є рівномірним із вибором компонентів лише відповідно до їх призначення. Збільшення кількості кризових ситуацій призводить до структурної складності систем, створених для реакції на них. Схема розподілу забезпечує інформаційне дублювання даних та призводить до ускладнення їх передачі та обробки. Ті ж принципи лежать в основі проектування програмного забезпечення, призначеного для здійснення процесу оперативного виявлення, захисту та здійснення активних контрзаходів проти інформаційних загроз у кіберпросторі. Згадані підходи не є достатньо ефективними в реальних умовах конфлікту, коли противник застосовує рівні або переважні ресурси для інформаційної війни, за якими слідує використання м'якої сили або кінетичних операцій для досягнення його цілей. Такий підхід є ключовою особливістю сучасних гібридних воєн.

Ретельне застосування принципів ситуаційного управління дає можливість для раціонального розподілу та перерозподілу власних ресурсів та концентрації сил на критичних (для забезпечення безпеки) напрямках дій ворога.

Методи фрактального аналізу, самоорганізації та біфуркаційні моделі дають можливість вчасно виявляти загрози та кризові ситуації, прогнозувати їх розвиток та реальні цілі.

На практиці такий підхід збільшує ефективність контрзаходів проти засобів інформаційної війни внаслідок покращення систем попередження, комплексності та точності інформації та своєчасності реакції.

8.3. Новітні інформаційні та кібер компоненти гібридної війни

На відміну від інформаційних кампаній у минулому, новітні інформаційні технології дають можливість досягати стратегічних цілей неконвенційними та когнітивними ефектами (технології соціального впливу та маніпулювання, кібер сфера, інформаційна зброя, можливості заподіяння істотної шкоди системам управління держави). Такі технології, як соціальні медіа дають можливість зацікавленим акторам дистанційно впливати на всі основні інституції та на інфраструктуру держави. Це стало основою неконвенційних посягань на територію, часто навіть без використання конвенційних військових компонентів. Або їхня присутність уможливила використання організованих і підтримуваних ззовні рухів опору та терористичних рухів, які також можуть сприяти досягненню стратегічної мети створення нестабільності та завданню шкоди інституціям без застосування військового насильства.

Західні вчені називають сучасну гібридну війну хай-тек конфліктом. Це продовження політики держави та/або коаліцій, політичних груп, транснаціональних корпорацій та недержавних акторів. Метою конфлікту є нав'язування волі акторів їх опонентам через інтегровані адаптивні та асиметрично синхронізовані деструктивні засоби впливу на них у багатовимірному просторі та у різних сферах життя. Гібридна війна раціонально поєднує конвенційні та неконвенційні компоненти з упором на використання безлічі джерел та інструментів нападу, синергію результатів та високий рівень невизначеності для опонентів щодо кінцевих стратегічних цілей.

У гібридних конфліктах основними цілями є захоплення контролю над суспільством, здійснення впливу на когнітивну сферу людини, маніпулювання масовою свідомістю, вплив на систему прийняття рішень у державі. Противник намагається вплинути на національні цінності та замінити їх власними цінностями.

Це досягається комплексним, збалансованим здійсненням впливу з використанням м'якої та жорсткої сили. Ось чому критичні елементи систем, тобто об'єкти асиметричних дій у гібридних конфліктах, є важливими для ключових елементів систем державного управління, політичних, дипломатичних, соціальних, технічних, соціотехнічних, енергетичних, фінансових, кібер, інформаційних та інших систем. Вплив на них у межах оптимальних заходів та кореляцій параметрів простору, часу та ресурсів для сторони, що надає цей вплив, призводить до бажаних, цілеспрямованих, швидких, каскадних, синергетичних та деструктивних для цих систем змін (порушень) у їхніх відносинах, структурах, процесах та результатах функціонування. .

Сучасні гібридні війни характеризуються поєднанням класичних тактичних прийомів, що використовуються за підтримки сил, які часто проводять операції в конвенційній манері та посиленим застосуванням нових технологій, що дозволяють більш глибоке проникнення асиметричних дій у критичні елементи та життєво важливі системи управління противника.

Критичними елементами системи є істотні ключові елементи (компоненти, підсистеми) різних систем, що стосуються тріщин, слабких місць у системі. «Натискання» на ці болючі точки може призвести до каскадних, синергетичних, деструктивних системних змін (руйнування) критичних компонентів і пов'язаних з ними систем.

Гібридна війна в Україні. Однією з відмінних характеристик «гібридної війни» в Україні є те, як вона зайняла всі аспекти суспільного життя. При анексії Криму у 2014 році та бойових діях на сході України Росією використовувалося новаторське та високо-технологічне військове обладнання:

електронні військові системи та комплекси та інші види електронних контрзаходів;

сучасні інформаційні та комунікаційні системи;

новаторські системи управління озброєнням;

інтегровані розвідувально-ударні комплекси;

новаторське, у тому числі автоматизоване, програмне забезпечення;

комплекси для ведення інформаційно-психологічних операцій та дій у кіберпросторі;

системи контролю навколишнього середовища та космічні системи;

роботизовані системи (зокрема, комплекси безпілотних літальних апаратів) та контрзаходи.

Інформаційні технології під час гібридної війни існують не сама по собі, а як частина більш широкої та стратегічно спроектованої кампанії з підриву довіри до центральних інституцій.

Початковою метою застосування таких технологій було створення умов для втрати громадянської довіри до уряду України шляхом здійснення інформаційних кампаній, спрямованих на дискредитацію державної влади, керівництва українських збройних сил та заохочення розширення злочинної та сепаратистської діяльності.

Ця стратегія успішно інтегрувала новаторські кібер технології у координації з ретельно спланованими діями неконвенційних та нерегулярних сил на місці, що призвело у 2014 році до анексії Криму та до військового конфлікту на південному сході України. У відповідь на неконвенційні та конвенційні загрози безпеці, як було згадано вище, більшість країн, які мають здібності для швидкого реагування, зосереджуються на двох основних компонентах їхньої безпеки, а саме:

потенціал стримування, що складається з традиційних видів збройних сил (сухопутні сили, військово-повітряні сили, військово-морські сили);

інноваційний військовий потенціал.

Сьогодні інноваційний військовий потенціал включає військове обладнання та особовий склад Сил спеціальних

операцій, інформаційно-психологічні операції та засоби електронної боротьби, а також кібер сили (кібер розвідка, кібер безпека та кібер операції), служби розвідки (електронні засоби розвідки, розвідка з використанням відкритих джерел - OSINT), технічні види розвідки, спостереження та рекогносцирування тощо), комунікацію для оперативного контролю, військові підрозділи, які обладнані роботизованими (безпілотні літальні апарати) комплексами та засобами для протидії відповідним нападам, інші високотехнологічні ресурси.

Концепція гібридної війни описує бойовий вплив на потенційного супротивника з відстані шляхом використання розвідувальної інформаційної підтримки, інформаційної та точної зброї, робототехнічних технологій тощо.

Новітні технології управління, на відміну від прямих бойових дій, дозволяють проведення атак здебільшого проти пріоритетних цілей з максимальною швидкістю та точністю дій, що впливають на «критичні» компоненти на будь-якій частині території держави (регіону) без необхідності фізичної присутності.

Реалізація такої проекції сили дозволяє досягнення стратегічних цілей без подолання традиційних перешкод: часу, відстані та логістики живої сили. Метою такої стратегії є дестабілізація противника та використання його слабкостей у критичних вузлах (підсистемах, компонентах, об'єктах), досягнення ситуації, коли немає необхідності контролювати його територію силою.

Інформаційні та психологічні операції ворога у кібер просторі вимагають використання різних Інтернет ресурсів. Прикладами інформаційних та психологічних операцій є підготовка та розповсюдження конкретної інформації в соціальних мережах та інших Інтернет ресурсах, спрямованої на дискредитацію української влади, командування АТ/ООС та військового складу. Дезінформація, чи неперевірена, фальшива інформація, зокрема з використанням спеціальних технологій підвищення рейтингу таких повідомлень, часто поширюються у національному кібер просторі як військово-патріотичні ресурси. Деякі з цих Інтернет ресурсів мають хостинг у Російській Федерації

Виявлення та ефективна протидія інформаційним та психологічним операціям ворога в кібер просторі вимагають створення національних центрів для контрзаходів проти інформаційних та кібер атак. Національні центри повинні об'єднувати та полегшувати координацію між міжнародними центрами, що забезпечують вжиття контрзаходів проти кібер загроз. Національні центри повинні забезпечувати моніторинг та виявлення деструктивних впливів та ідентифікувати ознаки, механізми (стратегії, тактики, технології, форми та методи) їх реалізації. Вони повинні виявляти джерела та варіанти поширення небезпечного змісту, взаємозв'язок під час операції (дій) між різними Інтернет ресурсами для визначення мети дій та можливих наслідків.

Заходами для нейтралізації деструктивних інформаційних та кібер впливів передусім є:

попередження власників (якщо вони відомі) Інтернет ресурсів про обмеження, що стосуються поширення хибної, недостовірної інформації з рекомендацією про її стирання, якщо ця інформація завдає шкоди суб'єктам та об'єктам національної безпеки (особам, суспільству, державі);

створення громадських регістрів ненадійних/підозрілих ресурсів.

У випадках, коли неможливо визначити господаря чи модератора, а зміст може перетворитися на реальну загрозу для суб'єктів та об'єктів національної безпеки, надається рекомендація заблокувати електронні інформаційні ресурси.

