НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

С. ДОМБРОВСЬКА, Н. КАРПЕКО, С. ПОРОКА, В. НОВАК

МОНОГРАФІЯ

ФОРМУВАННЯ ДІЄВИХ МЕХАНІЗМІВ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ВПЛИВУ ЦИФРОВИХ ТЕХНОЛОГІЙ

Харків – 2026

УДК 351:355:342.7

Монографію розглянуто та рекомендовано до друку Вченою Радою
Національний аерокосмічний університет
«Харківський авіаційний інститут»
Протокол № 7 від 18.02.2026

Рецензенти:

Сиченко В.В. – ректор комунального закладу вищої освіти "Дніпровська академія неперервної освіти" Дніпропетровської обласної ради," доктор наук державного управління, професор, Заслужений працівник освіти України

Палюх В.В. – начальник докторантури – ад'юнктури Національного університету цивільного захисту України, доктор наук державного управління, с.д.

Формування дієвих механізмів публічного управління у сфері національної безпеки в умовах впливу цифрових технологій: Монографія: С.М. Домбровська, Н.М. Карпеко, С.Г. Порока, В.М. Новак: НАУ «ХАІ», 2026. 250с.

В монографії розглянуто формування дієвих механізмів публічного управління у сфері національної безпеки в умовах впливу цифрових технологій та розробленні практичних рекомендацій щодо вдосконалення публічного управління в цій сфері в Україні.

У роботі визначено системний і синергетичний підходи до вдосконалення системи публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні. Застосування цих підходів дозволить модернізувати інституційне й організаційне забезпечення цієї системи з позиції, що передбачає систематизацію дії механізмів публічного управління в досліджуваній сфері. З цією метою узагальнено типи цифрових технологій і соціально-політичних ефектів цифровізації, серед яких особливе місце відведено ефектам технології великих даних (big data) у публічній політиці та їх впливу на сферу забезпечення нацбезпеки. Рекомендовано здійснювати визначення цифрових бар’єрів, рівня цифрової довіри та перспектив трансформації балансу між забезпеченням конфіденційності персональної інформації та розвитком системи національної безпеки.

С.М. Домбровська,
Н.М. Карпеко,
С.Г. Порока,
В.М. Новак

ЗМІСТ

ВСТУП

Актуальність дослідження обумовлена постійно зростаючою роллю цифрових технологій в усіх сферах суспільної життєдіяльності України, особливо у сфері національної безпеки та системі публічного управління. У сучасних умовах цифрового простору відповідні технології зумовлюють формування як позитивних, так і негативних тенденцій. Щодо позитивних тенденцій, то варто вказати на застосування цифрових технологій для забезпечення сталого й інноваційного розвитку держави та її суспільства. Негативний же вплив цих технологій полягає в тому, що за їхньою допомогою чиняться кібератаки та ведуться війни, які передбачають застосування кінетичної та нетрадиційної зброї. Останній факт є свідченням актуалізації нового типу війн – гібридних, що притаманно також і для України, проти якої рф веде неоголошену війну відповідного типу. Зважаючи на це, можна відзначити, що забезпечення на належному рівні національної безпеки України в умовах впливу цифрових технологій набуває все більш важливого значення як в науково-теоретичній площині, так і в практичній. В їх межах має бути визначено роль і місце цифрових технологій у системі публічного управління, а також особливості їхнього виваженого використання з метою гарантування нацбезпеки та сталого розвитку. Варто зазначити, що відповідні зміни у сфері правового регулювання національної безпеки знайшли практико орієнтований відгук на найвищому рівні, зокрема, у межах Закону України «Про національну безпеку України», Стратегії національної безпеки в Україні тощо. У той же час, ці нормативно-правові документи потребують доопрацювання з позиції визначення особливостей інституційного забезпечення національної безпеки, а також протидії негативному впливу цифрових технологій на всіх рівнях її управління. Це дозволить забезпечити розвиток системи безпеки та цифрового суспільства,

здатного протистояти такому впливу, а також державний захист інтересів українських громадян в інформаційній і безпековій сферах. Крім того, необхідним є наукове осмислення самого феномену цифрових технологій і його впливу на систему публічного управління у сфері національної безпеки, що набуває ознак парадигмальності.

Отже, сучасне становище України є нестабільним через вплив держави-агресорки, що зумовлює збільшення кількості конфліктів і зміну підходів до ведення війни нетрадиційними засобами шляхом використання цифрових технологій. Останні 10 років через неоголошену війну рф Україна та її населення змушені відчувати на собі насамперед деструктивний вплив зазначених технологій. Відтак, одним із найбільш важливих завдань для нашої держави є вдосконалення наявних механізмів публічного управління у сфері національної безпеки в умовах впливу цифрових технологій. Адже виважене їх застосування може дозволити підтримати на належному рівні систему безпеки, яка, до того ж, виходить і від самого населення у вигляді дотримання норм і правил, легітимації політики та курсу держави, а також довіри до діяльності її апарату. З огляду на це, актуальним є визначення концептуальних й організаційно-правових засад дієвого функціонування механізмів публічного управління України у сфері національної безпеки в умовах впливу цифрових технологій.

Сутність, структура та інші аспекти публічного управління у сфері національної безпеки крізь призму розвитку цифрових технологій неодноразово досліджувалися у працях зарубіжних науковців Л. Антопулос, С. Арадау, Е. Аркін, У. Бека, З. Бжезінського, С. Бергера, С. Брозе, Д. Бетца, А. Волферса, М. Веле, М. Гарсії-Алонсо, С. Гібба, А. Гідденса, Р. Гранта, М. Девідсона, Д. Деннінга, П. Едвардса, А. Едельштайн, І. Кекіш, Т. Келлі, М. Клавер, А. Кларка, К. Крісті, Б. Маби, Ф. Майлза, В. Мустаки, Н. Наєма, Дж. Найа, Т. Накаї, П. Норвіга, М. О'Коннелла, Дж. Паджетт, Дж. Паркера, І. Пула, С. Рассела, С. Рінальді, Дж. Розе, С. Родан, М. Ронки, С. Сассен, Т. Стівенса, Е. Тоффлера, М. Хоровітц, Ф. Хоффмана, П. Шарре, Дж. Шуха,

Т. Яновскі та ін. [108; 112; 135; 136; 144; 185; 188; 198; 203–204; 206; 207; 223; 237; 238; 248; 251; 258; 259; 260; 261; 268; 272; 274; 277; 285; 292; 296; 298; 301; 304; 305; 341; 352].

Крім того, значний внесок у розвиток фундаментальної вітчизняної науки у сфері реалізації безпекової та цифрової політики зробили вчені В. Антонюк, В. Баштанник, С. Бєлай, О. Бондаренко, Д. Вєдєнєєв, Т. Воропаєва, В. Горбулін, О. Довгань, С. Домбровська, Ю. Древаль, О. Копанчук, О. Кравчук, С. Крук, О. Крюков, О. Курбан, Є. Магда, О. Машков, О. Мережко, Н. Нижник, О. Пархоменко-Куцевіл, А. Помаза-Пономаренко, С. Порока, Г. Почепцов, Р. Прав, Р. Примуш, О. Радченко, А. Рубан, І. Рущенко, Г. Ситник, В. Скуратівський, В. Степанов, В. Торічний, Е. Щепанський, Т. Яровий та ін. [3; 4; 8; 11; 12; 19; 24; 25–27; 27; 38; 39–43; 44–45; 62; 63–72; 73; 74; 75; 77; 90; 91; 102–103; 104; 289].

Методологічну основу роботи становить сукупність способів наукового пізнання та загальнонаукових принципів проведення дослідження, що враховують фундаментальні положення й праці вчених щодо аспектів публічного управління, інституціоналізму, конфліктології, стратегування, політичної комунікації тощо.

Монографія побудована на системному, синергетичному й інституціональному підходах, а також сукупності методів, а саме:

1) *логічного узагальнення, синтезу й абстрагування* (під час дослідження генези сфери національної безпеки із розкриттям сутності феномену цифровізації та цифрової трансформації, яка чинить вплив на цю сферу);

2) *теоретизування й історичної формалізації* (для визначення механізмів публічного управління у сфері національної безпеки в умовах впливу цифрових технологій);

3) *системного аналізу, порівняння, вибірки й опису* (з метою дослідження особливостей і ризиків функціонування механізмів публічне управління у сфері національної безпеки в умовах впливу цифрових

технологій в Україні);

4) *індукції та дедукції* (під час визначення концептуальних засад формування та розвитку механізмів публічного управління у сфері національної безпеки в умовах впливу цифрових технологій);

5) *групування та прогнозування* (з метою вдосконалення підходу до визначення перспектив упровадження моделі публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні).

Інформаційно-фактологічною базою дослідження є закони України, укази Президента України, нормативні акти Кабінету Міністрів України, статистична інформація Державної служби статистики України тощо.

Практичне значення одержаних результатів полягає в можливості їхнього застосування в діяльності органів публічної влади, що сприятиме підвищенню результативності інституційної реалізації публічного управління у сфері національної безпеки України в умовах цифровізації.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ ДІЄВИХ МЕХАНІЗМІВ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ВПЛИВУ ЦИФРОВИХ ТЕХНОЛОГІЙ

1.1. Генеза сфери національної безпеки та її місце в системі публічного управління

Розширення інформаційного та цифрового простору, а також оперативний обмін інформацією як у державному секторі, так і в приватному – це всі явища та процеси, які є реальністю всіх країн світу. Ці процеси та процедури відбуваються із використанням нових технологій, що дозволяють оцифровувати дані, підвищувати рівень безпеки для громадян та ін. У той же час, такі технології зумовлюють накопичення реальних і штучно створюваних суперечностей у сфері державної політики у сфері національної безпеки загалом та інформаційної безпеки зокрема. При цьому слушним є твердження науковців щодо важливості [53–56; 91; 270; 271]. На погляд авторів, технології цифровізації є тим інструментарієм, який усе більше використовується у сфері національної безпеки. На жаль, не поодинокими є випадки, коли цей інструментарій використовується із метою дестабілізації ситуації як у межах країни в цілому, так і в її регіонах, або публічних чи приватних інституціях. З огляду на це вчені слушно наполягають на співвіднесенні національної безпеки та цифрової безпеки як загального та часткового, адже національна безпека є більш ємною категорією, що включає застосування не тільки традиційної зброї (кінетичної), а й інформаційної та цифрової. При цьому інформаційна безпека також є більш ширшим поняттям, по відношенню до цифрової безпеки, цій підставі вважаємо, оскільки інформаційна безпека проявляється під час застосування не тільки

цифрових технологій, хоча вони пришвидшують обмін інформацією. На цій підставі можна стверджувати про витіснення деяких суб'єктів з інформаційного простору та його інституційного забезпечення на належному рівні. Мова йде, зокрема, про тих суб'єктів, які не використовують цифрові та інші новітні технології для збору, аналізу та передачі інформації, що може бути цінною для державного та/або приватного секторів, які, у свою чергу, входять до системи публічного управління. Крім того, відзначимо, що зазначені суб'єкти будуть виконувати все менше важливих інформаційно-комунікативних функцій, опиняючись на периферії забезпечення системи безпеки. Саме з урахуванням такої гіпотези ми будемо проводити наше дослідження.

У межах цієї глави вважаємо за доцільне зупинитися на теоретичному визначенні й обґрунтуванні парадигми поєднання предметної галузі національної безпеки та політики цифровізації. У цьому контексті набуває важливості дослідження концепту генези (еволюції) сфери національної безпеки під впливом цифрових технологій. Уважаємо, що перший рівень аналізу має бути спрямовано на виявлення еволюційного розвитку як розуміння концепту «національної безпеки», так і предметного поля досліджень цифрової безпеки. Цей концепт передбачає теоретичний аналіз, спрямований на демаркацію галузі дослідження безпеки (security studies), виявлення ключових перетворень розуміння та підходів до національної безпеки, а також формулювання погляду на сучасні зміни, пов'язані із застосуванням цифрових технологій. У межах цього розділу буде здійснена спроба концептуалізації розуміння безпеки, а також демонстрації історичного розвитку підходів до такого розуміння. У результаті буде запропоновано розглядати проникнення цифрових технологій у питання національної безпеки не як формування самостійного сектору безпеки (у логіці Копенгагенської школи), а як процес, що пронизує всі сектори (що забезпечує трактування, схоже на специфіку інформаційної та цифрової безпеки). Запропонований теоретичний

концепт спрямований на вивчення взаємозв'язку цифрових технологій у сфері національної безпеки.

Учені зазначають, що сфера забезпечення національної безпеки еволюціонує, зокрема, у бік забезпечення саме безпеки людини (особистості) [28; 30; 97]. У цьому контексті національна безпека буде розумітися з позиції соціальної орієнтованості та захисту прав громадян нба безпечне життя та довкілля. Певною мірою така характеристика концепції національної безпеки (national security concept) відзначається уніфікованим та доктринальним спрямуванням. Для теоретичного аналізу розвитку досліджень національної безпеки ми прагнемо її конкретизованого розгляду. Такий підхід не є новим: його застосовував С. Шабтай [306] у своєму дослідженні національної безпеки Ізраїлю для позначення концепту «сфери безпеки» (security sphere). Автор концептуалізує «сферу безпеки» як парасолькову конструкцію, що включає як доктринальні підходи до визначення національної безпеки (з фіксацією національних цілей та інтересів), так і підходи до формулювання політики у сфері національної безпеки.

У свою чергу, «безпека» розуміється як функція держави в питаннях гарантування національної безпеки. Така функція містить як безпосередню політику (policy), так і конкретні моделі реалізації конкретних цілей національної безпеки (див. дослідження Дж. Колльєра [158] про характер забезпечення безпеки та моделі забезпечення безпеки на прикладі кібербезпеки). При цьому сам термін «безпека» (security provision) використовується для співвідношення безпеки – держави – історичного контексту змін (наприклад, у дослідженні Б. Мабі [248] представлено історичний аналіз розвитку взаємодій держава-суспільство, пов'язаних із нацбезпекою). Таке розуміння дозволяє нам використовувати термін «забезпечення» у межах системи безпеки, а також звертатися до змістовного зв'язку з історичним контекстом для однакового теоретичного розгляду еволюції досліджень безпеки та безпосередньо розуміння

національної безпеки. Саме на це спрямовано цю частину роботи.

Отже, наповнення конструктів «безпека» та «загроза» розвивається, а відтак межі та сфера поширення національної безпеки також трансформуються. Традиційно забезпечення такої безпеки розглядалося у категоріях війни та миру. У розробці Е. Міда [253] історія військової стратегії від Макіавеллі до сучасників 1950-х рр. розглядається на основі саме такого – військового – розуміння національної безпеки. Іншими словами, нацбезпека починається й обмежується виключно питаннями ведення війни. Подібним чином безпека розглядається в історичній перспективі в наукових розробках зарубіжних учених П. Парета, Г. Крейга,Ф. Гілберта та вітчизняних науковців [30; 276].

Згодом автори (наприклад, Д. Болдуїн [130]) вказували на фундаментальні зміни як у політиці, так і в питаннях безпеки через ефекти Другої світової війни. Проте фокус безпеки залишався суто у військових рамках. У роботах про соціальні, економічні та політичні успіхи Заходу в XVI–XVIII ст. наголошувалося, що безпеку необхідно розглядати в категоріях війни, а досягнення розвитку (development) залежали від тих поліпшень у здатності вести війни, які позначалися концептом «військова революція» [277]. Таким чином, загрозами безпеці загалом і національній безпеці зокрема сприймалися лише ті загрози, які безпосередньо перебували у площині військової готовності/можливості держав. Саме тому дослідження війни та миру є окремим напрямом академічних досліджень, кількість яких на вітчизняних теренах збільшується через вплив повномасштабної агресії рф проти України.

Після Першої світової інтенсивно розвивалася концепція колективної безпеки [235], хоча практики колективної безпеки (у межах вузьких альянсів) – існували як і раніше. При цьому колективна безпека не прирівнювалася до міжнародної безпеки, оскільки вона поширюється лише на тих акторів (держави), які взяли на себе відповідальність за підтримання певного рівня безпеки (за міжнародними угодами та договорами).