Таким чином, «гібридна війна» є хай-тек конфліктом. Це продовження політики держави та/або коаліцій, політичних груп, транснаціональних корпорацій та недержавних акторів. Метою конфлікту є нав'язування волі акторів їх опонентам через інтегровані адаптивні та асиметрично синхронізовані деструктивні засоби впливу на них у різних сферах життя. Гібридна війна раціонально поєднує конвенційні та неконвенційні компоненти з упором на використання безлічі джерел та режимів нападу, синергію результатів та високий рівень невизначеності для опонентів щодо кінцевих стратегічних цілей.

8.4. Можливості та пріоритети розвитку штучного інтелекту в Україні у контексті гібридної війни

Перетворення гібридної війни (ГВ) на новий вид міждержавного протистояння актуалізує проблему створення засобів підготовки та прийняття рішень на базі штучного інтелекту (ШІ), що дозволяють забезпечити військову, економічну, інформаційну та технологічну перевагу.

Системний підхід дає можливість вивчати та прогнозувати розвиток ГВ як нелінійного об'єкта, що функціонує в умовах невизначеності. Адекватне уявлення про складні феномени ГВ, що постійно змінюються, і технології, засновані на моделюванні та застосуванні ШІ, дозволяють виробляти ефективні стратегії протидії ГВ і враховувати їх у системі забезпечення національної безпеки України.

Згідно тексту «Концепції розвитку штучного інтелекту в Україні», прийнятої розпорядження Кабінету Міністрів України від 2 грудня 2020 р. впровадження інформаційних технологій, частиною яких є технології штучного інтелекту, є невід'ємною складовою розвитку соціально-економічної, науково-технічної, оборонної, правової та іншої діяльності у сферах загальнодержавного значення. А пріоритетними сферами, в яких реалізуються завдання державної політики розвитку галузі штучного інтелекту, є: освіта і професійне навчання, наука, економіка, кібербезпека, інформаційна безпека, оборона, публічне управління, правове регулювання та етика, правосуддя.

Кібербезпека. Основним завданням у сфері кібербезпеки під час реалізації державної політики розвитку галузі штучного інтелекту є захист комунікаційних, інформаційних та технологічних систем, інформаційних технологій, передусім тих, що використовуються операторами (постачальниками) ключових послуг (включаючи об'єкти критичної інфраструктури) і є важливими для безперервності функціонування держави, суспільства та безпеки громадян.

Комплекне розв'язання проблем кібербезпеки вимагає виконання таких завдань:

удосконалення законодавства і створення сучасної нормативно-правової бази для впровадження кращих світових практик штучного інтелекту у сфері кібербезпеки і кіберзахисту;

розроблення інноваційних систем кібербезпеки, які широко застосовують технології штучного інтелекту для автоматичного аналізу та класифікації загроз і автоматичного вибору стратегії їх стримування і запобігання;

вивчення питання ліцензування іноземних розробок штучного інтелекту у сфері кібербезпеки, особливо у державному секторі;

створення національних інформаційних систем, платформ і продуктів з метою зменшення частки іноземного програмного забезпечення у сфері кібербезпеки, що використовується органами державного управління;

оновлення державних стандартів щодо інформаційної безпеки, зокрема державних інформаційних ресурсів, а також розроблення нових національних стандартів у сфері кібербезпеки і кіберзахисту, зокрема організаційних і технічних вимог, що стосуються безпеки додатків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень. Оновлення стандартів та розроблення нових необхідно здійснювати з урахуванням європейських та міжнародних стандартів, зокрема стандартів ISO 27001, ISO/IEC 27032.

Інформаційна безпека. Застосування технологій штучного інтелекту в забезпеченні інформаційної безпеки є одним із факторів, що сприятиме забезпеченню національних інтересів. Зокрема, моніторинг соціальних мереж та інтернет-ресурсів електронних медіа з використанням технологій штучного інтелекту дає можливість виявляти системні тренди і проблематику, діяти на випередження, аналізувати цільову аудиторію.

Для досягнення мети Концепції у зазначеній сфері слід забезпечити виконання таких завдань:

формування і використання інформаційного ресурсу, забезпечення високих темпів його наповнення і заданих критеріїв якості (доступності, достовірності, своєчасності, повноти);

створення захищеного національного інформаційного простору за допомогою технологій штучного інтелекту;

виявлення, запобігання і нейтралізація реальних і потенційних загроз поширення засобами масової інформації культу насильства, жорстокості, порнографії, намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Оборона. Для досягнення мети Концепції у сфері оборони слід забезпечити використання технологій штучного інтелекту у системах:

командування та управління;

озброєння та військової техніки;

збору та аналізу інформації під час ведення бойових дій;

аналізу/розвідки, підтримки проведення розвідувальних заходів, обробки картографічної інформації;

протидії кіберзагрозам у сфері оборони, що базуються на застосуванні технологій штучного інтелекту, у тому числі таких, що дозволяють швидко виявити кібератаки, попереднє сканування та наступне уникнення шкідливих кодів або сканування підозрілих моделей поведінки, а не конкретного коду;

імітаційного та когнітивного моделювання бойової обстановки;

когнітивного аналізу спроможностей військових підрозділів.

Пріоритетні напрями і основні завдання з розвитку технологій штучного інтелекту у сфері оборони визначаються у відповідних документах оборонного планування.

Публічне управління. Для досягнення мети Концепції у сфері публічного управління слід забезпечити виконання таких завдань:

формування переліку адміністративних послуг, рішення за якими приймаються автоматично, за мінімальної участі державних службовців та/або співробітників державних та/або комунальних підприємств, установ, організацій;

дослідження та застосування технологій штучного інтелекту у сфері охорони здоров’я, зокрема щодо протидії

епідеміям та пандеміям, а також прогнозування та попередження потенційних епідемічних спалахів у майбутньому;

запровадження діалогового інтерфейсу для електронних адміністративних послуг із застосуванням технологій штучного інтелекту;

розвиток технологій штучного інтелекту для цифрової ідентифікації та верифікації осіб, у тому числі для надання державних послуг;

застосування технологій штучного інтелекту для проведення аналізу, прогнозування та моделювання розвитку показників ефективності системи публічного управління, окремих галузей економіки під час планування, технічного регулювання та стандартизації;

оптимізація процесів аналізу та оцінки міжнародних інформаційних, політичних, економічних та оборонних трендів для використання таких результатів під час прийняття управлінських рішень у зовнішній та внутрішній політиці України;

застосування технологій штучного інтелекту з метою виявлення випадків неправомірного втручання у діяльність електронної системи державних публічних закупівель та інших державних електронних систем;

застосування технологій штучного інтелекту для виявлення недобросовісної практики в діяльності посадових осіб та державних службовців за різними напрямами шляхом проведення аналізу текстів управлінських рішень та інших даних, які формуються в комп'ютеризованих системах/реєстрах під час провадження такої діяльності.

Крім того, для розв'язання проблем, пов'язаних із функціонуванням державних реєстрів, кадастрів, баз даних, архівів, власником яких є держава, необхідне:

визначення напрямів конвертації даних в електронну форму, створення (у разі відсутності) або актуалізація та очищення наявних державних електронних інформаційних ресурсів;

забезпечення у рамках розвитку відкритих даних пріоритетності оприлюднення динамічних даних;

оприлюднення таких даних у режимі реального часу через прикладний програмний інтерфейс (API);

визначення переліку тематичних категорій наборів даних високої суспільної цінності, розпорядниками яких є органи державної влади. Розроблення та затвердження вимог щодо оприлюднення та періодичності оновлення таких наборів;

розроблення механізмів анонімізації персональних та інших даних під час обробки у системах штучного інтелекту, що унеможливить ідентифікацію осіб.

Багатоагентні мережі – ефективна технологія для вирішення задач безпеки. Згідно з прогнозом американської компанії " Market Research Reports", щорічне зростання до 2025 р. світового ринку систем та засобів ШІ складе близько 14,75%. Створення ШІ, призначеного вирішувати різні завдання, взаємодіяти і адаптуватися до умов ГВ, що змінюються, знаходиться на перетині наукової, технічної та соціально-гуманітарної сфер знання. Вирішення завдання забезпечення безпеки зводиться до створення з взаємодіючих агентів багатоагентних систем де кожен агент володіє частковим уявленням про глобальну проблему і вирішує частину спільного завдання, тому необхідно створити безліч агентів та організувати їх ефективну взаємодію, що дозволяє побудувати багатоагентну систему. У системах безпеки комплекс завдань розподіляється між агентами з присвоєнням кожному ролі, згідно його можливостей.

Для організації процесу розподілу завдань у багатоагентних системах, які працюють у умовах ГВ, створюється система розподіленого вирішення проблеми чи децентралізований ШІ. У першому випадку процес декомпозиції завдання та зворотний процес композиції знайдених рішень відбувається під управлінням єдиного "центру". При цьому багатоагентна система проектується зверху вниз, виходячи з ролей агентів та результатів розбиття завдання на підзавдання. У разі децентралізованого ШІ розподіл завдань відбувається в процесі взаємодії агентів і буде спонтанним, що призведе до появи резонансних, синергетичних ефектів.

Перспективною є модель самонавчального агента, який використовує вилучення знань та машинне навчання. Навчання агентів колективному поведінці – складна проблема, оскільки комплексування завдань передбачає спільне використання знань.

Процесу формування бази знань сценаріїв розвитку обстановки при ГВ за умов високої невизначеності передує оцінка компетенцій експертів та формування експертної бази знань. Це дозволяє працювати з суперечливими знаннями про різні аспекти ГВ та з неповною інформацією, враховувати компетенції експертів та дослідити вплив конкретного експерта на кінцевий висновок.

При формуванні бази знань сценаріїв розвитку обстановки при ГВ в умовах невизначеності з використанням ШІ необхідно враховувати, що роботи в галузі багатоагентних систем вимагають залучення знань і технологій з ряду галузей, які були поза увагою фахівців з ШІ. Це стосується паралельних обчислень, технології відкритої розподіленої обробки, забезпечення безпеки та мобільності агентів.

Поява нових форм агресії обумовлює необхідність створення механізмів нейтралізації негативного впливу зовнішніх втручань та внутрішніх екстремістських дій, захисту національних цінностей та національних інтересів як факторів внутрішньої мобілізації для протистояння зовнішньої агресії та проявам ГВ.

Особлива увага має приділятись випереджальним розробкам, націленим на адаптацію до військових потреб сучасних інформаційних та гуманітарних технологій. Функція держави полягає у підтримці балансу між безпекою та національними інтересами суспільства. Актуальною в цих умовах стає проблематика формування ефективних форми правового регулювання технології ШІ у сфері безпеки в епоху ГВ, що дасть можливість сформувати нову законодавчу базу та сформулювати нові принципи у сфері забезпечення національної безпеки.

ГЛАВА 9. СТРАТЕГІЧНІ КОМУНІКАЦІЇ ТА СТРАТЕГІЧНІ НАРАТИВИ ЯК ІНСТРУМЕНТИ ДОСЯГНЕННЯ ЦІЛЕЙ ПОЛІТИКИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

9.1. Поняття та складові стратегічних комунікацій

Стратегічна комунікація – це термін, який використовується для опису комунікаційних принципів, стратегій та ініціатив, які використовуються для досягнення цілей, місії чи цінностей організації.

Концепція «стратегічної комунікації» (strategic communication, stratcom — СК) з'являється в США на початку XXI століття. 16 березня 2010 року у доповіді Білого Дому Конгресу США «Національні рамки стратегічних комунікацій» визначаються основні цілі, завдання і організаційні форми СК США. У діючої стратегічній концепції НАТО, що була затверджена на саміті в Лісабоні в листопаді 2010 року приводиться наступне визначення стратегічних комунікацій: «...скоординоване і належне використання комунікативних можливостей НАТО: публічної дипломатії, зв'язків з громадськістю, PR-служби ЗС, інформаційних і психологічних операцій для підтримки політики альянсу і заходів, направлених на просування цілей НАТО».

Поняття «стратегічні комунікації» вперше з'являється в українському законодавстві у двох документах: Воєнній доктрині України (2015) та Доктрині інформаційної безпеки України (2017). У цих документах дається однакове визначення стратегічних комунікацій - «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».

Стратегічна комунікація здійснюється в трьох основних формах: зв'язки з громадськістю, публічна дипломатія і інформаційні операції. При цьому, всі складові повинні діяти синхронно, але при цьому мають свої особливості.

Так, зв'язки з громадськістю орієнтовані, перш за все, на інформування зовнішнього реципієнта і повинні в значній мірі відповідати його базовим світоглядним установкам, іншими словами, говорити з ним на одній мові понять і символів.

Істотним доповненням зв'язків з громадськістю повинна стати публічна дипломатія, що включає «зусилля по прямій взаємодії з громадянами, громадськими діячами, журналістами і іншими лідерами громадської думки за межами країни. Публічна дипломатія доповнює традиційну міждержавну дипломатію, в якій переважає офіційна взаємодія професійних дипломатів. Неформальний характер публічної дипломатії значно спрощує процес взаємодії з громадянами іншої держави та формує позитивне відношення до політики і національних інтересів країни, спонукає до дій в їх підтримку.

Третьою формою стратегічної комунікації є інформаційні операції, під якими розуміють «інтегроване використання радіоелектронної війни, комп'ютерних мережевих операцій, психологічних операцій, маніпулювання у військових цілях і оперативної безпеки, включаючи їх супутні і прикладні аспекти, з метою вплинути, зруйнувати, зіпсувати або перехопити процес людського або автоматизованого ухвалення рішення противником».

Військово-наукова група США визначає стратегічну комунікацію як інтерактивний процес і послідовний набір заходів, який включає:

розуміння національної ідентичності, моделей поведінки, національної культури;

розуміння специфіки розвитку національних ЗМІ, сегменту соціальних мереж

надання консультацій особам, які приймають рішення: державним службовцям, дипломатам і військовим лідерам;

сприяння реалізації національних інтересів.

налагодження взаємозв'язку із суб'єктами громадянського суспільства;

вимірювання та моніторинг впливу комунікаційної діяльності.

Стратегічні комунікації виникли як державна, національна концепція набуття впливу в міжнародних

відносинах, як частина військової стратегії США, Великобританії, а відтак і НАТО. Це концепція залучення різних цільових груп у комунікаційну діяльність, що зазвичай реалізується через інструменти зв'язків з громадськістю, некомерційні маркетингові та фінансові комунікації, публічну дипломатію, інформаційні та комунікаційні кампанії.

Таким чином, можна узагальнити поняття, описані вище та викласти їх у такому вигляді.

Стратегічні комунікації — це 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.

Кризові комунікації — комплекс заходів, що реалізуються державними органами України у кризовій ситуації і передбачає їх діалог із цільовою аудиторією з питань, що стосуються кризової ситуації.

Стратегічна комунікація покликана забезпечити політику держави за межами національних кордонів. Основним об'єктом дії є певна цільова аудиторія — політична (економічна, наукова, культурна тощо) еліта тієї держави, відносно якої робляться відповідні дії.

Результатом дії є формування в цільової аудиторії такої системи стійких уявлень про дії іншої держави, які б повністю виправдовували дані дії. Тим самим забезпечується лояльність політичної еліти держави, на яку направлена дана дія, а, отже, і формування дієвої системи геополітичного контролю над заданою територією.

Однією з актуальних завдань системи стратегічних комунікацій є створення та підтримка позитивного іміджу структурам сектору безпеки та оборони України.

Впливовими психологічними технологіями для формування іміджу силових відомств є наступні:

формування образу героя-військовослужбовця;

зміна асоціативного ряду, що визначає сприйняття органів структури сектору безпеки та оборони України в масовій свідомості;

позиціонування в інформаційному просторі позитивних новин про діяльність органів структури сектору безпеки та оборони.

9.2. Стратегічні наративи як інструмент досягнення цілей політики національної безпеки

Сутність стратегічних наративів. У сучасному світі актуальним предметом дослідження, не тільки для гуманітарних наук, а й теорії безпеки, стає концепція стратегічного наративу. У широкому значенні стратегічний наратив є «засіб, за допомогою якого політичні актори намагаються сконструювати спільне бачення минулого, теперішнього і майбутнього міжнародної політики і політики безпеки з метою формування бажаної поведінки з боку внутрішніх і міжнародних акторів».

У Доктрині інформаційної безпеки України, прийнятої Указом Президента України від 25 грудня 2017 року та Стратегії інформаційної безпеки 2021 року дається дається таке визначення поняття *«стратегічний наратив»* - це спеціально підготовлений текст, призначений для вербального викладення у процесі стратегічних комунікацій з метою інформаційного впливу на цільову аудиторію.

Стратегічний наратив створює рамки, призначені для того, щоб люди мали можливість розуміти значення подій, що відбуваються в світі. У тому випадку, якщо суб'єктом комунікації є держава, стратегічний наратив включає в себе історії/оповідання, що розповідаються від імені держави та спрямовані на досягнення певних національних цілей, вони впливають на позитивне сприйняття громадськістю діяльності держави щодо забезпечення національної безпеки та реалізації національних інтересів, а також формують уявлення про функціонування інститутів держави.

У вузькому значенні, стратегічний наратив можна визначити як сукупність взаємопов'язаних історій, які формують певні образи минулого, сьогодення і майбутнього, що призначені для управління сприйняттям цільових аудиторій. Важлива ознака стратегічного наративу полягає в тому, що він являє собою когнітивний продукт, сконструйований для

досягнення стратегічних цілей. При цьому стратегічний наратив звертається не тільки і не стільки до логіки, скільки до емоцій, цінностей, архетипів культури, міфів та історичних аналогій. Сила стратегічних наративів полягає в їх здатності мобілізувати цільові аудиторії для досягнення цілей політики національної безпеки, навіть при нестачі фінансових, матеріальних або військових ресурсів.

Стратегічний наратив — це ефективний спосіб для слабшого гравця отримати конкурентну перевагу над сильним: «слабкі м'язи, зате відмінні історії». Таким чином, концепція стратегічного наративу дає можливість розкрити процес формування, поширення і проектування ідей в міжнародній політиці та політиці безпеки.

Особливу роль стратегічні наративи грають в сучасному глобальному інформаційному суспільстві, яке характеризується швидким поширенням цифрових технологій. Вони стають набагато більш гнучкими інструментами, ніж, наприклад, ідеологічна доктрина, і, таким чином, можуть стати ефективним механізмом просування інтересів суб'єкта стратегічних комунікації в диференційованому глобальному інформаційному просторі.

Таким чином, стратегічний наратив є складового стратегічних комунікацій та має пряму кореляцію із стратегічними завдання держави у сфері національної безпеки.

Здатність геополітичних суб'єктів використовувати наративи в стратегічних цілях політики національної безпеки перетворює їх на зброю, що володіє великою потужністю. Протягом усієї світової історії релігійні лідери, філософи, політики розглядали наративи в якості потужного інструменту, що змінює переконання і поведінку аудиторії. Якщо, під впливом ворожих наративів, великі соціальні групи і суспільство в цілому перестають довіряти національним наративам, духовним і політичним лідерам, ЗМІ, вченим і моральним авторитетам, то наслідком стане загроза, що прирівнюється до ефекту традиційної війни. Історія показує, що протиборство наративів є природним контекстом світової історії і може привести до реальних війн, перемогу в яких бере той, що в змозі створити і розповісти найбільш переконливі історії.