Незважаючи на розвиток сфер стратегії та тактики ведення війни, а також збільшення ролі політики та дипломатії у питаннях системи безпеки, основний фокус все одно залишився на категоріях війни та збройних конфліктів.

Після Другої світової війни концепція безпеки та національної безпеки постійно модернізувалася, адже сам факт ще однієї світової війни протягом відносно короткого періоду часу продемонстрував неспроможність підходів до забезпечення системи безпеки, що діяли раніше. Відтак, колективна безпека (зі створенням відповідної системи) стає домінуючою концепцією та практикою. Так, А. Волферс [352] вказував на невизначеність оцінки загроз (одна і та ж загроза може по-різному оцінюватися й інтерпретуватися державами, їх урядами та регіональною владою) у національній безпеці. Учений Д. Болдуїн [129] наголошував на значущості переосмислення поняття «безпека» у контексті перевизначення політичного порядку денного національних держав, концептуалізуючи розширення типів загроз. При цьому знаковим моментом є виявлення концептуальних відмінностей, що становлять підґрунтя різних концепцій безпеки (у тексті співвідноситься економічна та екологічна безпека з традиційним розумінням національної безпеки). Стрімкого розвитку набула концепція дилеми безпеки («security dilemma», особливо у період Холодної війни) [148], що окреслила формування специфічної політики «стримування».

У той час як Україна проголосила власну незалежність, у світі (у 1991 р.) була запропонована теорія сек'юритизації [131; 149]. У межах цієї теорії було запропоновано використовувати секторальний підхід до визначення національної безпеки, яку зазвичай відносять до Копенгагенської школи безпеки [148; 149]. Цей підхід розширив класичні уявлення про сектори безпеки та включив економічні, екологічні, соціальні та політичні сфери, належність функціонування яких забезпечується за допомогою державних та недержавних секторів. У цей період часу

актуалізувалися питання глобалізації та екологічні виклики (у тому числі кліматичні зміни), які вимагали переосмислення та іншої концептуалізації системи безпеки з позиції гарантування безпеки державним і суспільним інтересам [189]. Зв'язок факторів навколишнього середовища з безпекою сформував нові цінності та ідеї в галузі досліджень безпеки, а також поставив питання про сам концепт безпеки [180].

Самостійний розвиток отримав напрямок досліджень безпеки людини (зокрема, запропонований Р. Хенлон та К. Крісті [199]). Ключові питання безпеки людини (human security) концептуалізуються через призму конфліктів та розвитку (development). Критична оцінка загроз (зміна клімату, злочини проти людяності, гуманітарна інтервенція, бідність, тероризм, транснаціональна злочинність та ін.) пов'язана з виявленням та розвитком потенційних механізмів стримування таких, як вирішення конфліктів, економічний розвиток, дипломатія, підтримання миру, дотримання норм та незалежне правосуддя. Очевидно, як відбувається розширення спектру загроз (поява нових форм і типів, що вже не пов'язані з збройним конфліктом між державами) і збільшуються можливості, що їх нейтралізують. Розширення концепції системи безпеки вплинуло не лише на формулювання національних інтересів, а й на переосмислення суб'єктних ролей держави та суспільства. На це звертає увагу, наприклад, Л. Нік [266], порівнюючи національні та міжнародні концепції та політики у сфері безпеки людини.

Незважаючи на критику та об'єктивні недоліки підходу Копенгагенської школи (наприклад, тези Паризької школи безпеки), розширення секторів продовжується. Наприклад, інформаційна безпека (як на рівні технологічного аналізу [109; 171; 261], так і на рівні соціальних і політичних ефектів [147; 346]) виділяється не просто в окремий сектор, а пронизує всі сектори безпеки і, по суті, є одним з ключових. Так само виділяється кібербезпека та цифрова безпека, яка активно проникає у всі сектори безпеки [91; 271].

Розширенню дослідницької порядку сфери забезпечення безпеки сприяли і терористичні акти 11 вересня 2001 р. Самі події, а також реакція на них з боку США викликали безпрецедентну увагу до зростання кількості недержавних акторів та їхнього впливу на національну та міжнародну безпеку. Науковці В. Ендерс і Т. Сандлер [208] виділяють два важливі компоненти нової форми загрози (тероризм): наявність чи загроза насильства, а також політичний та соціальний мотив. Дослідження спирається на політекономічний підхід для опису тероризму та супутніх змін у сфері безпеки. Мотиви, індивідуальна та групова динаміка також досліджуються з позиції судової психіатрії.

Так, М. Сейджман у дослідженні «Джихад без лідера» [300] рекомендує звернути увагу і на суб'єктивно-індивідуальну складову з питань нацбезпеки. Учений Б. Хоффман [203–204] розширює дискусію щодо загроз тероризму та можливостей сфери нацбезпеки, пропонуючи своє розуміння еволюції тероризму та терористичного мислення.

Дослідник Р. Пейп [278] висуває тезу про неправильне уявлення про мотиви терористів у зниженні рівня національної безпеки (основна увага приділена терористам-смертникам), висуваючи тезу про те, що тероризм смертників використовується для досягнення світської та стратегічної мети примусу до виведення збройних сил.

Таким чином, спостерігається спроба повернення безпеки до витоків – до війни (у зазначеному дослідженні до категорії збройних сил належать також військові бази, логістика тощо). Учений А. Кронін [160] пропонує систематизований погляд на те, які дії можуть бути вжиті у питаннях безпеки для припинення існування таких організацій.

Розглянуті авторами виклики нацбезпеці і засоби реагування на них вказують на кілька значних аспектів. По-перше, секторальне уявлення безпеки та нацбезпеки, на даний момент уважається одним із конвенційних. Дискусія ведеться швидше про обсяг секторів, їх розширення тощо. По-друге, тероризм знову зробив актуальними питання

стратегії та військових практик у сфері нацбезпеки. Незважаючи на те, що більшість досліджень приділяють увагу проблематиці війни (war studies) та безпеки (security studies), існують наукові роботи щодо взаємозв'язку зазначених напрямків. По-третє, можна стверджувати про еволюційний розвиток як розуміння самого концепту безпеки, так і дослідницької діяльності з нацбезпеки. Еволюція спостерігається й у змістовному наповненні «безпеки», й у концептуалізації та розширенні типів загроз, й у можливостях (політичних, економічних тощо) держав протистояти загрозам (інформаційним, військовим, соціально-політичним, екологічним та ін.).

У такому розвитку розуміння системи безпеки сформувалися нові дискусійні простори про «війну з терором» у відносинах держави та громадянського суспільства, у тому числі в ліберально-демократичних країнах (наприклад, обговорення концептуальних інструментів «управління через ризик» у практиках «війни з тероризмом» [112]); дослідження ефективності та законності заходів ЄС по боротьбі з тероризмом [323]; дослідження сучасних напрямів війни з тероризмом – від військових кампаній та репресій до судового переслідування підозрюваних у тероризмі, поліцейської діяльності щодо боротьби з тероризмом, програм боротьби з радикалізацією тощо [225]), а також відбулося збільшення уваги до проблем технологічного розвитку.

Аналіз предметної галузі та еволюції системи безпеки зроблено для формування змістовно-теоретичного концепту даного дослідження. У його межах можемо зазначити, що розуміємо можливу критику такого уявлення розвитку предметного поля. Критика може стосуватися дискусії про «зіткнення» традиційних підходів із новими розширеннями загроз та самої національної безпеки. У цьому контексті важливою може бути дискусія про наукові підходи – наскільки допустимо «об'єднувати» підходи реалізму (структурного реалізму) з підходом, наприклад, критичних досліджень нацбезпеки. Дане дослідження не фокусується на вирішенні

існуючих протиріч і не прагне узгодити сутнісне значення різних підходів.

У продовження відзначимо, що усвідомлено приймаємо можливу критику, що може з’явитися у наукових дискусіях щодо різних наукових підходів під час парадигмальної характеристики концепції національної безпеки (наприклад, див. збірку з міжнародної безпеки, в якій представлені різні підходи [191] або наукові розробки Б. Болдуїна, де він демонструє протиріччя «традиційного» розуміння безпеки та розширення концепту до рівня екологічної, економічної та інших підвидів національної безпеки [129]).

Застосовуючи системний підхід до визначення генези сфери національної безпеки, можемо вказати на її (генези) еволюційний характер. Він передбачає реалізацію заходів по досягненню таких завдань: 1) продемонструвати дослідження нацбезпеки та саму безпеку як динамічну та адаптовану сферу наукового знання з позиції врахування факту проникнення до неї (сфери) цифрових технологій; 2) запропонувати розглядати питання загроз національній безпеці та потенційних можливостей протидії таким загрозам, причому ці можливості доречно розглядати як напрями, що розвиваються та доповнюють один одного. Іншими словами, беручи існуючі протиріччя, ми прагнемо продемонструвати причинно-наслідкові зв'язки розвитку сфери національної безпеки. Безперечно, сьогодні загрози такій безпеці наповнюються іншим змістом, їх концептуалізація змістовно змінюється. Останнє відбувається під наростаючим впливом цифрових технологій.

Таким чином, ми пропонуємо розглядати змістовні зміни у дослідженнях національної безпеки поза дискусією про школи, але з огляду на аналіз змістовних аспектів наповнюваності концептів, розширення секторів у сфері національної безпеки. Варто зазначити, що такий погляд на безпеку не є новим чи унікальним. Свідченням цього є погляд групи науковців Г. Шлаг, Дж. Джанк, К. Даасе, які у книзі «Трансформації досліджень безпеки: діалоги, різноманітність та

дисципліна» [302] по суті запропонували схожий погляд на складність існуючих підходів до акцентування на нових аспектах у забезпеченні національної безпеки.

Спираючись на підхід Копенгагенської школи, ми не лише розглядаємо сферу національної безпеки на секторальному рівні, а відзначаємо, що інформаційна та цифрова безпека пронизує всі сектори безпеки й оборони. По суті, інформаційна та цифрова безпека наскрізно проходить крізь усю сферу національної безпеки. Саме в цьому ми можемо побачити, як цифрові технології пронизують усі сектори. Таке бачення дозволяє розглядати цифрові технології та саму концепцію цифровізації комплексно у всій сфері національної безпеки. При цьому нацбезпека розглядається нами на двох рівнях. На першому – горизонтальному, йдеться безпосередньо про сектори, теорію сек'юритизації та технології (у даному випадку поєднуємо інформаційні та цифрові технології), що пронизують усі сектори безпеки й оборони. На другому – вертикальному, нацбезпека представляється ієрархічно та залежить від того, наскільки вона забезпечується державою для гарантування безпеки суспільства. Власне кажучи, на другому рівні відбувається перехід від суспільства до соціальних груп, а від останніх до рівня індивідуального сприйняття безпеки та її забезпечення (рис. 1.1).

Аналіз генези сфери забезпечення нацбезпеки дозволив сфокусуватися на розумінні такої безпеки, не ототожнюючи її з військовою безпекою (відсутність/наявність загроз та викликів військової агресії – це не одне й те саме). У той же час, національна безпека не синонімічна по відношенню до безпеки держави, адже остання є складовою частиною нацбезпеки (див. Закон України «Про національну безпеку України» (2018 р.)).

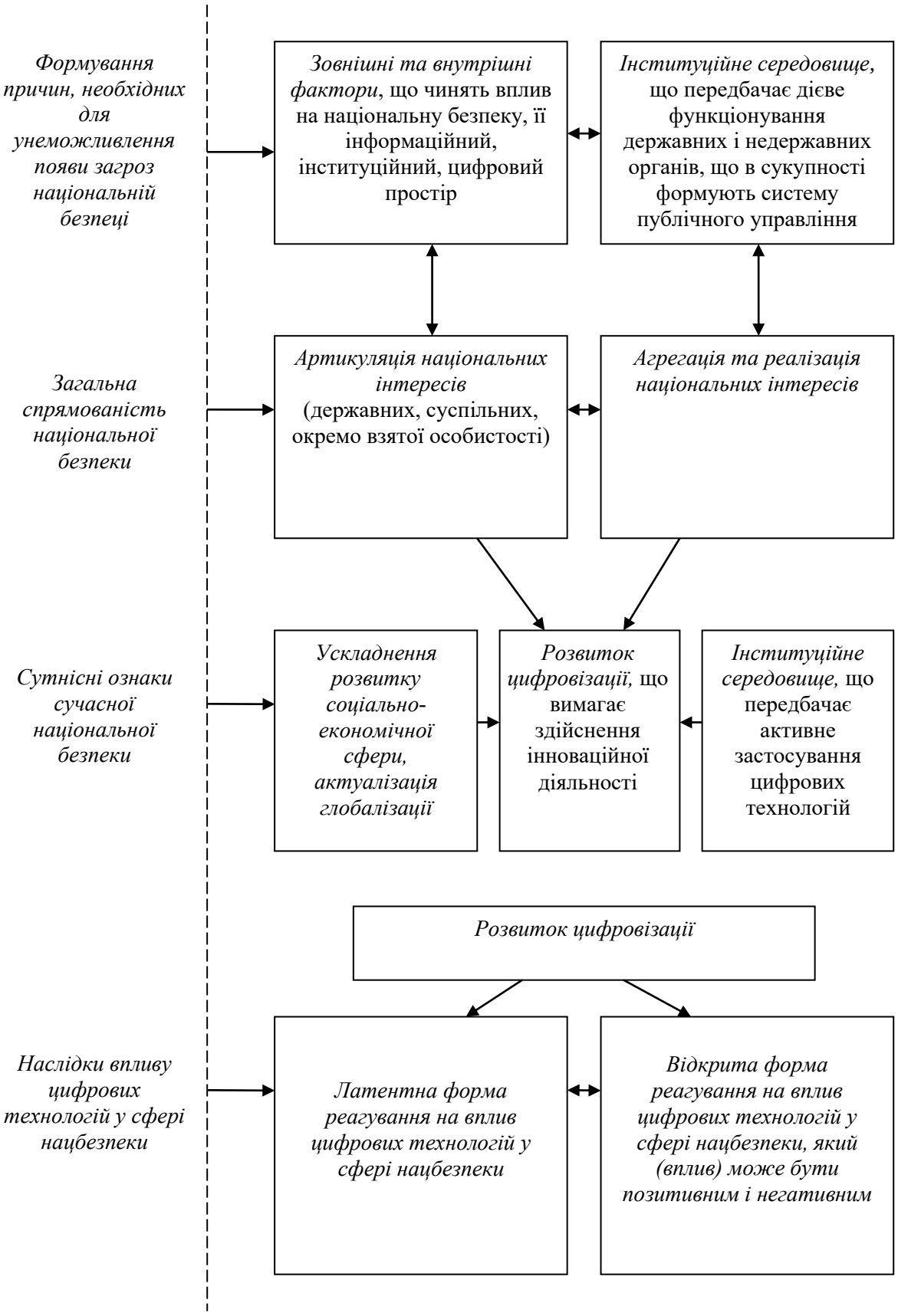

Рис. 1.1. Генеза сфери національної безпеки в умовах розвитку цифрових технологій

Джерело: авторська розробка

Відповідно, це дослідження перебуває у предметному полі досліджень національної безпеки (national security studies) і підпорядковане логіці розгляду інтересів, що становлять її базис.

На наш погляд, основна складність операціоналізації та концептуалізації предметного поля генези нацбезпеки знаходиться у двох площинах. Перша стосується розмежування досліджень сфери забезпечення нацбезпеки (national security studies) із суміжними (безумовно взаємопов'язаними та важливими) напрямками такими, як: дослідження оборони (defense studies), дослідження війни та миру (war and peace studies), стратегічні дослідження (strategic studies), військові дослідження (military studies) та ін. [30; 284]. Слід відзначити, що завдання даного дослідження не є демаркація предметних сфер одиниць аналізу кожного напряму. Проте цим дослідженням ми підкреслюємо, що чітко окреслюємо як теоретичне, так і методологічне предметне поле досліджень національної безпеки (national security studies).