У 1993 р. Джон Аркілла і Девід Ронфелдт в статті «Cyberwar Is Coming!» передбачили застосування мережі і програмного забезпечення в якості військового інструменту. Більш того, вони заявили, що не тільки військові, але все суспільство незабаром зіткнеться з так званої «мережевою війною» (netwar). Вести військові дії в мережевий війні «означає намагатися зруйнувати, пошкодити, або змінити те, що цільова група населення «знає» або думає, що знає». Виграє в мережевий війні той, «чия історія перемагає». Іншими словами, вже в 1993 р. американські дослідники передбачили, що у майбутніх війнах центральну роль будуть мати наративи, що створять середовище, у якому «виклики ідентичності сприймаються як екзистенційні загрози».

Смислова війна, що ведеться проти суспільства противника з застосуванням наративів, може привести до розмивання національної ідентичності і втрати національної «території смислів». У населення країни — жертви військової агресії відбувається повна втрата орієнтації в системі координат «свій — чужий». Замість того щоб об'єднатися перед обличчям зовнішньої агресії, частина населення вступає в боротьбу проти іншої частини свого народу. Агресор при цьому виступає в ролі «захисника» однієї зі сторін внутрішнього конфлікту, їм же спровокованого. Швейцарський історик Яків Бурхард назвав дане явище «жахливими спрощеннями», використовуваними авантюристами і демагогами для досягнення влади, спираючись на фрустрації і стреси в суспільстві.

Соціальні інститути, не витримуючи негативного інформаційного впливу зазнають тиску та стають неефективними або навіть дисфункціональними, національна культура фрагментується. Народи, що визначають свою ідентичність насамперед через національну державу, відступають до міфічного націоналізму «золотого століття», в той час як ті, хто в якості пріоритету вибирають культурні та релігійні кордони, відступають до культурного і релігійного фундаменталізму.

Пропонуючи спрощений погляд на все більш і більш складний світ, наратив, який використовується в якості зброї дає людині і суспільству емоційну впевненість, що спирається на

ясне, раціональне розуміння того, що відбувається. В руках професіоналів сильні емоції гніву і страху, вписані в войовничі наративи, стають унікальною формою м'якої сили, здатної впливати на поведінку противника, обмежити і зруйнувати функціональні можливості його соціальних інститутів і систем. При цьому істинність інформації грає другорядну роль. В епоху постмодерну правда не завжди перемагає, коли стикається з ворожими наративами.

Масовість і інтенсивність когнітивної атаки — це одна з умов застосування наративів в якості зброї, це залишає суспільству, яке атакується, мало часу на реагування та протидію. І з часом, якщо система національної безпеки не здійснює протидію ворожим впливам, виклики, що спровоковані дією ворожих наративів переростають у загрози національній безпеці, що характеризуються довгостроковими і глибокими наслідками. Застосування таких наративів як зброї у гібридній війні є ознакою сучасного світу в XXI столітті. Це потребує перегляду класичних понять теорії безпеки епохи модерну, плюралістичних концепцій істини постмодерну та розробки нових концепцій забезпечення безпеки у епоху метамодерну. Наратив епохи метамодерну — це єдиний потік сенсів, де кожна одиниця істини важлива та самодостатня. Де медіа і інтернет-технології в цілому виступають єдиним середовищем для взаємодії не тільки окремих людей, а й інститутів, де рівноправні масова та елітарна культура, диктатура та демократія тощо.

Наративи завжди складали невід'ємну частину війни і країни-противники прагнуть виглядати справедливими і моральними в очах власного населення та міжнародної спільноти. Наратив держави, що перемогла у війні, зміцнюється, коли переможці починають писати національну історію. Якщо війна не закінчується однозначною перемогою однієї зі сторін, виживають обидва наративу. Наратив держави, що програла вимирає або виживає і відновившись, може викликати новий військовий конфлікт.

Наратив, що використовується для реалізації цілей політики національної безпеки комбінує у себе досягнення

когнітивної науки, нейробіології, теорії комунікацій, інформаційних технологій.

У нової стратегі національної безпеки Російської Федерації, прийнятої 2 липня 2021 року захисту традиційних духовно-моральних цінностей, культури та історичної пам'яті присвячено цілий розділ. Російська держава стурбована тим, що руйнується її «культурний суверенітет» та насаджуються чужинні цінності, на думку авторів Стратегії це підриває фундамент політичної стабільності та державності. При цьому, РФ веде гібридну війну проти України з використанням саме смислової зброї, здійснює агресивний інформаційно-психологічний вплив на свідомість громадян України, просуває цінності «русского мира». У цієї смисловій війні вона використовує радянські наративи за всіма правилами інформаційних та смислових війн.

Чинники ефективності наративів. В сучасних міждисциплінарних дослідженнях виділяють шість чинників, які роблять наративи настільки ефективними: векторність, вразливість, вірулентність, розмах, швидкість і синергетичність

Векторність — здатність контенту поширюватися в інформаційному середовищі з глобальним «радіусом ураження». Якщо фізична зброя вимагає систем доставки і потужної логістики, інформація поширюється, копіюється і розмножується практично без обмежень.

Уразливість — здатність ворожих наративів через організацію серії послідовних когнітивних атак долати опір традиційних наративів суспільства. Процес, аналогічний тому, як стреси, хвороботворні мікроби і віруси можуть знижувати імунітет організму, в кінцевому рахунку, приводячи до хвороби та навіть смерті живого організму.

Вірулентність — здатність відобразити факт того, що знання когнітивних недоліків і вразливих місць наративів суспільства, дозволяє розробити способи когнітивних атак, яким важко протидіяти.

Розмах — здатність залучати велику кількість акторів до організації атак на когнітивний домен суспільства. Низька вартість таких акторів в інформаційному середовищі дозволяє

організувати атаки, в яких беруть участь мільйони користувачів і мережі ботів.

Швидкість — здатність до проведення інтенсивних когнітивних атак в інформаційному середовищі. Перекручена і маніпулятивна інформація може наповнити когнітивний домен суспільства, що атакується протягом хвилин, та навіть секунд та набути вірусний характер. Ця інформація впровадить у когнітивний простір країни-жертви потрібні країні-замовнику ідеї, смисли і значення.

Синергетичність — здатність до кумулятивного ефекту, коли всі перераховані вище фактори, що застосовуються разом або в тій чи іншій послідовності, можуть бути використані таким чином, щоб досягти синергетичного ефекту, якісно підсилює дію кожного з них.

Таке ефективне та широке застосування наративів в якості зброї можливо тільки на умовах системності підходу до процесу їх створення і використання. Однією з фундаментальних причин такого підходу є безпрецедентна складність сучасних інформаційних потоків та прискорене зростання обсягів і швидкості обміну контентом в інформаційній сфері.

Таким чином, стратегічні наративи для досягнення цілей політики національної безпеки стають ефективною когнітивною зброєю, їх використовують для досягнення тактичних цілей як частина військового або геополітичного конфлікту, або стратегічних цілей, як спосіб послабити, нейтралізувати державу або систему національної безпеки іншої держави. Будучи успішно застосованими, такі наративи полегшують застосування збройних сил для досягнення політичних і військових цілей.

9.3. Інфодемія як результат неефективних стратегічних комунікацій, її наслідки та інструменти протидії

Інфодемія як соціальне явище. Вперше термін «Інфодемія» вжив гендиректор ВООЗ Тедрос Адганом Гебреєсус у лютому 2020 року. *Інфодемія* – інформаційна епідемія, що характеризується швидким поширенням неточної

і/або брехливої (маніпулятивної) інформації через ЗМІ, соціальні мережі про пандемією COVID-19 у вигляді чуток, плиток, думок псевдоекспертів тощо.

Інфодемія характеризується відсутністю колективного інформаційного імунітету (критичного мислення) у більшості населення. Всесвітня організація охорони здоров'я (ВООЗ) попереджає, що «інформаційна епідемія», поширюється швидше, ніж вірусна.

В умовах криз різного характеру діяльність державних структур повинна бути спрямована на посилення зв'язків з існуючими соціально-орієнтованими комунікаційними мережами для інформування, захисту та мобілізації населення. Це може стати життєво важливим для зміни поведінки населення з метою зниження розповсюдження вірусу при пандемії і надання людям належного лікування на дому.

Налагодження системи стратегічних комунікацій під час пандемій COVID-19 повинно було відбуватися з метою підвищення рівня обізнаності та формування конвергентних повідомлень про методи і способів профілактики і лікування населення від короновіруса.

Результатом ефективних стратегічних комунікацій під час пандемії повинно стати:

переконання населення у підконтрольності ситуації діям влади з метою схвалювання суспільством державних рішень та вплив на масову поведінку задля її корекції;

міжвідомча комунікація задля координації дій у процесі здійснення державної влади під час пандемії;

деконфліктизація суспільства та зняття психологічної напруги у населення.

Причини виникнення інфодемії та її «симптоми». Серед основних причин виникнення інфодемії виокремлюють наступні.