Друга складність стосується розмежування феноменів нацбезпеки (скоріше навіть популярних та розхожих термінів) «інформаційна безпека» – «кібербезпека» – «цифрова безпека» – цифрові технології у сфері забезпечення безпеки (рис. 1.2).

На наше переконання, феноменологічне розмежування та визначення чітких відмінностей даних дефініцій дещо виходить за рамки даного дослідження. Аналіз наукових напрацювань [91; 102; 282] дав змогу виявити: 1) має місце історична формалізація еволюції сфери забезпечення нацбезпеки із застосуванням секторального підходу; 2) ґенезу сфери національної безпеки можна представити крізь призму використання цифрових технологій у сфері забезпечення такої безпеки. Авторська позиція в науковій дискусії про зазначені терміни полягає в тому, що «інформаційна безпека» та «цифрова безпека» є чітко закріпленими сферами вияву нацбезпеки (як в академічних джерелах, так і на рівні національних та міжнародних законодавчих актах). Складності ситуації

додає те, що «цифрова безпека» на сьогодні не має власного унікального обґрунтування, але вважаємо, що допоїти в цьому може врахування міждисциплінарного підходу в межах галузі науки «Публічне управління та адміністрування» (рис. 1.3). Дещо простішою виглядає ситуація з теоретичною характеристикою «інформаційної безпеки».

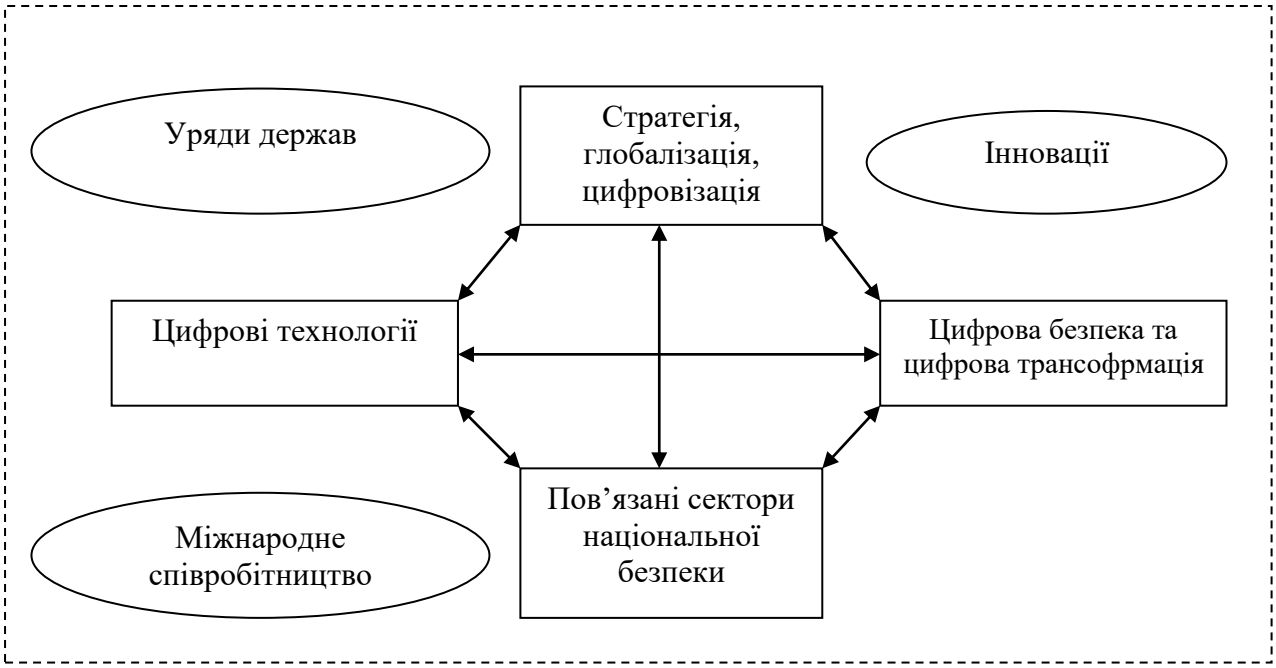

Рис. 1.2. Особливості розмежування феноменів національна безпека, цифрова безпека, цифровізація та цифрова трансформація

Джерело: авторська розробка

Інформаційна безпека є найконвенційнішим терміном [39–40; 53–57]. З одного боку, у науковій літературі існує досить чітке розуміння сфер застосування даного терміна (технічний контекст, питання доступу до інформаційних систем та безпека зв'язку [308]). З іншого боку, держави та їх уряди на доктринальному рівні закріплюють інформаційну безпеку аналогічно міжнародним підходам, у тому числі міжнародних організацій таких, як ООН, ЄС і НАТО. Однак, у певних випадках національні інституції чинять інакше. Прикладом може бути закріплення на нормативному рівні поняття інформаційної безпеки України, де концепція

інформаційної безпеки охоплює буквально «усе», що пов’язано з інформацією та інформаційним простором [60]. Для цілей цього дослідження ми спираємося на уніфіковане (міжнародне) розуміння інформаційної безпеки. На рівні концептуалізації також можна спиратися на окремі приклади національного доктринального закріплення такого терміну, що не має суперечити міжнародному.

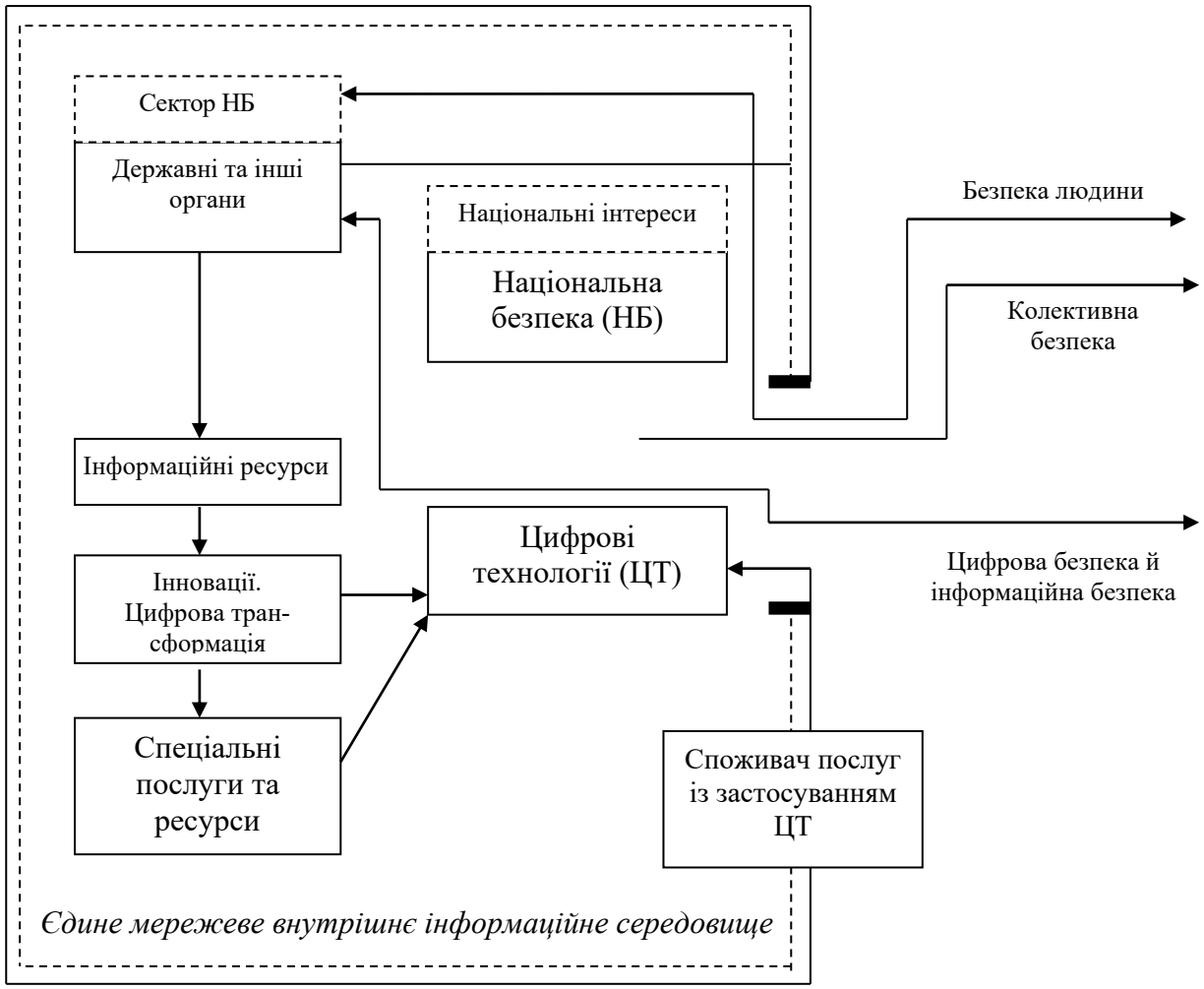

Рис. 1.3. Місце національної безпеки в системі публічного управління

Джерело: авторська розробка

Розглядаючи тематику цифрової безпеки, слід зазначити, що існує неоднозначність навіть на офіційному рівні щодо терміну цифрового та

кіберпростору. Наприклад, Міністерство оборони США у 2010 р. визначало такий простір як «глобальну галузь (домен) в інформаційному середовищі, що охоплює взаємозалежні мережі інфраструктур інформаційних технологій» [332], наповнюючи термін вкрай загальними та широкими конструкціями. Очевидно, що дане визначення не позбавлене недоліків, оскільки поза увагою залишаються положення теорії інституціоналізму.

Щодо змісту цифрової безпеки, то тут також ведуться численні дискусії як у теоретичній та практичній площинах. Найчастіше цей термін розглядають у дискурсі просторових та біологічних аналогій, при цьому використовуючи «військову мову» [136]. Наявність синонімічності на наднаціональному рівні, наприклад ініціатива ООН, що закріплює в резолюції 2341 (2017) Ради Безпеки напрями цифрової безпеки (обмін інформацією та захист об'єктів), не дає універсального розуміння. Однак цей термін закріплюється на нормативному рівні у різних країнах у єдиному ключі. Починаючи з 13.03.2024 року, цим ключем є обмеження застосування деяких цифрових технологій, що охоплюють алгоритми штучного інтелекту [341]. Власне, Європарламент прийняв перший у світі Закон «Про штучний інтелект». Розгляд його положень дав змогу стверджувати про важливість правового закріплення галузі цифрова безпека, а також її універсального розуміння для різних держав [27].

Однак наразі феномен цифрової безпеки є найменш концептуалізованим у логічному ланцюгу «національна безпека – інформаційна безпека – цифрова безпека». У науковій літературі поки відсутній єдиний підхід до визначення цифрової безпеки. Це, у свою чергу, унеможливлює її унікальність та відмінність від інформаційної та/або кібербезпеки. На цій підставі слушними є рекомендації дослідників, які визначають «цифровий контекст» безпеки [303], що оцифровується, спонукаючи до розгляду такого нового феномена. Однак відсутність повноцінної термінологічної та змістовної точності визначення такого

феномену дозволяє апелювати до його характеристики із урахуванням положень теорії інституціоналізму. Даний висновок нами зроблено з огляду на те, що держава є соціальним інститутом, відмінною ознакою якої є населення, правова база, державний апарат тощо. Вони, у свою чергу, складаються в окремі інституційні групи – правові, соціальні, державні, публічні тощо.

Зважаючи на вищевказане, повною мірою усвідомлюємо значущість феноменів «цифрова безпека», «цифрові технології» тощо з позиції комплексного забезпечення національної безпеки, їх взаємозв'язок та змістовну диференціацію. У зв'язку з чим уважаємо, що існує необхідність у більш детальному розгляді цифрових технологій у сфері національної безпеки, що становить об’єкт публічного управління.

1.2. Типологізація цифрових технологій і їх соціально-політичні та державно-правові ефекти на сферу національної безпеки

Прискорений розвиток цифрових технологій та їх упровадження у різні сфери життя суспільства зумовлює фундаментальні зміни не лише технологічного та економічного характеру, а й у сфері державної політики і публічного управління. Зміни у сфері комунікації, збирання та використання інформації, цифрової взаємодії держави з суспільством призвели до появи нових концепцій управління та політики: теледемократія [113], електронна демократія [152; 345], віртуальна демократія [268], електронний уряд [143; 249; 298], GovTech [209] та ін. Ці концепції розвивалися протягом останніх років. Однак наукова спільнота та політичні діячі виявилися не готовими до швидкого розвитку сучасних цифрових технологій (наприклад, складні математичні та статистичні алгоритми, машинне навчання, нейронні мережі, штучний інтелект, технологія блокчейна, технологія зв'язку 5G, технологія розпізнавання

осіб, великі дані тощо).

Масштабність і всеосяжний характер змін, що відбуваються в сучасному суспільстві, під впливом цифрових технологій ускладнює концептуалізацію «цифровізації» [254]. У рамках цього дослідження цифровізація (цифрова трансформація, діджиталізація) сприймається як комплексна система трьох взаємодіючих елементів, а саме:

1) інфраструктура (hardware) – комплекс технологій, які забезпечують обчислювальні, телекомунікаційні та мережеві потужності, реалізації цифрових товарів;

2) програмне забезпечення (soft) – сукупність програм, процедур, цифрових правил, системи обробки інформації та програмних документів (у тому числі, алгоритми, хмарні обчислення);

3) процес взаємодії технологій і користувачів, людей один з одним за допомогою технологій, а також взаємозв'язок технологій та їх системне функціонування.

Згідно з міжнародними звітами [335], значна частина національних урядів заявляють і реалізують національні програми та стратегії у сфері цифрової трансформації. Якість цифровізації при цьому залежить від спільних дій політичних інститутів і технологічних компаній. Ілюстрацією до цього твердження може бути приклад електронна участь у політичному порядку денному країни [226]:

– у країнах, де свобода онлайн-участі гарантується завдяки високоякісній технологічній інфраструктурі та демократичним політичним інститутам, існує високий рівень електронної участі (Великобританія, Австралія, США);

– країни з низьким рівнем технологічного розвитку та низькою політичною інституціоналізацією демонструють низьку електронну участь (Ангола, Єгипет, Сальвадор);

– у свою чергу, уряди країн Азії мають досить передові цифрові технології, але участь громадян в електронній сфері є низькою через

конкретні політико-інституційні механізми.

Як інструмент колективних процесів цифрові технології вплинули на традиційні державноуправлінські практики. Політичні інститути були змушені провести реформи (у контексті змінних процесів та механізмів спостерігається розвиток використання цифрових технологій) і водночас – встановити нові правила та стандарти для регулювання й контролю таких технологій. Ця потреба була зумовлена масштабами проникнення технологій, ступенем залучення людей в онлайн-середовище та зростаючим впливом «цифри» на повсякденні «реальні» процеси.

Протилежний підхід виявляється у безпосередньому стимулюванні політичними інститутами розвитку цифрових технологій. Іншими словами, рушійною силою цифровізації є «державна політика» (state policy), яка створює не лише умови, а й механізми для залучення населення до соціального та політичного порядку денного, використовуючи цифрові технології як інструмент забезпечення системи безпеки (соціальної та національної, які виходять від самого суспільства).

Вищезазначене демонструє складний характер відносин між політичними інститутами та цифровими технологіями. Незважаючи на те, що аналіз природи відносин виходить за рамки даного дослідження, важливо вказати, що в даному випадку «зіштовхуються» підходи технологічного детермінізму й ототожнення суспільно-політичної волі.

Більшість країн прагнуть формування єдиної політики у сфері цифровізації, приймаючи стратегії, національні програми та інші комплексні документи, які охоплюють все суспільно значимі сфери життя.

Простежується тимчасова тенденція – більшість звітів з цифровізації, електронного уряду та ін. публікуються протягом вже більше десятиліття (наприклад, індекс електронного управління ООН – з 2003 р.). Проте до цього державне регулювання сфери мало хаотичний, локальний чи частковий характер. Можливо, це пояснюється тим, що держави реагують на зміни постфактум. Власне, включеність та активний прояв суспільно-

політичної волі виникає лише після того, як використання цифрових технологій або досягло значних масштабів, або продемонструвало значні результати.

Суспільно-політична воля не завжди супроводжується формальним закріпленням у вигляді документа (через бюрократичні витрати, складності та специфіку прийняття та видання нормативно-правового акту, політичні ризики, пов'язані з формалізацією новаторських або не цілком популярних рішень тощо). З огляду на це можна визначити дискусійну тезу про феномен «суспільно-політичного дозволу» щодо застосування цифрових технологій: за реалізацією точкових програм цифровізації стоятиме локальне державноуправлінське рішення. Тобто застосування цифрових технологій може відбуватися без відома суспільно-політичних акторів/інститутів стратегічного рівня (тобто без залучення представників громадськості, об’єднань громадян та ін.). У цьому контексті спроби практикувати «технологічний детермінізм» первинно відбуваються на стадії узгодження. Таким чином, «суспільно-політичний дозвіл» (або «new public menedgement») як акт вираження політичної волі на рівні соціуму апріорі (хоч і опосередковано) присутній у практичній реалізації стратегії цифровізації, виявляючись локально.

На жаль, непоодинокими є випадки, коли в країнах із низьким рівнем використання цифрових технологій простежується стимулювання розвитку цифровізації «згори». Поясненням такого явища може бути те, що країни, у яких напрацьовано менший досвід застосування цифрових технологій (на рівні розробки, комерціалізації тощо), більше орієнтуються на закордонний досвід. Відтак, ці країни проводять цифровізацію «згори донизу», але саме суспільно-політична воля стимулює висхідний розвиток цифровізації в країні. У свою чергу, у країнах з вищим рівнем застосування технологій ми можемо спостерігати елементи державно-приватного партнерства, в якому розвиток не стимулюється безпосередньо, але він підтримується урядами, які реагують на соціальний запит. У таких

кейсах технологічні компанії є драйвером змін і, по суті, викликають трансформацію, що розглядається, на перших етапах [70; 282; 315]. Однак це не свідчить про домінування «технологічного детермінізму». Аналіз літератури та політичних практик явно вказує, що будь-які технологічні нововведення супроводжуються політичними рішеннями.

Зазначене спонукає розглядати механізм взаємодії політики (у широкому розумінні) і цифрових технологій за принципом роботи зубчастих коліс, при якому природа сполучення ґрунтується не на фактичному примушуванні та безпосередньому стимулюванні, а на своєрідній тяговій силі, де зусилля, що додається, на одне зубчасте колесо обертає друге. Однак застосування сили до одного зубчастого колеса має бути достатнім для початку другого. Розвиток цифрового технологічного ринку, за належної результативності, починає «тягнути» політичну владу у бік трансформації та модернізації. І навпаки, сильна політична інституціоналізація може призводити до розвитку ринку інновацій, зокрема цифрових технологій. Зазначена теза пропонується як ширша рамка розгляду взаємодії політики та цифрових технологій.

Таким чином, можна зробити висновок, що феномен цифровізації є політичним процесом, який безпосередньо залежить від якості та функціонування інститутів.

Удосконалення цифрових технологій та їх впровадження у різні сфери життя суспільства знаходять формальне закріплення у стратегіях та політиках «цифровізації» як на національному, так і на міжнародних рівнях [330]. З 1971р. в академічному середовищі почалося обговорення соціальних наслідків «цифровізації суспільства» [343, с. 30] у контексті розгляду комп'ютерних, обчислювальних та цифрових можливостей у гуманітарних дослідженнях [там же]. З цього моменту сформовано широке науково-дослідне поле, в якому все більше уваги приділяється процесам перетворення/трансформації структури цифрових технологій. їхньому формуванню, а також впливу на сучасний світ.

Дослідження вказують на нову цифрову систему засобів масової інформації та комунікацій як способу пояснити та зрозуміти більшість аспектів сучасного соціального та політичного життя. Учений Кастельс [151] розглядає цифровізацію як одну з визначальних характеристик сучасної доби. Науковець Ван Дейк вказував, що вперше в історії у нас складається єдина комунікаційна інфраструктура, яка пов'язує всі види діяльності в суспільстві [340]. Така комунікаційна система повністю характеризується «новими медіа» [40], які стрімко і кардинально змінюють традиційні/звичні соціальні та політичні процеси.

Переформатування соціальної, економічної та політичної сфери виходить за межі національних політик держав. Учена С. Сассен ще в 1998 р. вказувала, що зростання глобалізації та розширення економік за межі національних кордонів проходили за допомогою цифровізації [301]. Цифровізація та глобалізація економіки змінюють традиційне уявлення про національний суверенітет, коригують уявлення про «матеріальність», тобто цифровізація створює середовище, яке імітує або поєднує різноманітні сфери діяльності, унаслідок чого таке цифрове середовище розглядається як «узагальнене середовище», що поєднує «різні форми інформації» [134, с. 26]. Зростання цифрових технологій та нових медіа «спричинило перегляд того, що таке цифрове середовище, тому що комп'ютер може відтворювати чи моделювати всі інші відомі носії» [227, с. 217].

Вплив цифрових технологій проявляється на чотирьох основних рівнях існування суспільно-політичної та соціальної системи:

1. Інфраструктурна конвергенція [340], як основа всіх суспільно-політичних процесів і технологій, де «будь-яка мережа може використовуватися для передачі всіх видів цифрових сигналів» [312, с. 1320]. Це означає, що один засіб – кабелі або радіохвилі – може забезпечувати надання послуг, які в минулому надавалися іншими способами [285, с. 29]. Безпосередньо інфраструктурні зміни дозволили

сформувати нові концепції управління та відправлення політики: «теледемократія» (Tele-Democracy) у 1960-ті рр. [162], «електронна демократія» (E-democracy) та «віртуальна демократія» (Virtual Democracy) [268], «електронний уряд» (E-government) [143; 249; 298], GovTech та ін.

2. Конвергенція пристрою як поєднання кількох мультимедійних пристроїв в одне ціле [312, с. 1320]. У цьому випадку йдеться про появу нових універсальних пристроїв і технологій (наприклад, сучасний смартфон замінює собою безліч пристроїв: телефон, комп'ютер, камера, аудіорекордер, календар, калькулятор, блокнот тощо). Зазначене безпосередньо впливає формування нових способів і методів відправлення політик та реалізації державного управління.

3. Конвергенція в послугах [340]. Яскравим прикладом може бути ідея «суперсервісу» Дія на прикладі сайту та додатку державних послуг, де в одному цифровому просторі зосереджені різні функції надання державних послуг, а також контрольно-наглядові та фіскальні функції держави. Подальший розвиток сфери цифрових послуг призводить до «розмивання» відносин держави-суспільства: змінюються «взаємно-однозначні відносини, які існували між середовищем та його використанням» [285, с. 23]. Іншими словами, тепер не тільки один пристрій може виконувати декілька функцій, але й тепер може бути надана «послуга, яка надавалася в минулому будь-яким середовищем, чи це мовлення, преса чи телефонія – тепер вона може бути представлена декількома різними фізичними способами» [там само].

4. Ринкова конвергенція, що виражається в консолідації (змішуванні/об'єднанні) «обчислювальних, телекомунікаційних, медіа та інформаційних секторів» [181]. Також відбувається розмивання меж у відмінностях між інфраструктурою та послугами, програмним забезпеченням та медіаконтентом [312, с. 1321]. У результаті відбувається як розширення е-бізнесу – компаній, які виходять на кілька цифрових ринків та/або секторів, формуючи таким чином нові інституційні

парадигми (так звані компанії BigTech – Facebook, Google, Amazon тощо) – так і фундаментальні зміни існування держав (кейс електорального процесу 2016 р. у США, що має великий вплив на внутрішню політику держави) та моделі міжнародних відносин (China–United States trade war 2018-2020).

Таким чином, цифровізація позиціонується як стабілізуюча-дестабілізуюча сила в соціальних і державно-політичних сферах.

Радикальні зрушення спостерігаються у сфері створення та виробництва культури та знань, що становлять базис соціальної безпеки. Учений Ю. Бенклер стверджує, що «рівноправне» та «соціальне» виробництво завдяки цифровизації може вперше сформуватися в глобальному масштабі [133]. Завдяки витратам на виробництво і розповсюдження цифрової інформації, що швидко знижуються, колективне виробництво починає витісняти інші ринкові механізми виробництва знань і культури. Створювати та розповсюджувати будь-який контент, починаючи від фільмів, знятих на мобільний телефон, до політичних коментарів, стало максимально просто та доступно практично всьому населенню світу. Учений Ю. Бенклер стверджує, що ці нові неринкові та кооперативні способи праці становлять економічну цінність, яка все більше конкурує із цінністю національних держав та бюрократії минулого [там само]. Іншими словами, усе нові цифрові форми виробництва культури та знань відбуваються, минаючи формальні структури державного управління.

Аналогічні наслідки цифровізації простежуються у процесах політичної участі. Б. Бімбер із колегами з Каліфорнійського університету встановили, як змінюється політична активність в інформаційному середовищі [139]: значно розширився вибір способів та можливостей політичної участі, змінилися стимули та форми взаємодії держава-суспільство. Багато форм взаємодії ґрунтуються на використанні цифрових даних та ускладненої аналітики. Науковець Д. Карпф вказує на

використання цифрової аналітики як форму «пасивного демократичного зворотного зв'язку» [233]. Громадські організації (як у дослідженні Д. Карпфа), компанії (як у кейсі з Cambridge Analytica) та держави вибудовують нові форми взаємодії на основі «trace data» та новими технологіями аналізу [там само]. У такому разі цифрові технології використовуються для відстеження та оцінки того, що важливо суспільству, організації, політичним акторам.

Ще ширше Д. Карпф показує, як змінилися самі структури, процеси та форми взаємодії з урахуванням інформаційних можливостей цифрових медіа [там само]. Більше того, кейси «Los indignados» в Іспанії та «Occupy Wall Street» у Сполучених Штатах Америки демонструють те, як цифрові технології сприяють формуванню колективних дій без лідера та централізації замість формального керівництва та організаційних структур. Змінюється сама структура комунікації, поєднуючи громадське і окреме вираження. Таким чином, роль і місце офіційних організацій та офіційних представництв влади зміщується, а їх позиції займають нові комунікаційні структури. Власне кажучи, персоналізовані розповіді замінюються колективними діями з децентралізацією думки з допомогою цифрових технологій.

Цифрові технології та нові медіа також відкрили нові форми транскордонної політики, розширили політичне поле для більшої кількості організацій та приватних осіб (з обмеженими політичними ресурсами), збільшили масштаби дій та інформацію, змінили локальні, національні та міжнародні політичні інституції. Дані явища були продемонстровані у дослідженні С. Сассен, яка, аргументуючи зміни у конфігураціях «території, влади та прав» [301], наголошує на важливості відділення цифровізації від Інтернету. Наприклад, у сфері фінансів глобальні зміни відбуваються не тільки завдяки Інтернету, а й зростанню «виділених приватних цифрових мереж», які відіграли свою роль у посиленні впливу глобального капіталу, в тому числі дозволяючи недержавним ринковим

силам посилювати фінансовий вплив на національні уряди та впливати на формування політики. Позиція С. Сассен показує, що цифрові та нецифрові сфери взаємопов'язані одна з одною [там само]. Цифрова комунікація формується розрізненими соціальними, політичними, економічними та культурними силами та контекстами. Глобальні цифрові спільноти переконфігурували аспекти території, влади та прав, але вони глибоко залучені до сили, які не пов'язані зі ЗМІ, та вкорінені на локальних рівнях. Учена С. Сассен показує, як у цифровому вигляді перероблені «просторово-часові порядки» [там само], у тому числі проти раціоналізації, стандартизації та бюрократизації.

Широке поширення має припущення, що соціальна й інституційна інфраструктура змінюється під впливом мереж зв`язку [340], при цьому цифрові мережі викликають величезні зміни у логіці та структурах глобальної соціальної організації. Учені стверджують, що зростаюча цифровізація соціальної організації призвела до «мережевого суспільства». Хоча існує багато суперечок про те, що є одиницею мережевого суспільства, – мережі [151], окремі особи [340] або «мережеві групи») – існує консенсус, що соціальні структури та глобальна цифрова інфраструктура безпосередньо пов’язані. Іншими словами, проникнення цифрових технологій у соціальну та державно-політичну структуру є настільки сильним, що технологія ототожнюється із суспільством, а суспільство не можна зрозуміти чи уявити без його технологічних інструментів [151].

Зазначимо, що ця проблематика перебуває на стику міждисциплінарності. Ми не можемо стверджувати, що всю складність трансформації, а також її ефектів можна охопити й окреслити в рамках суспільно-політичної науки. Адже питання виходять далеко за межі одного наукового напряму, і найчастіше виявляються в симбіозі наук і напрямів, починаючи від очевидного прояву в поведінковій економіці (на стику психології, когнітивної науки й економіки) і закінчуючи складними

підходами семіотики [29] та теорії еволюціонізму.

Так, в останні роки з’явилися напрями когнітивної науки, що фокусуються на дослідженнях distributed mind, distributed conscience, distributed language, а також розподіленої суб'єктності (distributed subjectness) [29]. Масштаби та форми трансформації дозволяють спостерігати сегментацію об’єктів та суб’єктів: традиційні підходи, комп'ютеризовані елементи, комбіновані елементи з підключеними інтерфейсами, а також явища (або прояви) систем штучного інтелекту (що належать до «сильних» систем з потенціалом розвинутись до рівня усвідомленості). Звісно, такі предметні поля існують і значно насичують дискусію про трансформацію та ефекти цифровізації. Однак для цілей даного дослідження (і щоб не розмивати фокус) ми не вторгатимемося в цей простір, а сфокусуємось виключно на інституційному прояві політичного.

Технологічний аспект також розглядається в предметній галузі досліджень науки та технологій (Science and Technology Studies – STS). Крім того, зв’язок технології штучного інтелекту з владою та безпекою можуть бути підпорядковані концептуальним підходам STS [282]. Із 2021 р. активізувався рух щодо застосування двох таких концепцій для аналізу динаміки, процесів, практики та нетрадиційних політичних акторів в управлінні. Також дослідження технологій може бути підпорядковане предметній галузі досліджень дифузій інновацій (Diffusion of Innovation – DOI). Наприклад, конкретна цифрова технологія може розглядатися як засіб для інновації (у 2022 р. аналізом технологічних переваг технологій штічного інтелекту відбувається в поєднанні зі стійкими економічними інноваціями як рушійної сили для їх ефективного впровадження). Це значно розширює розуміння ролі та місця технології, у тому числі й у сфері безпеки. Окремим важливим напрямом є прийняття технологій (Technology aceptance/adoption model – TAM), яке фокусується на дослідженні суспільного сприйняття та прийняття технологічних моделей і

рішень. Такий підхід дозволяє моделювати «прийнятність» користувачами з погляду поведінкового наміру використовувати продукти на основі технологій. Ми усвідомлюємо значимість зазначених напрямів, саме тому розділах з концептуалізацією цифрових технологій і саме технології штічного інтелекту частково спиралися на дослідження STS і TAM. Однак прагнемо не розмивати предметне поле дослідження, чітко фокусуючись рамками політичної науки та досліджень безпеки.

Таким чином, для цілей даного дослідження застосовується концептуалізація цифровізації онтологічно як прийняття, використання й імплементація цифрових технологій у різних сферах функціонування бізнесу, держави, що окреслює відповідні вектори цифрової політики та публічного управління. При цьому вважаємо за доцільне розмежовувати терміни «оцифрування» та «цифровізацію», розглядаючи цифрові технології як самостійний тип/вид технологій [14]. При цьому цифровізація охоплює не тільки технологічні досягнення, а й інституційні зміни такі, як стандарти якості, мережа Інтернет та безпека даних, фінансові та правові основи, а також науковий, інноваційний та людський капітал [218].