1. *Кризові ситуації* (стихійні лиха, аварії, терористичні атаки, епідемії, пандемії). Це ситуації високої невизначеності, які в свою чергу породжує тривогу та страх. В умовах кризи, коли людина про щось не знає або не може знайти необхідну інформацію, виникає інформаційна порожнеча, яка в свою чергу породжує невпевненість у майбутньому та живить тривогу. Це

змушує людину шукати способи подолання невизначеності та зменшення тривоги через пошук інформації про загрозу. Люди намагаються зрозуміти загрозливу ситуацію та відповісти на питання: *що ми повинні робити*?

Відбувається колективне осмислення вхідної інформації, її збір, додумування, обмін з рідними, друзями, колегами. Саме у цей період з'являються чутки, плітки. Дезінформація небезпечна, оскільки змушує людей приймати неправильні рішення, в тому числі рішення, що загрожують життю людини та її оточення. Ця проблема посилюється, коли громадяни втрачають довіру до офіційних джерел (уряду, ЗМІ).

2. *Відсутність інформаційної стійкості* (резилетності) до інформаційних вірусів. Низькій інформаційний імунітет населення. Дослідники з Університету Східної Англії (UEA) виявили, що дезінформація під час епідемій інфекційних захворювань може зробити їх спалахи серйознішими.

3. *Неефективна системи стратегічних комунікацій* в країні, наслідком якої стала недовіра населення до офіційних джерел інформації.

Найбільш поширені «симптоми» інфодемії є:

продукування вигаданих «теорій змов» про походження вірусу;

поширення відомостей про фейкові методи лікування;

поширення дезінформації про реальний стан справ з рівнем захворювання;

недостовірна інформація про методи профілактики;

надання екстремального емоційного забарвлення існуючої достовірної інформації.

Фактчекінговий український ресурс «По той бік новин» у березні 2020 року сформував список «експертів», яким вірять українці під час пандемії COVID-19 (за кількістю лайків, репостів та переглядів у Інтернеті):

шкільні чати у Вайбері;

молодий лікар Юра Клімов;

медсестра з Італії;

секретна служба НАЗУ;

українка, яка вижила у Вухані;

таємна розсилка МОЗ;

лікар-вірусолог зі США;

екскурсовод з дипломом вірусолога з Італії;

дзвонили з аеродрому, військової частини, шпиталя, МНС...;

астролог передбачив;

брат, який працює в СБУ;

засідання вченої ради Далекосхідного університету;

лікарка з Тенеріфе.

Академія охорони здоров'я Товариства зв'язків з громадськістю США (PRSA Health Academy) розробила інструкцію для боротьби з інфодемією. Її зміст полягає у наступному:

фокусуйся на фактах (факт — це не думка друзів, не чутки з інтернету, не он-лайнові теорії, не суперечливі новини, не соцмедіа і не політичні спічі. Від фактів і думок експертів, яким можна довіряти, залежить ваше життя і здоров'я);

використовуй два джерела, що заслуговують на довіру, коли оновлюєте інформацію (МОЗ і ЦГЗ МОЗ і ВООЗ);

оновлюй інформацію тричі на день (ситуація змінюється швидко, будьте пильні щодо неточної інформації або брехні).

Правила інформаційної гігієни під час інфодемії.

1. *Коли шукаєш та аналізуєш інформацію думай повільно*! Не панікуй, не реагуй швидко, особливо якщо не впевнений у правдивості інформації. Річ у тому, що у людини є два типи мислення: інстинктивне та критичне. Інстинктивне мислення залишилося у людини з первісних часів, це тип мислення швидкий на реакцію. Це автоматична реакція організму на подразник. *Критичне мислення* — це повільне мислення, ретельне осмислення того, що ми бачимо. До висновків у вигляді власного судження нас приводить сумнів, роздум, аналіз, фактчекінг. На це потрібен час.

2. *Не підживлюй паніку*. Не будь сам джерелом її розповсюдження. Не перепощувай інформацію з сумнівних джерел.

3. *Не пиши емоційні пости в соціальних мережах*.

4. *Не слухай псевдоекспертів*.

5. *Слідкуй за офіційною інформацією* (МОЗ, ВОЗ).

6. *Обмеж кількість вхідної інформації*. Визначте два-три перевірених джерела (ЗМІ, журналісти, експерти) та слідкуйте за інформацією від них.

7. Проводь роз'яснювальну роботу серед груп ризику, пояснюй ризики інфодемії.

Наслідки інфодемії для України та інструменти протидії. Наслідками інфодемії під час пандемій COVID-19 в Україні стали наступні явища.

1. *Паніка, поява конспірологічних теорій.* Конспірологічні теорії, плітки та зловмисне дезінформування може швидко набути вірусного поширення в соціальних мережах, особливо за низького рівня довіри громадськості до державних інституцій.

У березні 2021 було оприлюднено результати дослідження, що проводилося в Україні на замовлення Програми розвитку Організації Об'єднаних Націй (ПРООН) та Дитячого фонду Організації Об'єднаних Націй (ЮНІСЕФ). Його мета визначити як інфодемія дезінформації про COVID-19 шкодить здоров'ю українців. Дослідження дає уявлення про поширення дезінформації у період пандемії, про основні теми вигаданих наративів, а також пропонує рекомендації для уряду, фактчекерів, лідерів думок і громадськості.

Впродовж 9 місяців (з березня до листопада 2020 року) дослідники, використовуючи передову платформу для моніторингу й аналізу соціальних медіа SemanticForce , відслідкували понад 30 мільйонів повідомлень пов'язаних з тематикою COVID-19 у соціальних медіа. У процесі дослідження було виявлено 250 000 повідомлень дезінформаційного характеру, пов'язаних із COVID-19, в українських онлайн ЗМІ, блогах, форумах, соціальних мережах та месенджерах.

Виявлені дезінформаційні наративи включають маніпулятивну та відверто неправдиву інформацію щодо носіння масок, конспірологічні теорії про походження та навіть сам факт існування новітнього коронавірусу та хвороби COVID-19, брехливі чутки щодо ефективності тестування на коронавірус і вакцинації, та іншу недостовірну інформацію щодо COVID-19.

Паралельно з моніторингом соціальних медіа в межах дослідження було опитано 1000 українців для вивчення громадської думки щодо пандемії. Серед результатів опитування — приблизно третина українців вважають, що їхні шанси заразитися новітнім коронавірусом низькі. Трійку лідерів джерел, яким надають перевагу громадяни, посідають соціальні медіа (42 %), телебачення (26 %) та лікарі й медики (24 відсотки). Незважаючи на це, українці зауважили, що джерела, яким вони найбільше довіряють, — це їхні лікарі та медики (39 %) і лікарі та спеціалісти у сфері охорони здоров'я (через ЗМІ) (29 %), тоді як лише 27 % довіряють соціальним медіа як джерелу надійної інформації.

Лотта Сильвандер, Голова представництва ЮНІСЕФ в Україні, наголосила, що ризики недостовірної інформації нині як ніколи високі. «Інфодемія загрожує посиленням сумнівів щодо вакцинації, що зі свого боку може ускладнити впровадження нових вакцин та підірвати довіру громадськості до системи охорони здоров'я», — сказала Сильвандер. «У час, коли пандемія продовжує викликати непевність і страх, існує гостра необхідність у більш рішучих діях і скоординованому підході до спростування брехливих новин і дезінформації», — додала вона. «Без належного рівня довіри та достовірної інформації кампанії з імунізації не досягнуть своєї мети, а вірус далі процвітатиме».

Основні висновки, до яких прийшли фахівці у результаті дослідження полягають у тому, що неконтрольована інфодемія:

знижує готовність населення дотримуватися настанов у сфері громадського здоров'я (носіння масок, дотримання фізичної дистанції тощо);

зменшує ймовірність того, люди радитимуть вакцинуватися найбільш уразливим особам зі свого кола спілкування;

здатна значною мірою підвищити рівень захворювання на COVID-19.

У дослідженні запропоновано низку рекомендацій для українського уряду, ЗМІ та соціальних медійних платформ щодо боротьби з інфодемією COVID-19, а саме:

створити Командний центр з питань COVID-19, щоб координувати ключові групи (уряд, громадські організації, організації фактчекерів, ЗМІ, лідери думок). Для подолання високого рівня недовіри до уряду йому потрібно систематично залучати лідерів думок із різних галузей для поширення меседжів щодо громадського здоров'я, йдеться у дослідженні;

використовувати гумору, щоб збільшити охоплення важливої інформації про громадське здоров'я, підтримка організацій фактчекерів грантами, медіапартнерств і спеціальних розділів на вебсайтах, а також заохочення соціальних мереж налаштовувати свої алгоритми так, щоб вони вловлювали дезінформацію та обмежували її появу в новинних стрічках користувачів.

2. *Пошук ворогів та винних.* Страх, який виникає у людини в умовах кризи, легко пояснити не раціональними фактами, а теоріями змови, конспірологією. На складні питання люди знаходять легкі відповіді. Все це призводить до того, що люди починають шукати «винних» і дуже часто ними стають «чужаки». У багатьох країнах світу дезінформація про коронавірус підживила старі забобони щодо азіатів і породила ксенофобію і расизм. Прикладом можуть бути події у Нових Санжарах (Полтавська область), де протестувальники хотіли перешкодити евакуйованим з китайського міста Ухань українцям та іноземним громадянам потрапити до медичного центру.

3. *Громадянська сепарація.* Інфодемія створює паніку і плутанину, а також роз'єднує людей у той час, коли солідарність і колаборація критично важливі для порятунку життя людей і подолання кризи.