Більше того, багато країн або заявляють, або серйозно підтримують політику, спрямовану на цифрову трансформацію економіки та соціально-політичної сфери [132]. Як правило, політика цифрової трансформації в країні набуває форми національної стратегії [211] або національної програми. Практично у кожній стратегії чи програмі є план стати лідером у програмі цифрової трансформації через 5–10 років (не є виключенням в цьому й Україна). Таким чином, формується глобальна конкуренція країн у галузі цифровізації.

Отже, проведений аналіз демонструє ефекти від розвитку цифровізації, які пов’язані зі суттєвими перетвореннями як соціально-політичного характеру, так і економічного, а аткож публічного та приватного секторів. Розгляд цифровізації як суспільно-політичного

процесу надає широкі можливості для аналізу її ефектів. У цьому контексті наголошуємо, що сам процес не є суто технологічним. Природа цифровізації складніша і пов'язана з сучасними та новоствореними інститутами (правовими, соціальними, політичними та ін.). Погоджуємося з вченними В. Баштанником, О. Баштанник, С. Домбровською, Р. Лукишою та ін., що при такому розгляді запропонована Нортом «інституційна матриця» найточніше охоплює обсяги та зміст феномена цифровізації.

Визначення технологій при різноманітті технологічних рішень, виходить із такого: 1) ідентифікації конкретних технічних проблем; 2) систем; 3) технологічних процесів практичної реалізації, адже технологія включає знання та навички про ці три складові елементи [304]. Створення, обробка та передача цифрових даних визначає технічну проблему сфери цифрових технологій [244]. Таким чином, цифрові технології – це знання, навички, технологічні та технічні рішення для створення, обробки, передачі та використання цифрових даних, а також системи та процедури для їх практичної реалізації [182].

Масштаби, багатогранність та різноманітність цифрових технологій ускладнюють однакову оцінку всього процесу розгортання цифрової трансформації. Цифрові технології включають такі *елементи*: створення цифрового рішення та нової інформації/даних, обробка та аналіз даних за допомогою цифрової технології, передача даних та інформації, застосування цифрової технології та результатів її використання. Взаємодія цифрових технологій реалізується у трьох формах:

1) соціальна – населення є одержувачами, а також трансляторами інформації;

2) фізична – фізичні пристрої (машини, інструменти, інші технології) транслюють, передають інформацію та дані;

3) цифрова (віртуальна) – програмне забезпечення, сервіси та ін. [74].

Окремим елементом реалізації цифрових технологій є цифрові

компетенції [142], які відображають ефективність та результативність застосування цифрових технологій у соціальному, політичному й економічному житті суспільства. Для успішності реалізації цифрові технології повинні відповідати характеристикам якості (змістовне функціонування технологій, націлене на високу якість та/або високу доступність ринку), продуктивності (розширення функціональної сфери та покращення функціональності) та зручності використання (працездатність цифрового продукту/технології).

Виділяються такі класи сучасних цифрових технологій [182]:

– технології зв’язку (connectivity) – усі цифрові технології, функціональні можливості яких призначені для надсилання та отримання цифрових даних (технологія зв'язку 5g, Bluetooth та ін.);

– технології зберігання (storage) – цифрові технології для зберігання даних, де сама технологія не вносить змін до даних (бази даних, хмарні технології тощо);

– технології аналітики (analytics) – технології аналізу та оцінки інформації (виявлення залежностей та закономірностей), доступної у формі цифрових даних (машинне навчання, нейронні мережі та ін.);

– технології виготовлення (fabrication) – цифрові технології, які створюють фізично вимірюваний результат на основі цифрових даних (адитивне виробництво – 3D друк);

– технології візуалізації (visualisation) – технології візуальної презентації цифрових даних (технології доповненої реальності);

– інтерактивні технології (interactivity) - цифрові технології, які підходять як для створення, так і для використання цифрових даних, де функціональна спрямованість залежить від конкретного випадку застосування (планшетний комп'ютер може використовуватися людьми як для введення даних/інформації, для створення цифрових даних, так і для відображення даних на пристрої). Цей клас є перетином технологій візуалізації та технологій інтерфейсу;

– технології інтерфейсів «людина-машина» (human to machine (H2M) interface) – технології «зв'язку» між людиною та цифровим світом для створення цифрових даних на основі інформації, яка спочатку доступна людям (наприклад, інтерфейс «мозок – комп'ютер», який створює цифрові дані на основі інформації, яка є в людському мозку);

– сенсорні технології (sensoring) – цифрові технології, що генерують цифрові дані на основі фізичної геометрії або фізичних рухів. Використовуючи цей технологічний клас, можна вимірювати як геометрію об'єкта (наприклад, довжину чи ширину), і фізичні (механічні) руху (наприклад, швидкість руху чи переміщення). Цифрові дані є носіями виміряної інформації та доступні як вихідні дані цифрової технології (3D-сканер, який може перетворювати геометрію фізичних об'єктів у цифрову 3D-модель).

Альтернативним підходом до класифікації цифрових технологій може бути розгляд їх у концепції рівнів проникнення та взаємодії. Така типологія виділяє 4 класи технологій [135]:

– пристрої (device level);

– мережа (network level);

– наповнення/зміст (content level);

– Сервіс (service level).

Кожен зазначений рівень поєднує схожі за своїми функціональними властивостями та технічними характеристиками цифрові технології. Так, пристрої включають прикладні продукти та інфраструктурні рішення; мережі – технології обміну інформацією та даними між об'єктами; контент – безпосередньо технології «змісту», функціонування яких пов'язане з отриманням (введенням) та подання (висновком) даних, а також їх використання та обробки; сервіс – технології надання послуг за допомогою цифрових майданчиків та платформ.

Сучасні дослідження [200; 233; 282] показують, що цифровізація державно-управлінських процесів розвивалася еволюційно та демонструє

досить складну структуру, запозичуючи позитивний досвід цифровізації управлінських процесів з приватного сектору. Аналіз такого еволюційного процесу можливий завдяки вивченню: 1) доступності цифрових технологій; 2) упровадження цифрових технологій; 3) інституціоналізації методів цифрового управління, визначення ключових технологій, їх ролі та значення, а також формулювання значущості технологічних взаємодій в єдиній концепції.

Для цілей даного дослідження типологізація та виділення основних (умовно, поширених та ключових) типів цифрових технологій ґрунтується на двох документах: 1) звіті Європейської парламентської дослідницької служби «Десять технологій, які можуть змінити наше життя: політичні наслідки та реалізація політики» [212]; 2) звіті про цифрову економіці» ООН [335]. На підставі чого було виділено такі типи цифрових технологій:

– великі дані (Big Data);

– штучний інтелект (Artificial Intelligence);

– Інтернет речей (Internet Of Things);

– автоматизація та робототехніка (Automation & Robotics);

– 3D друк (3D Printing);

– віртуальна валюта та блокчейн (Virtual Currency and Blockchain);

– хмарні обчислення (Cloud Computing);

– технологія зв’язку нового покоління – 5G.

Очевидно, що розглянута типологізація цифрових технологій відображає складність і специфічність цифрових технологій. Ця робота передбачає врахування найбільш гнучкого підходу, що дозволяє одержати свободу в емпіричному аналізі. Безумовно, дискусії щодо концептуалізації технологій, а також їх типологізації можуть прийти до зіткнення. Однак теоретичний аналіз, представлений у роботі, дозволяє з упевненістю стверджувати, що: 1) цифровізація є політичним процесом (попри значимість технологічної складової); 2) у процесі реалізації значну роль відіграють інститути (їх якість, адаптивність та ін.); 3) сам процес

цифровізації безпосередньо пов'язаний і залежить від застосування конкретних типів цифрових технологій.

1.3. Механізми публічного управління у сфері національної безпеки в умовах впливу технологій цифровізації: структура та класифікація

Цифрові технології є невід'ємною частиною існування сучасної світової спільноти та глобальної тенденції світового розвитку. У цьому зв'язку можна сміливо стверджувати, що цифровізація та національна безпека держави є взаємозалежними та взаємозалежними явищами, які становлять базис для формування гібридного поняття – цифрова безпека. Власне вона перебуває на стику обох понять – національної безпеки та цифровізації, сприяючи розвитку фундаментальної та прикладної науки. У цьому зв'язку потрібно дати відповіді на такі питання: 1) яка роль цифровізації як інструменту забезпечення національної безпеки; 2) чи може цифровізація стати загрозою національній безпеці; 3) які фактори, що гальмують розвиток цифрових технологій, які потребують державного втручання, а, відтак, які необхідно застосовувати для цього механізми публічного управління.

У XXI ст. цифрові технології стали одним із головних драйверів прогресу та ресурсів економічного розвитку та протистояння [289]. Інформаційно-комунікаційні технології визначають динаміку розвитку світової економіки та низку змістовних аспектів відносин між державами [там само]. Однак цифровізація – не лише джерело довгострокового економічного зростання країни й інституційний інструмент економічної конкуренції на світовій арені (наприклад, за допомогою підвищення конкурентоспроможності країни на ринку товарів та послуг, рівня життя населення та ін.), а й фактор суверенності та стабільності держави, її

національної безпеки [283; 284].

Водночас, не лише цифровізація впливає на національну безпеку держави, а й державна політика, яка має у т.ч. «дерево цілей» щодо забезпечення національної безпеки, безпосередньо впливає на темпи та сфери розвитку цифровізації [36; 282]. Таким чином, можна говорити про взаємодію й узаємний вплив цифровізації та національної безпеки [317].

Слід погодитися з К. Лободенко [47], що одним із каталізаторів модифікації суспільних відносин та державної політики служить впровадження цифрових технологій у господарську практику та систему суспільних взаємодій, що набувають форми правовідносин, тобто проходять процедуру легітимації. Цифрові технології є «драйвером» державних інноваційних процесів, орієнтованих формування цифрової економіки та забезпечення національної безпеки, а також суверенності держави. Інформація, інформаційні технології, інформатизація всіх сторін соціуму привносить такі зміни в життя індустріального та постіндустріального суспільства, які вимагають змін, часом докорінних, в інститутах організації управління та права.

Апріорі цифрові технології не повинні негативно впливати на національну безпеку безпосередньо, а вплив має відбуватися через вплив на динаміку та вектор соціально-економічного прогресу, тому країни, які «відстають» за темпами та масштабів цифровізації, стикаються з рядом загроз національній безпеці. Серед таких загроз можна виділити, наприклад, наздоганяючу роль світової економіки, обмеження перспектив інноваційного розвитку, зниження конкурентоспроможності компаній (особливо у порівнянні з транснаціональними корпораціями, орієнтованими на найбільш економічно розвинуті країни), обмеженість інструментарію для забезпечення національної безпеки тощо [283].

Особливого значення цифрові технології набувають у період, коли та чи інша держава стикається з значними викликами, як, наприклад, погіршення санітарно-епідеміологічної обстановки у світі на початку

2020 р., зумовлене поширенням коронавірусної пандемії інфекції нового типу – COVID-19. За цим прикладом стає очевидно, що об’єктивна й оперативно отримана інформація, здебільшого через Інтернет, стає життєво необхідною. Подібні обставини вимагають також швидкого й ефективного реагування з боку світової спільноти (на рівні держав, інтеграційних об'єднань, окремих міжнародних організацій тощо), що прискорюють реалізацію та розвиток накопиченого потенціалу використання інформаційних та цифрових технологій.

Так, нові методи в охороні здоров'я, як, наприклад, інтернет-медицина, он-лайн консультації, телемедицина тощо, обговорювалися в науковій літературі давно [159], але впроваджуються у практику тільки останніми роками. Це зумовлено впливом позасистемних, неочікуваних факторів, що створили нові умови – обмеженої суспільної життєдіяльності.

Тим не менш, у відповідь на такі глобальні загрози, як потепління клімату, забруднення довкілля, недотримання прав людини відбувається повсюдне поширення інформаційно-комунікаційних та цифрових технологій, особливо у сферах освіти, державного управління, правосуддя, онлайн-комунікацій, електронної торгівлі, фінансів тощо [33; 47; 68; 91; 98; 102–103]. Це, у свою чергу, викликає необхідність удосконалення чинного законодавства з метою приведення його у відповідність існуючим реаліям, збільшення фінансування у сферу інформаційних та цифрових технологій, підвищення ступенязахисту персональних даних тощо [там само]. Цей процес яскраво виявився у різних державах, у т.ч. в Україні, під час пандемії. З введенням державою обмежувальних заходів, вітчизняні суди призупинили розгляд більшості справ, а для забезпечення доступу до правосуддя почали проводити онлайн-засідання. Звісно ж, що цей процес не буде припинено зі зняттям обмежувальних заходів, а онлайн-правосуддя отримає розвиток [297]. Крім того, на період карантину всі освітні установи були переведені до режиму електронно-дистанційного навчання, для чого державними органами були розроблені інтернет-платформи, які

сприяють подібному навчанню [140].

Важливою запланованою законодавчим зміною в нашій країні, викликаною одним із заходів, що перешкоджають поширенню пандемії COVID-19, а саме: тривалою відсутністю працівників на виробництві, є зниження оподаткування у сфері інформаційних технологій, що традиційно відрізняється високою мобільністю. Це дозволить створити в Україні сприятливі податкові, фінансові та правові умови підвищення конкурентоспроможності країни та запобігання «податковій міграції» ІТ – спеціалістів до інших юрисдикцій [64].

Вищевикладене свідчить про зацікавленість держави у розвитку цифровізації задля забезпечення національної безпеки й інтересів суспільства. Проте чи цифровізація може стати загрозою національній безпеці.

Як і в будь-якого соціально-економічного явища, у цифровізації є не тільки позитивні сторони, а й приховані загрози, які потенційно можуть завдати шкоди національній безпеки загалом і системі публічного управління зокрема в разі, якщо вчасно не будуть взяті під контроль питання негативного впливу цифровізації на вищевказані сфери. Як найбільш очевидні слід назвати загрозу економічній стабільності держави та суспільства через поширення неконтрольованих коштів і загрозу соціальної дестабілізації через зміни ринку праці [там само]:

1)крипто валюта. Криптовалюта – це умовна назва зашифрованого нерегульованого цифрового активу, що використовується як аналог валюти в обмінних операціях. Криптовалюта не має фізичної форми, вона існує тільки в електронній мережі як різновид оцифрованих даних [297]. Банки, а, отже, і держава практично не можуть регулювати емісію криптовалюти, а тому такі фінансові інновації, у т.ч. так звані криптотехнології, розцінюються як загроза національній безпеці.

Під час розв’язання цієї проблеми слід виділити чотири аспекти. Перший з них полягає в тому, що саме криптовалюта найчастіше

використовується для легалізації незаконних доходів, фінансування терористичних організацій та інших незаконних операцій. Злочинців приваблює анонімність розрахунків криптовалютою, а також труднощі, майже неможливість, відстеження операцій, які у криптовалюті [165].

Другий проблемний аспект пов'язаний із децентралізованою природою криптовалюти (відсутність єдиного емітента такої валюти і, як наслідок, її екстериторіальність та неможливість підпорядкування будь-якій юрисдикції). Капіталізація криптовалюти зможе суттєво впливати на економіку країни і навіть може потенційно підірвати суверенітет та економічну незалежність держави як єдиного суб’єкта, наділеного правом грошової емісії й організації грошового обігу. Це, у свою чергу, може спричинити інфляцію, оскільки фінансові інновації прискорюють темпи проходження операцій, що підвищує швидкість обігу грошей та, як наслідок, прискорює процес інфляції.

Третій проблемний аспект пов’язаний із так званими «скам-проєктами», які виражаються у створенні шахрайських інвестиційних схем за допомогою використання криптовалюти. Криптовалюта, будучи високо ризиковим активом, може потенційно призвести до втрати коштів пересічними громадянами при її використанні у вигляді засобу платежу та накопичення, що, у свою чергу, негативно позначиться й на функціонуванні держави. У зв’язку з цим, держава має брати на себе роль регулятора, що захищає права інвесторів від купівлі «спам-токенів», громадян при здійснені фінансових накопичень та ін. [165].