4. *Недовіра до органів державної влади.*

5. *Ріст злочинності.* За перші декілька місяців з початку карантину через коронавірус Департамент кіберполіції Національної поліції України виявив:

170 випадків поширення дезінформації про коронавірус на інформаційних ресурсах;

79 осіб, які поширювали фейки про коронавірус, із них — 4 інтернет-агітатори, які діяли за завданням російської сторони;

28 осіб вже притягнуті до адміністративної відповідальності за ст. 173-1 (поширення неправдивих чуток, що можуть викликати паніку серед населення або порушення громадського порядку) КУпАП;

139 випадків шахрайства під час купівлі засобів індивідуального захисту.

Кіберфахівці СБУ заблокували поширення фейкового контенту у понад 1 тисячі інтернет-спільнот, що загалом мають понад 500 тисяч дописувачів.

Тривожним показником стану стратегічних комунікацій в українському суспільстві стали результати дослідження Центру Контент-аналізу дописів громадян України про короновірус у соціальних мережах, яке було проведено у березні 2020 року, а саме:

кількість українських користувачів соцмереж, охоплених панічними настроями, постійно зростає;

половина джерел інформації про коронавірус, цитованих у соцмережах — ненадійні;

як панічні, так і надміру оптимістичні дописи переважно посилаються на фейкові та маніпулятивні дані, серед конструктивних постів частка фейків набагато менша;

найчастіше жертвами маніпуляцій щодо короновірусу стають жінки, які раніше не цікавилися політикою;

підтримка дій влади дуже низька, що, ймовірно, пояснюється традиційною недовірою до неї;

РФ активно продукують фейки про відсутність небезпеки від вірусу та теорії змови про його штучне походження у лабораторіях НАТО або Китаю.

Таким чином, можна констатувати фак того, що інфодемія становить реальну загрозу громадському здоров'ю в Україні і українському уряду важливо об'єднати зусилля з ЗМІ, громадськими організаціями, фактчекерами та лідерами думок у соціальних медіа щодо протидії її проявам. Так можна стимулювати поширення достовірної інформації та подолати небезпеку дезінформації про COVID-19.

Таким чином, можемо дійти таких загальних висновків.

1. Стратегічне інформаційне протистояння нині становить небезпечний компонент гібридної війни, розгорнутої Росією

проти України, причому головною загрозою інформаційній безпеці України сьогодні залишається загроза негативного впливу на інформаційну інфраструктуру, інформаційні ресурси, на суспільство, свідомість і підсвідомість особистості з метою нав'язати власну систему цінностей, поглядів, інтересів і прийняття управлінських рішень органами державної влади у життєво важливих сферах суспільного життя.

2. Цілями реалізації стратегічних комунікацій є налагодження дієвої та ефективної координації між всіма структурами систем національної безпеки держави, просування загальнодержавного наративу, формулювання і впровадження ключових повідомлень для підвищення розуміння суспільством діяльності складових сектору безпеки і оборони України. Вкрай важливо надалі залишається завдання інституалізації, нормативного закріплення стратегічних комунікацій у секторі безпеки і оборони України та розбудова відповідної навчально-методичної бази у цій сфері.

3. Стратегічні наративи є тими інструментами, за допомоги яких національні держави, корпорації, громадські та партійні структури тощо артикулюють свої інтереси, цінності та аспірації.

4. Переважаючий напрям світового культурно-інформаційного розвитку у певній сфері (політичній, економічній, науковій, медійній тощо), характерний для певного періоду часу, формується за посередництва наративів за допомоги панівних медіа (mainstream media — MSM), які використовують передусім наративи для реалізації:

фреймінгу (framing) — ситуація, коли ми приділяємо увагу тому, що в рамці, і ігноруємо те, що поза рамкою;

праймінгу (priming) — «окреслення пріоритетів» — теорія, згідно з якою активація за допомогою медіа однієї думки у споживача інформації може викликати пов'язані з нею думки;

встановлення «порядку денного» (agenda setting).

Інфодемія — ще один складний виклик, який виник у зв'язку з пандемією COVID-19. Це швидке поширення неточної і/або брехливої інформації, або ж засилля незрозумілих наукових чи медичних термінів, які нефахівцям складно зрозуміти.

Запитання та завдання для самоконтролю

Які переваги надає автоматизація процесів прийняття рішень?

Які передумови та складники автоматизації процесів прийняття рішень?

Розкрийте зміст компонентів інформаційної системи управління та її функцій

Які програмні продукти належать до проблемно-орієнтованих пакетів прикладних програм?

За якими ознаками класифікують інформаційні системи?

Які типи інформаційних систем виділяють на різних рівнях управління та які завдання вони виконують?

Яка мета інформаційних систем підтримки прийняття рішень та які компоненти її утворюють?

Дайте загальну характеристику підходів щодо класифікації систем підтримки прийняття рішень

Які технології аналітичного моделювання використовують для підтримки прийняття управлінських рішень?

Опишіть функціональні елементи базової моделі інформаційного супроводження управлінських рішень у сфері національної безпеки

Чому ситуаційні центри є важливим інструментом аналітичного забезпечення у сфері національної безпеки?

Дайте загальну характеристику воєнно-політичних конфліктів XXI ст.

Яку роль відіграє інформація в сучасних проксі-війнах?

Яку роль відіграє інформація в сучасних гібридних війнах ?

Яку роль відіграє інформація в сучасних мережевих війнах ?

Яку роль відіграє інформація в сучасних приватизованих війнах?

Дайте загальну характеристику гібридної війни як простору невизначеності

Які чинники зумовлюють маніпулятивний дискурс гібридної війни?

Чому вчені називають сучасну гібридну війну хай-тек конфліктом?

Чому паралельний світ (паралельна реальність) є одним із механізмів гібридної війни?

Розкрийте зміст поняття «стратегічні комунікації» та їх складових

Які особливості необхідно враховувати при виборі цільової аудиторії в комунікативних стратегіях?

Які основані чинники впливають на вибір ефективної комунікативної стратегії?

Розкрийте зміст етапів впровадження комунікативної стратегії

Розкрийте складові алгоритму стратегічних комунікації як інструменту подолання гібридних загроз.

Які чинники зумовлюють можливості стратегічних комунікацій у генеруванні кризових ситуацій?

Назвіть шість чинників, які роблять наративи ефективним інструментом комунікації.

Якими джерелами користуватися для перевірки інформації щоб не стати жертвою інфодемії?

Що може стати результатом інфодемії в українському суспільстві і які є інструменти протидії?

Чому інфодемія є результатом неефективних стратегічних комунікацій в умовах криз?

Список рекомендованої літератури

1. Бухтатий О. Публічні комунікації демократичної держави: монографія. Дніпро: Журфонд, 2018. 297 с.

2. Доронін І.М. Національна безпека України в інформаційну епоху: теоретико-правове дослідження. Дис…докт. юрид. наук: 12.00.01; Наук.-досл. інст. інформ. і права, Нац. акад. прав. наук України. Київ. 2020.539 с.

3. Драгомирецка Н.М. Сучасні тенденції комунікацій у сучасному світі. *Публічне урядування* : збірник. 2015. N 1. Київ: ДП «Видавничий дім «Персонал», 2015. С. 85-97.

4. Драгомирецька Н.М., Кандагура К.С., Букач А.В. Комунікативна діяльність в державному управлінні: навч. посібник. Одеса: ОРІДУ НАДУ, 2017. 180 с.

5. Дрешпак В.М. Комунікації в публічному управлінні: навч. пос. Д. : ДРІДУ НАДУ, 2015. 168 с.

6. Глобальна та національна безпека: підручник / авт.кол.: В.І. Абрамов, Г.П. Ситник, В.Ф. Смолянюк та інш.; за заг.ред. Г.П. Ситника. К.: НАДУ, 2016. 784 с.

7. Глобалізаційні виклики сучасності: підручник /авт.кол.Л.Г. Комаха, І.В. Алексеєнко, В.Л. Гура та ін.; за заг.ред. Л.Г.Комахи.- К.: ВПЦ "Київський університет", 2022. 350 с.

8. Гнатенко В. Застосування інформаційно-комунікаційних технологій у забезпеченні економічної безпеки держави // *Літопис Волині*. *Всеукраїнський науковий часопис*. №. 22. 2020. С.88-92

9. Інформаційна складова державної політики та управління : монографія / Соловйов С.Г., та ін. ; заг. ред. Грицяк Н.В. ; НАДУ. К.: К.І.С., 2015. 320 с.

10. Комунікаційна стратегія МЗС/ Стратегія публічної дипломатії МЗС. URL: https://mfa.gov.ua/pro-ministerstvo/strategiyi-mzs

11. Клубань О.М., Курбан О.В., Любовець Г.В., Король В.Г., Савчук Р.П. Сучасні комунікаційно-контентні процеси в безпековій сфері:навч. посібник. Київ: ВІКНУ, 2016. 170 с.

12. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі: навч. посібник. К.: ВІКНУ, 2016. 286 с.

13. Литвиненко О.В. Спеціальні інформаційні операції та пропагандистські кампанії: Монографія. Київ: ВКФ “Сатсанта”, 2000. 222 с.

14. Магда Є. Гібридна війна: вижити і перемогти. — Х.: Віват, 2015. — 304 с. URL: https://balka-book.com/files/2017/06_10/12_24/u_files_store_6_68818.pdf?srsltid=AfmBOorDASEhRocy-Y6APos3RX8bB3HABSKT039uIUnbgUBazMrWnANp

15. Ніколаєнко Н.О. Інформаційна безпека та політична комунікація: навч.-метод. посібник. Миколаїв: НУК, 2022. 121 с.

16. Основи стратегічних комунікацій у сфері забезпечення національної безпеки та оборони: навч. Посіб. К.: НУОУ імені Івана Черняховського, 2020 86 с.