Заключний, четвертий, проблемний аспект пов’язаний із фіскальною функцією держави, адже криптовалюта є інструментом, сприятливим для обходу процесів оподаткування. Криптовалюта є інструментом, що швидко розвивається, створюючи ситуацію, в якій правове регулювання (у т.ч. податкове) суттєво відстає від розвитку цифрових технологій, що унеможливлює отримання значних податкових надходжень до бюджету держави від операцій з криптовалютою.

Однак у сучасних реаліях неможливо ігнорувати популярність та затребуваність криптовалюти, тому державам, зокрема, й Україні, ще належить розробити грамотне правове регулювання цієї галузі, де має бути дотриманий баланс між національними інтересами та безпекою держави, а також первісною природою криптовалюти, щодо якої неможливий тотальний контроль, оскільки це зруйнує всю ідею та сенс її існування;

2) ринок праці. Одним із дискусійних питань є наслідки цифровізації для соціального розвитку та публічної безпеки в цілому, а саме: як впровадження нових технологій позначиться на ринку праці. Найчастіше висловлюються позиція про те, що роботизація й автоматизація праці можуть спричинити скорочення робочих місць та, як наслідок – зростання безробіття, падіння рівня життя значної частини населення, зниження показників народжуваності, збільшення масштабів злочинності та подальше загострення соціально-економічних протиріч у суспільстві [62; 64]. Це побоювання простежується на прикладі технологічних революцій, які відбувалися раніше в історії, що неминуче призводило до скорочення робочих місць (аж до зникнення окремих професій) і зміни вартості робочої сили. Так, наприклад, зникли такі професії (про існування яких мало хто пам’ятає взагалі), як льодоруб, писар, плотогон, людина-будильник, оператор-комунікатор, шляхоукладач та багато інших [там само].

Історично роботизація та використання новітніх технологій насамперед впливала на ті професії, які не вимагають високої кваліфікації найманого працівника або пов’язані з виконанням виробничих задач. Обумовлюється це тим, що роботизація та використання новітніх технологій підвищує продуктивність певної діяльності, зниження витрат і здешевлення виробництва товарів [там само]. Однак у XXI ст. починають з’являтися прогнози про те, що роботу через використання новітніх технологій можуть втратити й працівники розумової праці – юристи, офісні та публічні службовці, системні адміністратори та ін. [там само].

Звісно ж, що подібні «апокаліптичні» прогнози не повною мірою відповідають дійсності та значно перебільшені. Перша причина в тому, що для підвищення продуктивності виробництва товарів і надання послуг потрібно тривалий період після впровадження новітніх технологій. Прикладом може бути використання кас самообслуговування, які на початкових етапах своєї роботи не тільки не підвищують продуктивність, а й вимагають залучення нового персоналу, який допомагає клієнтам «освоювати» технологічні новички. Крім того, упровадження новітніх технологій вимагає проходження тривалого випробувального періоду для забезпечення належного рівня безпеки для їхнього повноцінного функціонування без допомоги людини (прикладом може служити безпілотний транспорт), а найчастіше й розробки відповідної нормативно-правової бази, що також потребує значного часу.

По-друге, у зв’язку з тим, що роботизація й автоматизація виробничих процесів підвищує продуктивність, тим самим збільшуючи прибуток, компанії починають прагнути до розширення власного бізнесу. Це вимагає залучення нових співробітників шляхом створення додаткових місць роботи. Таким чином, у даному випадку слід говорити не про потенційне зростання безробіття населення, а про його перекваліфікацію. Крім того, найчастіше автоматизація зачіпає не всю професію в цілому, лише окремі функції, що виконуються працівниками в межах професії.

Найпомітніше та парадоксальне явище в проблемі зайнятості у зв’язку з цифровізацією – це так звана поляризація. Таким чином називають вимивання середнього шару працівників за одночасного зростання зайнятості у інших стратах (соціальних групах). Такий процес поляризації був спочатку відзначений у країнах ОЕСР [197], фахівці вказують, що головною причиною поляризації є цифровизація й автоматизація [108]. Можна припустити, що в основі цього явища знаходяться соціальні причини, а саме: до середнього класу відносяться ті, хто почувається здатним робити не найпростішу роботу, але у них немає

належної можливості освоїти цифрові навчики й операції;

3) кіберзагрози. Термін «кіберзагрози» використовується для позначення потенційно злочинних дій проти інформаційної системи держави [27; 36; 74], тому вони можуть виявлятися й в економіці, й у роботі публічних службовців і приватного сектору. При цьому й суб'єкти, й об'єкти злочинних кібердій дуже різноманітні. Суб'єктами можуть бути індивіди, які прагнуть отримати незаконний доступ до банківських баз даних, а можуть бути й держави, які навмисно завдають шкоди іншій країні (як-то вчиняє рф проти України); об'єктами завжди виступають інформаційні системи, але вони, в одних випадках, можуть належати громадянам і задовольняти їхні інтереси, а в інших – виконувати функції державного управління чи підтримання нормальної життєдіяльності держави.

Кіберзлочинність почалася з елементарного пограбування, тобто заволодіння чужою власністю шляхом обману чи шахрайства. Уже у XXI ст. хакерські атаки почали застосовувати як засоби ворожого впливу на держави. Наявні дані про те, що можливостями такого впливу володіють більше тридцяти держав. Однак події з руйнуванням «веж-близнюків» на Манхеттені показали, що складні технологічні структури можуть опинитися в руках приватних осіб і використовуватися ними для ворожих дій проти держав [205].

Усе це призводить до необхідності залучення додаткового інвестування (як бюджетного, такм і приватного) задля забезпечення інформаційної та цифрової безпеки. В умовах, коли окремі підприємства нездатні самостійно знайти джерела для фінансування, кіберзагрози можуть стати не лише фактором стримування цифровізації окремих галузей, а й потенційною загрозою національній безпеці всієї держави (залежно від обраного для кібератаки об'єкта або відомостей різного ступеня значущості та секретності) [272].

Необхідність забезпечення кібербезпеки є глобальною проблемою, а

також проблемою окремо взятої держави, оскільки сьогодні з кіберзагрозами стикається кожна держава, навіть така, яка має незначні інформаційні та цифрові технології у своєму розпорядженні.

Наведені дані показують, що боротьба з кіберзлочинністю – це складна проблема, яка не може бути вирішена звичними засобами. Необхідне досягнення організаційно-правового режиму інформаційної та цифрової безпеки [36]. Прикладом може бути Китайська Народна Республіка як один із лідерів на ринку інформаційних та цифрових технологій. Специфіка забезпечення інформаційної безпеки (у КНР використовується саме термін «інформаційна безпека», а не «кібербезпека») суттєво відрізняється від західної моделі [47; 67; 77]. У КНР із метою недопущення витоку значимої для держави та національної безпеки інформації або, навпаки, проникнення небажаних даних КНР інформації, дотримуються політики, що Інтернет є важливою інфраструктурою держави і тому його слід тримати під контролем (аж до блокування низки соціальних мереж і пошукових систем) [49; 53–57]. Крім того, підлягає обов'язковому ліцензуванню діяльність компаній, що надають послуги у кіберпросторі на території КНР. У цій країні створено й ефективно функціонує розгалужена система державних органів, головним завданням яких є забезпечення інформаційної та цифрової безпеки країни [там само]. Будь-яке посягання на цей внутрішній сегмент сприймається як загроза національній безпеці.

Підбиваючи проміжні підсумки, хотілося б відзначити, що, незважаючи на всі зазначені загрози повсюдної цифровізації, видається, що глобальний процес трансформації соціально-економічних відносин матиме неминучий подальший всебічний розвиток. У зв'язку з цим, слід детальніше розглянути фактори, які можуть загальмувати процес розвитку цифрових технологій, зокрема. фактори, зумовлені інтересами національної безпеки та системи публічного управління в цілому [47; 67; 77; 282; 283].

Сьогодні проводиться значна робота як на вітчизняному, так і на наднаціональному рівні для розвитку цифрових технологій та їх повсюдного проникнення у всі сфери життя суспільства – інвестування у розвиток національного IT-сектору, фінансове стимулювання створення новітніх інформаційних технологій, кооперація для їх створення на міжнародному рівні, стимулювання інвестицій та підприємницької активності у даній області та ін. [282] Однак, незважаючи на все це, ще існує безліч факторів, які гальмують розвиток цифрових технологій, серед яких виділяють наступні.

По-перше, ступінь довіри суспільства (особливо суспільства країн, що розвиваються) до цифрових технологічних новинок, готовність (а часто й базова можливість) їхнього сприйняти та повсюдного використання знаходяться на низькому рівні, що, відповідно, формує низьки попит і, у свою чергу, згідно із законами економіки, безпосередньо впливає на пропозицію в даній сфері [45; 76]. Усунення цього бар'єру можливо, наприклад, за допомогою проведення політики держави щодо підвищення цифрової й інформаційної грамотності населення (у т.ч. політики з популяризації технологій у повсякденному житті), створення доступної технологічного середовища у всіх регіонах держави (незалежно від ступеня добробуту населення) та забезпечення безпеки інформаційних та інноваційних технологій (наприклад, гарантування недоторканності приватного життя при роботі в мережі Інтернет, захист користувачів даних та прав споживачів, платіжних додатків, персональних даних тощо).

По-друге, навіть сьогодні ще не всі компанії усвідомлюють користь від упровадження та використання цифрових й інформаційних технологій для бізнесу (починаючи з укладення угод в електронній формі, хмарного зберігання даних і роботизації, закінчуючи блокчейном, машинлернінгом та штучним інтелектом), і відповідно не використовують свої потенційні виробничі можливості з технологічними потужностями на максимум. Відбувається це, наприклад, через небажання змінювати сформований хід

речей, перебудовувати корпоративну культуру та налагоджені бізнес-процеси. Аналогічні процеси можна спостерігати й на рівні функціонування публічного сектору, під час надання ним публічних послуг [1].

По-третє, найважче видається представникам приватного сектору, що займається переборкою якихось матеріалів, що вимагає комплексного усунення технологічних бар'єрів на цьому шляху, який є незахищеним від цифровізації та кібератак. Викликано це тим, що у зв'язку з динамічністю розвитку даної сфери, загрози, яким вона наражається, також не стоять на місці, тому заходи боротьби з ними мають бути універсальними і працювати на випередження, а не на усунення наслідків кібератак, що вже відбулися.

У всьому світі повсюдно державна політика у сфері цифровізації вибудовується шляхом формування комплексних стратегій боротьби з кіберзлочинністю, яка може завдати значної шкоди системі національної безпеки. Питання цифровізації мають становити базис для розробки та реалізації національних безпекових програм і стратегій держав.

Так, остання подібна стратегія США [263] передбачає посилення покарань за хакерські атаки. У ЄС прагнуть посилення повноважень агентства з кібербезпеки, а також створення загальноєвропейської системи сертифікації в мережі [53–56; 293]. В Україні ще остаточно не сформована державна інституційна система щодо виявлення, попередження та ліквідації наслідків комп'ютерних атак на інформаційні ресурси публічного сектору, функціонують відповідні відділи СБУ, Центр протидії дезінформації при Раді національної безпеки і оборони України, а також різні центри кібербезпеки при стратегічно значущих об'єктах критичної інфраструктури (які, зокрема, належать до фінансового та банківського сектору). Проте єдиної системи протидії кібератакам немає на вітчизняних теренах.

Погоджуючись з ученими [67; 76; 99; 102–103], відзначимо, що для

розвитку та повсюдного поширення цифрових технологій необхідна гарантія певного рівня національної стабільності (сталості), а також дотримання прав громадян та бізнесу, як, наприклад:

– забезпечення прав користувачів у цифровому світі та збереження їхніх цифрових даних (у т.ч. за допомогою захисту від зовнішнього інформаційно-технічного впливу на інформаційну інфраструктуру за допомогою технологій штучного інтелекту (AI));

– підвищення рівня довіри до цифрового середовища й інституційного середовища, яке використовує цифрові технології;

– мінімізація кількості кіберзагроз, забезпечення доступу до досягнень цифровізації на території всієї країни, нарощування кадрового та наукового потенціалу в цифровій галузі для підвищення конкурентоспроможності країни, запровадження вітчизняних розробок з метою зменшення залежності соціально-економічного розвитку від експорту та ін.

Поки державою не буде вибудувано та забезпечено ефективну політику у сфері використання цифрових технологій, вона не зможе належним чином виконувати свої функції та служити національним інтересам, адже процеси цифровізації та національної безпеки мають безпосередній узаємовплив і перебувають у постійному взаємозв'язку.

У цьому контексті набувають актуальності питання визначення механізмів публічного управління у сфері національної безпеки, що забезпечується в умовах цифрової трансформації (рис. 1.4). З метою унеможливлення зайвих наукових дискусій з приводу того, чому обрані саме механізми публічного управління, відзначимо, що вони охоплюють як державний сектор (адже без пекова функція – пріоритетне завдання держави), так і надбання приватного сектору, який начною мірою виступає інвестором у забезпеченні розвитку цифрових технологій. Крім того, зацікавленим суб’єктом у розвитку цих технологій зокрема та забезпеченні національної безпеки загалом є суспільство, найдостойніші представники

якого повинні залучатися до формування та контролю за державною політикою, що має відзначатися соціальною орієнтованістю.

Загальнодержавний рівень

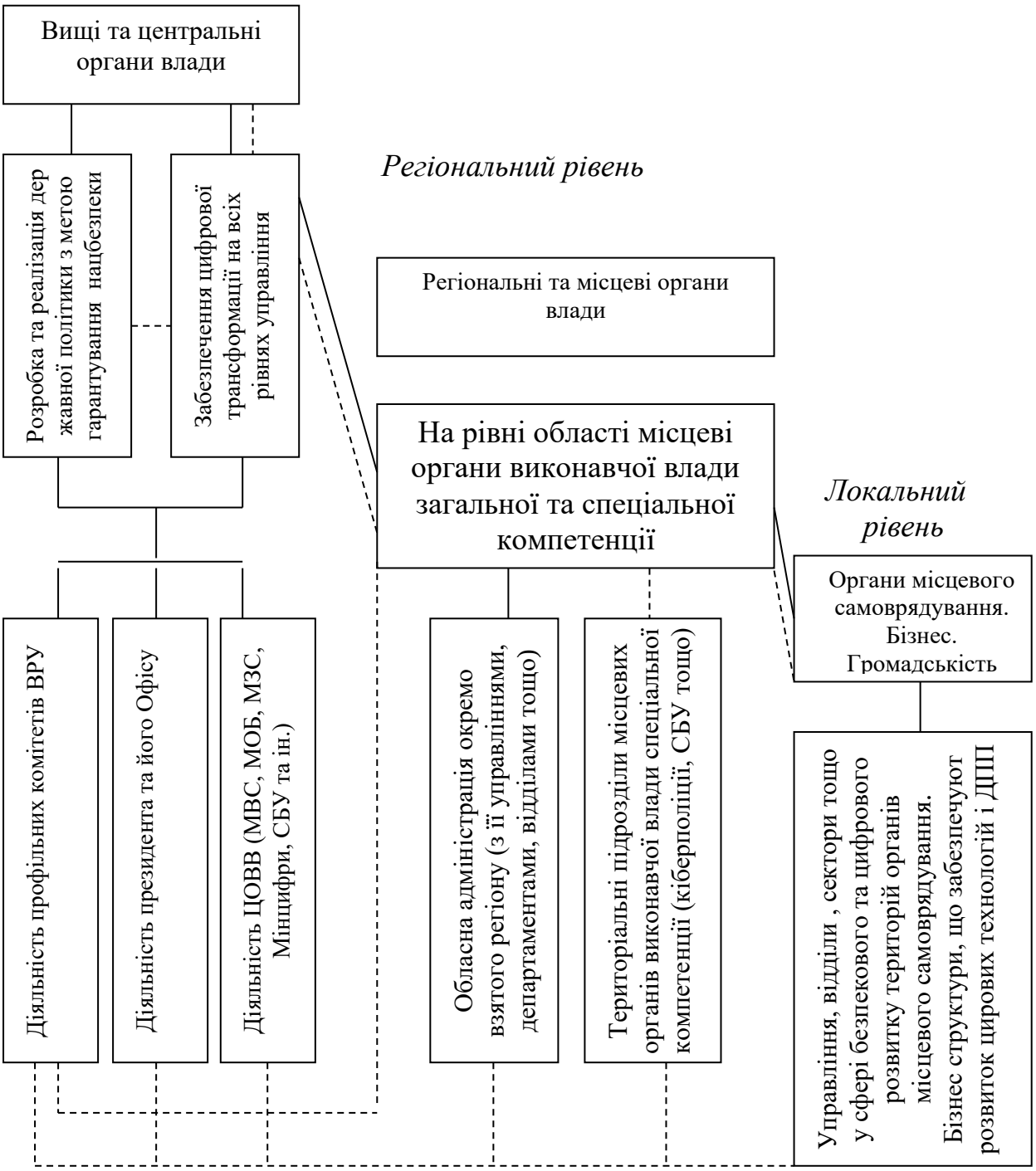

Рис. 1.4. Формування механізмів публічного управління у сфері національної безпеки в умовах цифровізації