17. Основи теорії управління у сфері національної безпеки: курс лекцій / Г.П. Ситник. К: ТОВ "САК Лтд.", 2023. 174 с.

18. Островська Н.В. Прикладні соціально-комунікаційні технології: навч. посібник. Запоріжжя. ЗНТУ, 2017. 110 с.

19. Пацурія Н. Упровадження технологій штучного інтелекту в забезпечення національної безпеки та обороноздатності України: правові проблеми і перспективи повоєнного періоду// *Теорія і практика інтелектуальної власності* . №3.2023. С.68-78

20. Почепцов Г. Г. Від покемонів до гібридних війн: нові комунікативні технології XXI століття. Київ: Києво-Могилянська академія, 2017. 260 с.

21. Практичний посібник для працівників комунікаційних структур в органах влади. 2016. URL: https://imi.org.ua/wp-content/uploads/2017/06/posibnyk.pdf

22. Про доступ до публічної інформації: закон України від 13.01.2011 № 2939-VI. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi

23. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi

24. Про затвердження Комунікаційної стратегії Державного комітету телебачення і радіомовлення України на 2022-2023 роки № 526 URL: https://zakon.rada.gov.ua/rada/show/v0526603-21#Text

25. Публічне управління та адміністрування у сфері національної безпеки: (системні, політичні та економічні аспекти): словник-довідник / С.П. Завгородня, М.Г. Орел, Г.П. Ситник [уклад.] /за заг.ред. Д.В. Неліпи, Є.О. Романенка, Г.П. Ситника. Київ: Видавець Кравченко Я.О., 2020. 380 с.

26. Світова гібридна війна: український фронт / За заг. ред. В.П. Горбуліна. Національний інститут стратегічних досліджень. – К.: НІСД, 2017. URL: http://resource.history.org.ua/item/0013707

27. Стратегічні комунікації в умовах гібридної війни: погляд від волонтера до науковця : монографія. К. : НА СБ України, 2018. 517 с.

28. Стратегія інформаційної безпеки. Указ Президент України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

29. Термінологічний довідник НАТО зі стратегічних комунікацій / І. Іжутова, О. Сальнікова, В. Шиповський. К.: НУОУ імені Івана Черняховського, 2020. 22 с.

30. Требін М.П. «Гібридна» війна як нова українська реальність. *Український соціум*. 2014. № 3 (50). С. 113-127.

31. Толстой В.В., Петречук Л.М., Іващенко Ю.С., Гуляєва О.А., Соболенко О.В.. Сучасні інформаційно-комунікаційні технології: навч. посібник. Дніпро: Нац.металур.акад. України, 2019. 230 с.

32. Швачич Г.Г., Толстой В.В., Петречук Л.М., Іващенко Ю.С., Гуляєва О.А., Соболенко О.В. Сучасні інформаційно-комунікаційні технології: навч. посібник. Дніпро: НМетАУ, 2017. 230 с.

ТЕМИ ДЛЯ САМОСТІЙНИХ РОБІТ

1. Інформації як специфічна субстанція
2. Інформаційна компонента влади
3. Інформаційна компонента національної безпеки
4. Інформаційна складова масової культури як загроза національній безпеці
5. Інформаційний аспект управлінської діяльності у сфері національної безпеки
6. Інформаційно-аналітична діяльність як складова управління у сфері національної безпеки
7. Етапи розвитку та компоненти ІКТ
8. Можливості та проблеми, які є наслідком розвитку ІКТ у контексті забезпечення національної безпеки
9. Проблема захисту ІКТ від кіберзагроз та пріоритети їх розвитку в Україні
10. Кризові ситуації у соціальних системах та роль ІКТ в їх моніторингу та генеруванні
11. Використання інформаційних систем при прийняття рішень у сфері національної безпеки
12. Ситуаційні центри як елемент ІКТ у сфері національної безпеки
13. Проксі-війни як простір використання сучасних ІКТ
14. Стратегічні комунікації як складова ІКТ в генеруванні загроз кризових ситуацій
15. Стратегічні комунікації як складова ІКТ в протидії загроз кризових ситуацій
16. Роль та значення інформаційно-аналітичних ресурсів при техніко-технологічному підході до управління
17. Використаняня інформаційно-аналітичної діяльності під час другої світової війни
18. Інформаційне суспільство як складова трансформацій у сфері публічного управління.
19. Проблема інформатизації суспільства в контексті забезпечення національної безпеки
20. Погляди Г. Почепцова на значення та роль пропаганди як різновида новітньої ІКТ

21. Забезпечення захищеності об’єктів критичної інфраструктури України в сфері кібербезпеки
22. Природа кризових ситуацій соціального характеру та їх вплив на національну безпеку
23. Використання технологій штучного інтелекту в інтересах національної безпеки
24. Перспективи розвитку сектору інформаційно-комунікаційних технологій в Україні
25. Напрями реалізації потенціалу сектора інформаційно-комунікаційних технологій у контексті забезпечення національної безпеки
26. Національна інформаційно-комунікаційна інфраструктура України: сучасний стан та перспективи розвитку.
27. Проблеми та перспективи розвитку ринку ІКТ України в умовах війни.
28. Функціональна модель системи підтримки прийняття рішень в системі стратегічних комунікацій Збройних Сил України
29. Інформаційні системи та інформаційне забезпечення правоохоронної діяльності
30. Основні заходи з забезпечення безпеки СППРР.
31. Управління ризиками під час впровадження інформаційних систем та технологій
32. Національні системи оцінювання ризиків і загроз: кращі світові практики

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бухтатий О. Публічні комунікації демократичної держави: монографія. Дніпро: Журфонд, 2018. 297 с.

2. Варенко В.М. Інформаційно-аналітична діяльність: навч. посіб. К.: Університет «Україна», 2014. 417 с.

3. Данильчук Л. Сутність і зміст поняття «інформаційно-комунікаційні технології». *Педагогіка і психологія професійної освіти*. 2012. № 4. С. 123-130

4. Державне управління : підручник : у 2 т. / Нац. акад. держ. упр. при Президентові України ; ред. кол. : Ю.В. Ковбасюк (голова), К.О. Ващенко (заст. голови), Ю.П. Сурмін (заст. голови) [та ін.]. К. ; Дніпропетровськ: НАДУ, 2012. Т. 1. 564 с.

5. Демартино А.П. Поняття і класифікація новітніх інформаційно-комунікативних технологій // *Науковий часопис НПУ імені М.П. Драгоманова* Випуск 24.2018.С.94-99

6. Державно-громадянська комунікація: шлях від кризи до взаємодії: монографія / Козаков В.М., Рашковська О.В., Ребкало В.А., Романенко Є.О., Чаплай І.В. К.: ДП "Вид. дім "Персонал", 2017. 288 с.

7. Доронін І.М. Національна безпека України в інформаційну епоху: теоретико-правове дослідження. Дис. докт. юрид. наук: 12.00.01; Наук.-досл. інст. інформ. і права, Нац. акад. прав. наук України. Київ. 2020.539 с.

8. Драгомирецка Н.М. Сучасні тенденції комунікацій у сучасному світі. *Публічне урядування* : збірник. 2015. N 1. Київ: ДП «Видавничий дім «Персонал», 2015. С. 85-97.

9. Драгомирецька Н.М., Кандагура К.С., Букач А.В. Комунікативна діяльність в державному управлінні: навч. посібник. Одеса: ОРІДУ НАДУ, 2017. 180 с.

10. Дрешпак В.М. Комунікації в публічному управлінні: навч. пос. Д. : ДРІДУ НАДУ, 2015. 168 с.

11. Глобальна та національна безпека: підручник / авт.кол.: В.І. Абрамов, Г.П. Ситник, В.Ф. Смолянюк та інш.; за заг.ред. Г.П.Ситника. К.: НАДУ, 2016. 784 с.

12. Глобалізаційні виклики сучасності: підручник /авт.кол. Л.Г.Комаха, І.В. Алексеєнко, В.Л. Гура та ін.; за заг.ред. Л.Г. Комахи.- К.: ВПЦ "Київський університет", 2022. 350 с.

13. Гнатенко В. Застосування інформаційно-комунікаційних технологій у забезпеченні економічної безпеки держави. *Літопис Волині*. *Всеукраїнський науковий часопис*. №. 22. 2020. С.88-92

14. Закон України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації». URL: https://zakon2.rada.gov.ua/laws/show/539/97- %D0%B2%D1%80.

15. Звоздецька О. Дезінформація як загроза національній безпеці Європейського Союзу: проблеми та підходи. *Історико-політичні проблеми сучасного світу: Збірник наукових статей.* Чернівці : Чернівецький національний університет, 2021. Т. 43. С. 30-39. DOI : https:// 10.31861/mhpi2021.43.30-39.

16. Інформаційна складова державної політики та управління : монографія / Соловйов С.Г., та ін. ; заг. ред. Грицяк Н.В. ; НАДУ. К.: К.І.С., 2015. 320 с.

17. Кириченко Г.В. Інформаційно-комунікаційні механізми як інновації в системі формування позитивного іміджу органів державної влади. *Вчені записки Таврійського Національного Університету імені В.І. Вернадського. Серія: державне управління* Т. 30 (69). № 6. 2020. С. 46-54.

18. Клубань О.М., Курбан О.В., Любовець Г.В., Король В.Г., Савчук Р.П. Сучасні комунікаційно-контентні процеси в безпековій сфері:навч. посібник. Київ: ВІКНУ, 2016. 170 с.

19. Кочубей Л. Особливості сучасних інформаційно-комунікативних технологій в Україні. *Наукові записки*. Вип. 3 (89). 2018. С. 44-70.