Джерело: авторська розробка

Урахування положень фундаментальної науки публічного управління й адміністрування дало змогу виокремити три рівня формування та функціонування механізмів публічного управління у сфері національної безпеки в умовах цифровізації: загальнодержавний; регіональний; локальний. На всіх рівнях управління відбувається взаємодія державного та приватного секторів з метою забезпечення національної безпеки та результативної соціально орієнтованої політики. У той же час, зрозуміло, що приватний сектор не може повноцінно залучатися до реалізації такої політики, адже цей обов'язок покладено на державний апарат. Відтак, слід говорити про залучення представників бізнесу до публічного управління у сфері національної безпеки в умовах цифровізації на засадах державно-приватного партнерства або як експертів у питаннях розвитку цифрових технологій. Щодо суспільства, то тут знову ж таки його участь є обмеженою у формуванні та функціонуванні механізмів публічного управління у сфері нацбезпеки в умовах цифровізації. Свідченням цього є, зокрема, норма Конституції України (що народ є *джерелом* влади) і постанова КМУ «Про забезпечення участі громадськості у формуванні та реалізації державної політики» від 03.11.2010 р. № 996 [60]. Із цих правових документів різної юридичної сили видно, що все суспільство не може залучатися до управлінських процесів, пов'язаних з формуванням і реалізацією державної політики. Із цією метою народ делегує владу державним і самоврядним органам, які (апріорі вважаються) є більш компетентними у питаннях ведення державних справ загальнонаціонального та/або місцевого значення.

Із рис. 1.1 видно, що перший рівень (загальнодержавний) представлено вищими та центральними органами влади. Ураховуючи загальні принципи побудови системи публічного управління, можемо в межах орбагого предмета дослідження до вищих органів влади віднести президента, парламент і уряд України [41; 42]. Вони розробляють (ті, хто володіє правом законодавчої ініціативи) відповідні законодавчі та

підзаконні акти, необхідні для формування соціально орієнтованої державної політики. Ця соціальна орієнтованість полягає у виконанні функцій держави щодо гарантування безпеки громадянам (на безпечне життя і довкілля) та їх гідного рівня життя. Одразу підкреслимо, що Офіс Президента України не є вищим органом влади, але входить до системи публічного управління центрального рівня. Щодо президента та парламенту, то вони є представницькими суб'єктами народовладдя, оскільки їх обирає безпосередньо населення на чергових (позачергових) виборах [63]. Уряд же призначається у вітчизняному парламенті шляхом голосування, якому передує висунення кандидатури Прем'єр-Міністра та складу уряду, тому він не належить до категорії представницьких органів публічної влади. Разом із тим, спільна діяльність цих трьох вищих органів влади дає результат у вигляді сформованої державної соціально орієнтованої політики, що має гарантувати громадянам їх права, у т.ч. на розвиток і безпеку.

Крім того, перший рівень публічного управління у сфері нацбезпеки та розвитку цифровізації представлено центральними органами влади, до яких належать загальні та спеціальні органи виконавчої влади. Вони мають різний обсяг повноважень у зазначеній сфері, що пояснюється спрямованістю роботи цих органів. Ми не випадково вказали, що серед їхнього складу виокремлюють загальні та спеціальні органи виконавчої влади. До них можна віднести Мінстрерство внутрішніх справ України, Міністрерство оборони України, Міністрерство законодонних справ України, Міністерство цифрової трансформації, СБУ та ін. Їхня діяльність має бути спрямована на реалізацію державної політики у сфері національної безпеки в умовах цифровізації, а також на її (політики) доповнення шляхом прийняття окремих розпоряджень, наказів, доручень тощо.

У продовження відзначимо, що другий рівень публічного управління у сфері національної безпеки в умовах цифровізації передбачає діяльність

регіональних і місцевих органів виконавчої влади, які також групують на інституції загальної та спеціальної компетенції [22; 31; 41; 42; 52]. Вони в різній мірі залучаються до реалізації державної соціально орієнтованої політики. Ураховуючи засадниці принципи публічного управління, можемо визначити, що обласна адміністрація окремо взятого регіону є ключовим регіональним суб'єктом у реалізації державної соціально орієнтованої політики, що відбувається на рівні конкретних управлінь, департаментів, відділів тощо. У той же час цей регіональний орган виконавчої влади наділений повноваженнями забезпечувати формування та реалізацію стратегій територіального розвитку. Даний аспект вказує на те, що обласні державні адміністрації виконують не тільки суто виконавську функцію, а й організаційно-розпорядчу, у т.ч. у сфері національної безпеки. Покликані допомагати в цьому територіальні підрозділи місцевих органів виконавчої влади спеціальної компетенції (кіберполіції, ДСНС, СБУ тощо).

Щодо третього (локального) рівня публічного управління у сфері національної безпеки в умовах цифровізації, то він включає самоврядні інституції, які не віднесені до державного сектору, але виконують важливі суспільнозначущі функції. Власне, цей рівень представлений органами місцевого самоврядування, бізнес-структурами та громадськістю. Остання артикулює й агрегує свої інтереси як через громаду в цілому, так і через окремих представників (об'єднання громадян, політичні партії, громадські й політичні діячі, місцеві еліти та ін.). За аналогією з вищими публічними органами влади громада виражає свої інтереси під час місцевих виборів, делегуючи таким чином місцевим органам владу. З огляду на це фахівці вказують, що органи місцевого самоврядування також є представницькими органами. Їхнім обов'язком є забезпечення реалізації права місцевих жителів комплексно, компетентно (професійно), результативно, вчасно, прозоро, скоординовано, децентралізовано та із дотриманням правил безпеки вирішувати питання місцевого значення. У цьому контексті

набуває актуальності робота ЦНАПів, що можуть створюватися регіональними органами виконавчої влади, а також органами місцевого самоврядування. Ці інституції на локальному рівні забезпечують дотримання всіх вищевказаних аспектів під час надання публічних послуг – комплексність, професійність, ефективність, оперативність, публічність, децентралізованість і безпековість. Участь громадськості у формуванні місцевої політики відбувається на різних рівнях, що залежить від стану розвитку самого суспільства, наявності суспільної волі на це (більш дет. про рівні замученості громадськості до формування та реалізації політики йдеться у наукових роботах вітчизняних і закордонних учених С. Арнштейн, О. Крутій, О. Крюкова, О. Правосуда та ін. [41; 42; 76]).

Приватний сектор є одним із найбільш зацікавлених суб'єктів публічного управління у сфері забезпечення національної безпеки. російська військова агресія проти України дуже позначилась на особливостях ведення бізнесу на її території: чимало суб'єктів малого та середнього бізнесу змушені були припинити свою підприємницьку діяльність, або здійснити релокацію бізнесу у більш безпечні регіони, або змінити профіль господарювання. У той же час бізнес зацікавлений в отриманні прибутку та забезпеченні розвитку територій, на яких він відкрився або розташований. Тому непоодинокими є випадки, коли бізнес-структури стають активними учасниками розвитку державно-приватного партнерства. Це поширена європейська практика співпраці зацікавлених публічних інституцій, особливо у сферах, покликаних виконувати життєво важливі для держава та суспільства функції [71]. Здебільшого ці сфеи відносять до секторів критичної інфраструктури (водовідведення, енергозабезпечення, охорони здоров'я, освітньої сфери тощо). Упровадження державно-приватного партнерства допомагає створювати нові робочі місця, залучати додаткові інвестиції, покращувати інвестиційний клімат, підвищувати міжнародний імідж країни, і, головне,

заощаджувати її бюджетні кошти. Усе надзвичайно болючі й актуальні проблемні питання для України, тому можемо наполягати на перспективності розвитку державно-приватного партнерства на її теренах для відновлення критичної інфраструктури й інших інфраструктурних об’єктів, що у своїй значній кількості перебувають у приватній власності. Очевидно, що хто ж як не приватний власник має бути зацікавленим у належному функціонуванні власного бізнес-проєкту.

Вищевикладене й урахування загальних положень фундаментальної науки публічного управління й адміністрування дозволили визначити таку будову механізмів публічного управління у сфері національної безпеки в умовах цифровізації: мета тазавдання публічного управління; суб’єкти й об’єкт публічного управління; функції та форми публічного управління; методи й інструменти публічного управління (рис. 1.5). У продовження думок вчених щодо класифікації механізмів державного управління [22; 31; 41; 52] можемо відзначити, що механізми публічного управління приводять у рух усю його систему. При цьому одними з найбільш рухливих її елементів є саме методи державного впливу, що забезпечують адаптивність цієї системи до мінливих умов зовнішнього середовища. Із метою унеможливлення кардинальної зміни структури системи публічного управління потрібне виважене та вчасне вдосконалення його методів, що дозволить модернізувати систему зсередини, не припинивши її функціонування. Виокремлюють правові, організаційні, інституційні, економічні, матеріально-фінансові, кадрові, інформаційні та інші методи публічного управління. Зважаючи на предмет нашого дослідження, уважаємо, що значна частина з вищеперерахованих методів притаманна також системі публічного управління у сфері національної безпеки. На цій підставі можемо стверджувати, що механізми публічного управління у сфері національної безпеки в умовах цифровізації можна згрупувати таким чином:

1) правові;

2) організаційні;

3) ресурсний;

4) інформаційний.

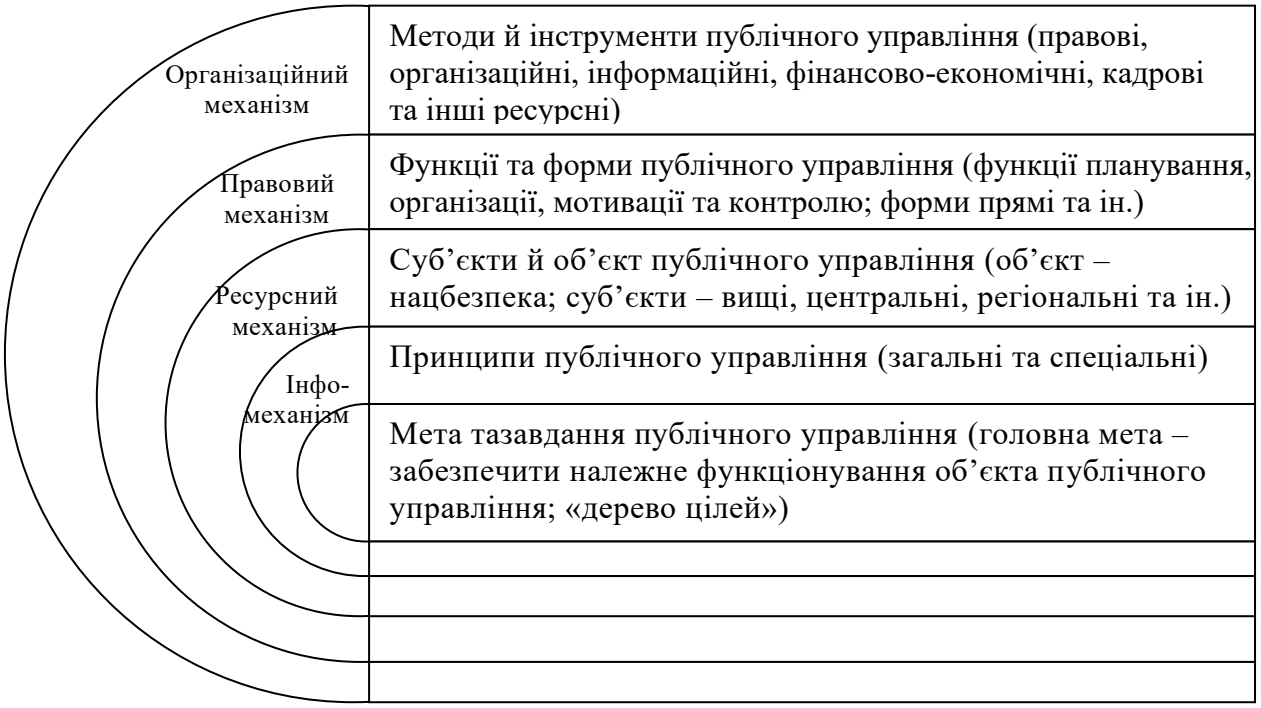

Рис. 1.5. Структура механізмів публічного управління у сфері національної безпеки в умовах впливу цифрових технологій

Джерело: складено на підставі [22; 41; 42; 52]

На наше переконання, кожен із запропонованих механізмів публічного управління у сфері національної безпеки в умовах цифровізації відіграє важливу роль, зумовлюючи взаємний вплив один на одного. На цій підставі можемо наполягати на комбінаторності формування та функціонування механізмів публічного управління у сфері національної безпеки в умовах цифровізації (рис. 1.6).

Із рис. 1.5 і 1.6 видно, що мета публічного управління у сфері національної безпеки в умовах цифровізації передбачає забезпечення належного функціонування об'єкту державного впливу, що представлений

сферою нацбезпеки. Досягнення цієї мети вимагає результативного функціонування суб'єктів публічного управління, що класифіковано залежно від рівня такого управління (на вищі, центральні, регіональні та локальні). Крім того, відзначимо, що об'єкт публічного управління потрібно розглядати з позиції захисту та реалізації національних інтересів, що включають державні, суспільні й окремо взятої особистості. Дане твердження висловлено нами з урахуванням наявного визначення поняття «національна безпека» у чинному законодавстві України [60].