20. Климанська Л.Д. Соціально-комунікативні технології в політиці: таємниці політичної «кухні». Львів: Видавництво Національного університету «Львівська політехніка», 2007. 332 с.

21. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі: навч. посібник. К.: ВІКНУ, 2016. 286 с.

22. Литвиненко О.В. Спеціальні інформаційні операції та пропагандистські кампанії: Монографія. Київ: ВКФ “Сатсанта”, 2000. 222 с.

23. Маліновська О.Я. Використання сучасного зарубіжного досвіду комунікацій в системі публічного адміністрування. *Збалансоване природокористування* № 2. 2022. С.39-44

24. Марутян Р. Інфодемія як наслідок неефективних стратегічних комунікацій. *STRATCOM.* Науково-публіцистичне видання. К., 2020. №.1. С.36-40.

25. Марутян Р. Моделі стратегічних комунікацій: ціннісно-смислові аспекти. Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи : ІІ міжнар. наук.-практ. конф., 1 жовт. 2021 р. : тези доповідей / Міністерство оборони України, НУОУ імені Івана Черняховського. К. : НУОУ, 2021. С.24-26

26. Марутян Р. Стратегічні наративи як інструмент досягнення цілей політики національної безпеки *STRATCOM*. Науково-публіцистичне видання. К., 2021. №.2. С.45-48.

27. Ніколаєнко Н.О. Інформаційна безпека та політична комунікація: навч.-метод. посібник. Миколаїв: НУК, 2022. 121 с.

28. Олешко А.А. Інформаційно-комунікаційні технології та людський розвиток. *Інвестиції: практика та досвід* № 16. 2019. С.16-19.

29. Орел М.Г. Теоретичні основи державного управління у сфері політичної безпеки: монографія. Київ: Поліграф плюс 2019. 320 с.

30. Основи теорії управління у сфері національної безпеки: курс лекцій / Г.П. Ситник. К: ТОВ "САК Лтд.", 2023. 174 с.

31. Островська Н.В. Прикладні соціально-комунікаційні технології: навч. посібник. Запоріжжя. ЗНТУ, 2017. 110 с.

32. Пацурія Н. Упровадження технологій штучного інтелекту в забезпечення національної безпеки та обороноздатності України: правові проблеми і перспективи повоєнного періоду. *Теорія і практика інтелектуальної власності* . №3.2023. С.68-78

33. Почепцов Г.Г. Від покемонів до гібридних війн: нові комунікативні технології XXI століття. Київ: Києво-Могилянська академія, 2017. 260 с.

Почепцов Г.Г. Державна інформаційна політика в Україні: шляхи вдосконалення [Електронний ресурс]: підручник URL: http://pidruchniki.ws/14940511/politologiya/derzhavna_ informatsiyna_politika_ ukrayini_ shlyahi_vdoskonalennya.

35. Практичний посібник для працівників комунікаційних структур в органах влади. 2016. URL: https://imi.org.ua/wp-content/uploads/2017/06/posibnyk.pdf

Про доступ до публічної інформації: закон України від 13.01.2011 № 2939-VI. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi

37. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi

38. Про затвердження Комунікаційної стратегії Державного комітету телебачення і радіомовлення України на 2022-2023 роки № 526 URL: https://zakon.rada.gov.ua/rada/show/v0526603-21#Text

39. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Постанова Кабінет Міністрів України від 29 березня 2006 р. n 373 із змінами, внесеними згідно з Постановою КМ N 645 (645-2022-п) від 03.06.2022 URL: https://zakon.rada.gov.ua/laws/show/373-2006-п#Text

40. Про захист інформації в інформаційно-телекомунікаційних системах: закон України від 05.07.1994 № 80/94-ВР // Законодавство України. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi

Про інформацію: закон України від 02.10.1992 № 2657-XII. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi

42. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації: розпорядження Кабінету Міністрів України від 03.03.2021р. №167-р. URL: https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text

43. Публічне управління та адміністрування у сфері національної безпеки: (системні, політичні та економічні

аспекти): словник-довідник / С.П. Завгородня, М.Г. Орел, Г.П. Ситник [уклад.] /за заг.ред. Д.В. Неліпи, Є.О. Романенка, Г.П. Ситника. Київ: Видавець Кравченко Я.О., 2020. 380 с.

44. Редька І. Інформаційні технології. Основні якості сучасних інформаційних технологій. *Матеріали Всеукраїнської науково-практичної конференції «Соціальні комунікації і нові комунікативні технології*». Запоріжжя, 2017. С. 20-25.

45. Саврук М. Проблеми інформаційної політики України в контексті забезпечення інформаційної безпеки. *Вісник Львівського університету. Серія міжнародні відносини*. 2017. Випуск 43. С. 172-184.

46. Ситник Г.П., Орел М.Г. Публічне управління у сфері національної безпеки: підручник /за ред. Г.П.Ситника. - Київ: Видавець Кравченко Я.О., 2020. 360 с.

47. Ситник Г.П., Борисов А.В. Політичний досвід розвинених країн світу щодо інформаційно-аналітичного забезпечення системи цивільної безпеки. *Національні інтереси України.* 2024. № 2(2) .С.124-133. URL: https://doi.org/10.52058/3041-1793-2024-2(2)-123-132

48. Ситник Г., Бондар В., Орел М. Системний підхід дослідження феномену інформація в державному управлінні. *Вісник Київського національного університету імені Тараса Шевченка. Державне управління*. №4. 2023. С. С. 63-74

49. Ситник Г.П. Інформаційна компонента критичних (надзвичайних) ситуацій у контексті забезпечення державної безпеки. *Науковий вісник: Державне управління*. 2020. №2(4). С.327-339

50. Ситник Г.П., Клименко Н.Г. , Гореліков І.О. Державна політика забезпечення інформаційної безпеки та кібербезпеки, як її складової: проблеми та шляхи їх вирішення. *Державне управління: удосконалення та розвиток*. 2024. No 5. URL: https://nayka.com.ua/index.php/dy/article/view/3678

51. Ситник Г.П. Концептуалізація “інформаційної безпеки” у контексті властивостей інформації як специфічної субстанції. *Державне управління: удосконалення та розвиток*. 2020. № 3. URL: http://www.dy.nayka.com.ua/?op=1&z=1595.

52. Соколов В.А. Інституалізація аналітичної діяльності в системі забезпечення національної безпеки на основі

застосування зарубіжного та вітчизняного досвіду. Дис. … канд. наук з держ.упр.: 25.00.01; Харківський рег. інст. держ. управ. НАДУ. Харків, 2020. 375 с.

53. Стратегічні комунікації в умовах гібридної війни: погляд від волонтера до науковця : монографія. К. : НА СБ України, 2018. 517 с.

54. Стратегічні комунікації для безпекових і державних інституцій : практичний посібник / [Л. Компанцева, О. Заруба, С. Череватий, О. Акульшин; за заг. ред. О. Давліканової, Л. Компанцевої]. – Київ: ТОВ «ВІСТКА», 2022. – 278 с.

55. Стратегія інформаційної безпеки. Указ Президент України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

56. Требін М.П. «Гібридна» війна як нова українська реальність. *Український соціум*. 2014. № 3 (50). С. 113-127.

57. Толстой В.В., Петречук Л.М., Іващенко Ю.С., Гуляєва О.А., Соболенко О.В. Сучасні інформаційно-комунікаційні технології: навч. посібник. Дніпро: Нац.металур.акад. України, 2019. 230 с.

58. Турчак А. Основні складові інформаційної безпеки держави. *Аспекти публічного управління*. Том 7. №5, 2019. С.44-56

59. Швачич Г.Г., Толстой В.В., Петречук Л.М., Іващенко Ю.С., Гуляєва О.А., Соболенко О.В. Сучасні інформаційно-комунікаційні технології: навч. посібник. Дніпро: НМетАУ, 2017. 230 с.

60. Шляхи удосконалення системи державного управління забезпеченням національної безпеки України: монографія / Г.П. Ситник, В.І. Абрамов М.М. Шевченко та ін.; за ред. Г.П. Ситника, В.І. Абрамова, М.М. Шевченка. К.: МАЙСТЕР КНИГ, 2012. 536 с.

61. Шустенко С.О. Інформаційна політика та стан інформаційної сфери країн Європи. *Journal of International Relations of KNU*. Київ. 2017 р. URL: http://journals.iir.kiev.ua/

62. Ярова Г.Д. Генезис наукових поглядів на комунікації у публічному управлінні. *Інвестиції: практика та досвід* № 11. 2021. С.103-107.

Київський національний університет імені Тараса Шевченка

Навчально-методичне видання

СИТНИК Григорій Петрович (розділ 1)
ЗАВОРІТНЯ Галина Петрівна (розділ 2)
МАРУТЯН Рена Рубенівна (розділ 3)

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Навчальний посібник / за заг. ред. Г.П. Ситника

для здобувачів першого (бакалаврського) рівня вищої освіти, які навчаються за освітніми програмами за спеціальністю 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону»

Друкується в авторській редакції

Підписано до друку 30.11.2024
Формат 60×90 1/16
Умовн. друк. арк. 11. Обл.-вид. арк. 9,7
Папір офсетний. Друк цифровий.
Гарнітура Таймс. Наклад 100

Видавець – ТОВ «Академпрес»
01011, м. Київ, вул. Панаса Мирного, 26.
E-mail: academpress@ukr.net

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців,
виготовлювачів і розповсюджувачів видавничої продукції:
серія ДК № 2634 від 04.10.2006 р.