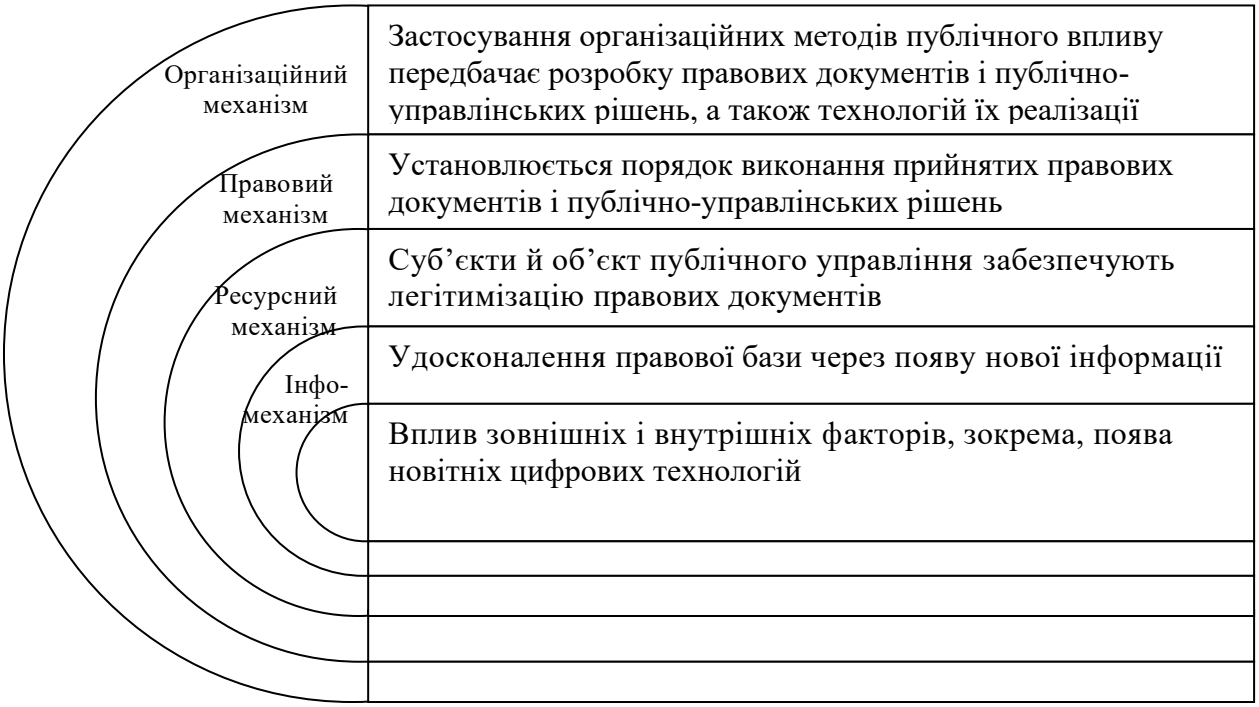

Рис. 1.6. Класифікація механізмів публічного управління у сфері національної безпеки в умовах впливу цифрових технологій

Джерело: авторська розробка

Щодо принципів публічного управління, то у їхньому складі виокремлено загальні та спеціальні, що охоплюють такі принципи: системності; комплексності; науковості; публічності (прозорості та відкритості); результативності й ефективності); оперативності; єдності; уніфікованості; централізованості – де централізованості тощо.

Серед функцій публічного управління у сфері національної безпеки в умовах цифровізації визначено основні – планування, організації, мотивації та контролю, що відзначаються циклічністю та взаємопроникливістю. Власне, елементи кожної функції можна зустріти на етапі виконання іншої функції.

Серед форм публічного управління у сфері національної безпеки в умовах цифровізації виокремлено прямі та непрямі. В онову класифікації цих форм публічного управління покладено принцип реалізації влади – безпосередньо або опосередковано. Це, у свою чергу, зумовлює необхідність дослідження особливостей функціонування органів представницької демократії та органів державної влади, до яких публічні службовці призначаються, а не обираються населенням. У цьому контексті вважаємо, що потребують більш глибокого дослідження особливості функціонування запропонованих вище механізмів публічного управління у сфері національної безпеки в умовах цифровізації як в Україні, так і у світі.

РОЗДІЛ 2
АНАЛІЗ СУЧАСНОГО СТАНУ РЕАЛІЗАЦІЇ ДІЄВИХ МЕХАНІЗМІВ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ВПЛИВУ ЦИФРОВИХ ТЕХНОЛОГІЙ

2.1. Особливості реалізації публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні та за кордоном

Первинною проблемою заявленого дослідження є відсутність можливості системно та комплексно проаналізувати весь плюралізм цифрових технологій та їхнього впливу на сферу забезпечення національної безпеки. З огляду на це, виникає необхідність визначити ключові технології та ризики їх використання в єдиному взаємозв'язку (inter-connection). Друга складність полягає у визначенні «інноваційних країн», що мають значні досягнення у сфері використання цифрових технологій в умовах невизначеності. Аналіз рейтингів та звітів дає підстави з'ясувати відмінні позиції країн у таких рейтингах [294; 295]. Крім того, для цього дослідження важливим є визначення не тільки «інноваційності» (інноваційного потенціалу) країн, а безпосередньо їхньої позиції щодо застосування та реалізації цифрової трансформації з метою забезпечення власної та колективної системи безпеки. Для вирішення зазначених проблем доцільно здійснити два незалежні мережеві аналізи, за результатами яких можна визначити пул країн, на яких буде сфокусовано дослідження. Окремо має бути виявлено «ключову» цифрову технологію, важливу для забезпечення національної безпеки.

Перший мережевий аналіз фокусується на досягненнях у сфері цифровізації серед держав, які забезпечують тим самим їх конкурентний розвиток. Як відомо, конкуренція – це складна система взаємодії між

країнами у тій чи іншій сфері суспільної життєдіяльності. При цьому мережевий аналіз є одним з ефективних інструментів вивчення конкурентного середовища. Свідченням цього є прецедент використання мережевого аналізу для вивчення еволюції глобальної конкурентної торгівлі вугіллям [344], світової нафтової конкуренції [353], глобальної конкуренції за природний графіт [267], конкуренції у сфері торгівлі сталлю [200], продуктами харчування [156], або урахування конкурентних переваг у сфері функціонування оборонно-промислового комплексу [185] тощо. Оскільки цифрові технології можна розглядати як ресурси, то глобальну конкуренцію країн у сфері цифровізації також можна вивчити за допомогою мережевого аналізу. За цією логікою було проранжовано країни, в яких зв'язки представлені індикаторами, що позначають широко застосовані цифрові технології, а також побудована мережа цифрових технологій, зв'язки якої представлені індикаторами країн, що не тільки використовують (упроваджують) а й розвивають певні технології. Теоретична рамка й інформація щодо опрацьованих даних представлені в додатку 1.

Формування двох мереж (мережі країн та мережі цифрових технологій) засноване на методі афіліації (affiliation) та ко-афіліації (co-affiliation). Логіка аналізу афілійованих мереж передбачає, що спільна участь у групах зацікавлених суб'єктів чи заходах є показником базового соціального та/або суспільно-політичного зв'язку (connection/ public connection) [124]. Іншими словами, спільна участь є можливістю для розвитку відносин, які, у свою чергу, представляють можливості для обміну ідеями, ресурсами та цифровими технологіями. У контексті конкуренції у сфері цифровізації спільне членство (co-membership) країн передбачає розробку й упровадження аналогічних конкретних типів цифрових технологій, у т.ч. у сфері нацбезпеки.

За результатами першого мережевого аналізу, щодо мереж країн, центральність за ступенем (degree centrality), центральність за близькістю (closeness centrality) та центральність власного вектора (eigenvector centrality) формують країни 1 рівня: Сінгапур, Китай, Німеччина, Бельгія, Канада,

Великобританія, Нідерланди, Фінляндія, Франція, Японія, Корея, Італія, Швейцарія, США, Швеція, Ірландія.

Країни 2 рівня, які відзначаються середніми показники в розвитку цифрових технологій, і не мають конфліктів з іншими державами (Індія, Іспанія та Австралія). Нижче представлена табл. 2.1 країн з найвищими показниками центральностей, тобто умовні країни-лідери (дет. про центральність див. [96]).

Країни 3 рівня, які відзначаються значними показниками в розвитку цифрових технологій і публічно-приватного партнерства в напрямку реалізації інноваційних проєктів, але при цьому мають конфлікти з іншими державами (Ізраїль, Китай, Тайвань, Північна Корея та ін.).

Країни 4 рівня, які мають низькі показники в розвитку цифрових технологій (Буркіна-Фасо, Ефіопія, Ємен, ДР Конго, Малі, Нігер та ін.).

Мережевий аналіз і ранжування країн проводився щодо показників центральностей у двох площинах:

1) стан використання Інтернету та Інтернету речей, кількість патентів на цифрові технології зв'язку, комп'ютерні та інші технології, стан розвитку штучного інтелекту, автоматизації та робототехніки, стан продажів відповідних технологій тощо;

2) рівень безпеки в країні, наявність на її території конфліктів (рис. 2). Під час мережевого аналізу показників у межах першої площини до уваги брались дані «Analyzing Affiliation Networks» (J. Scott) і Європейського інвестиційного банку, а в межах другої площини – дані дослідницької організації International Crisis Group [71; 93].

Європейський інвестиційний банк навів такі дані щодо реалізованих інноваційних проєктів у межах публічного-приватного партнерства (далі – ППП) у 2023 році:

– 38 транзакцій у межах ринку ППП досягли фінансового завершення загальною вартістю 13,6 млрд євро.

– у вартісному вираженні ринок ППП Європи зріс на 35% порівняно з

2022 роком.

– у 2023 році в кількісному вираженні ринок ППП скоротився на 17% порівняно з 2022 роком.

– у звітному періоді найактивнішим учасником ринку ППП була Німеччина за вартістю та кількістю проектів ППП (до речі, у 2022 р. найактивною була Франція на ринку ППП);

– 13 країн Європи закрили принаймні один проєкт ППП, порівняно з 15 проєктами ППП у 2022 році;

– у звітному періоді транспортна сфера була визнана найбільшим результативним сектором як у вартісному, так і в кількісному вираженні реалізованих проектів ППП (рис. 2.2);

– понад 53% закритих транзакцій у Європі були проведені в межах ППП;

– виявлено, що Європа прагне досягти плато в розвитку ринку ППП (рис. 2.3) [там само].

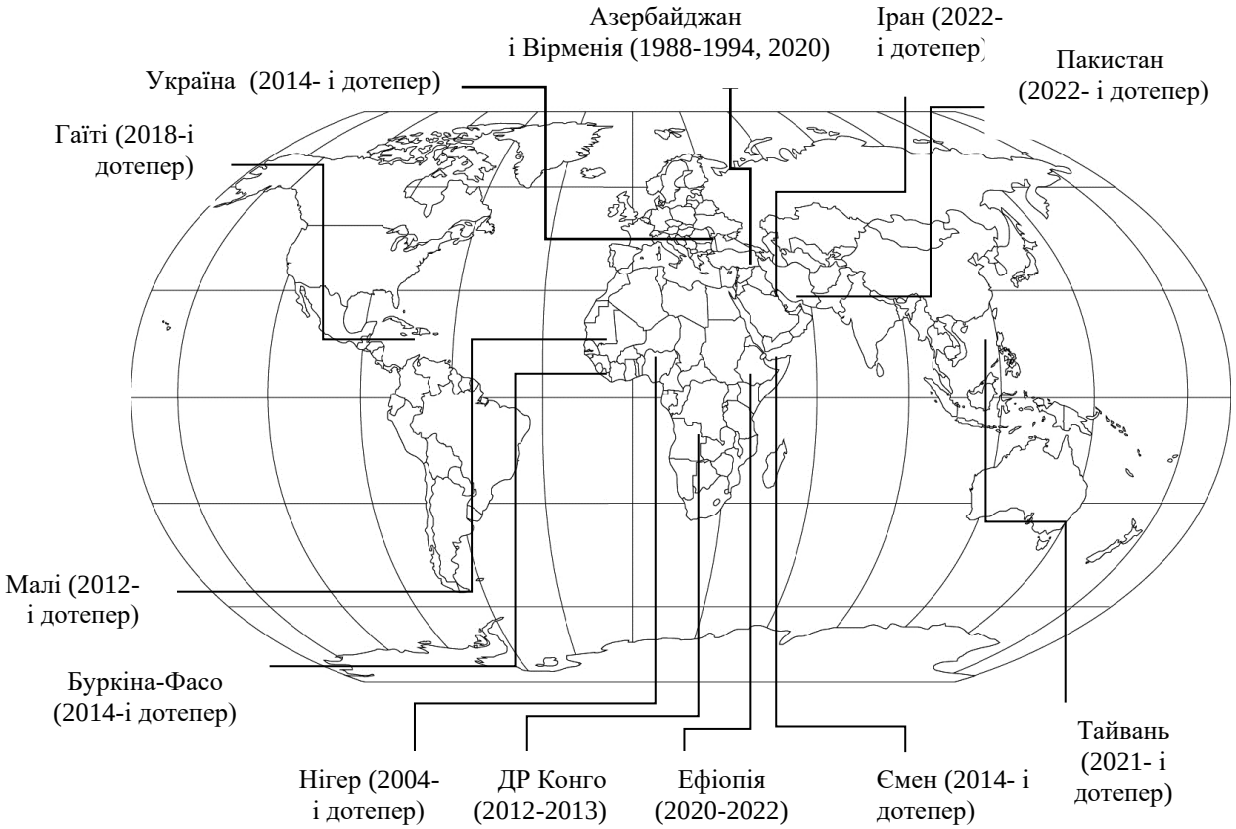

Рис. 2.1. Найбільша кількість збройних і військово-політичних конфліктів у світі у 2023 році

Джерело: складено на підставі [71; 93]

Рис. 2.2. Кількість проєктів ППП у Європі, що реалізуються в основних інфраструктурних секторах у 2023 р., у %

Джерело: складено на підставі [71]

Слід відзначити, що серед не Європейських країн лідируючі позиції на ринку ППП займають такі держави: у 2018 році лідером із реалізації найбільших проєктів ППП є Туреччина, а у 2023 році – Ізраїль.

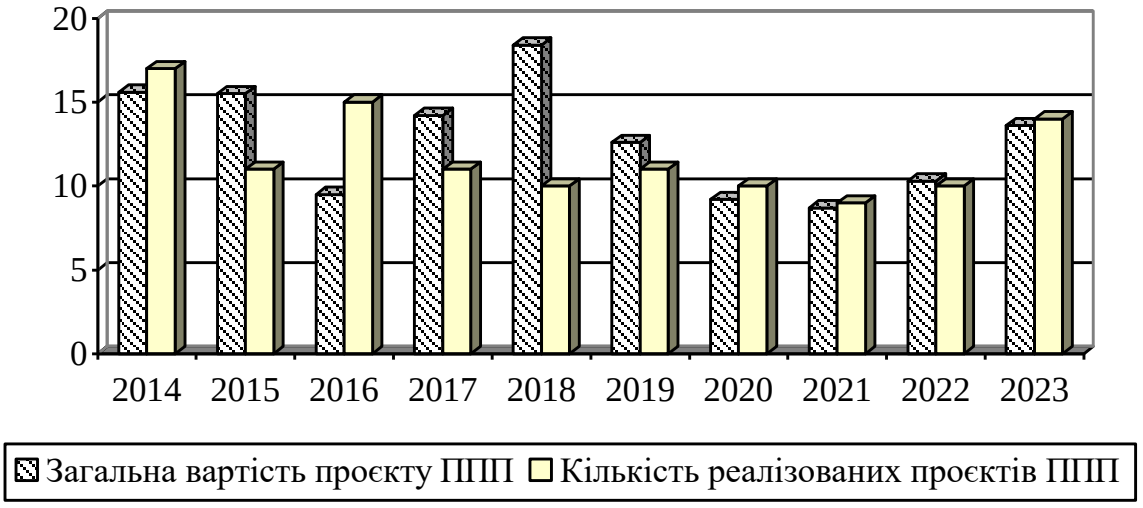

Рис. 2.3. Стан зміни європейського ринку ППП за вартістю та кількістю реалізованих проєктів (2014-2023 рр.)

Джерело: складено на підставі [71]

Погоджуємось із ученими, що російсько-українська війна актуалізувала значну кількість збройних конфліктів по всьому світові (Азербайджан, Ізраїль, Тайвань та ін.) [71; 93]. У 2023 р. безпековий сектор отримав фінансування для реалізації європейських проєктів ППП в обсязі щонайменше 995 мільйонів євро складається (6 проєктів ППП було реалізовано в Німеччині, по 2 проєкти ППП у Литві та Бельгії) [там само]. Слід зазначити, що 4 з 6 проєктів ППП у секторі громадського порядку та безпеки в Європі спрямовані на покращення надання поліцейських послуг.

Таблиця 2.1

Таблиця центральностей мережевого аналізу країн

№ з/п	Назва країни	Централь-ність за ступенем	Централь-ність за близкістю	Централь-ність за посередністю	Централь-ність власного вектору	Централь-ність за Боначичем
1	Австралія	41	0,019	3,902	0,825	0,406
2	Бєльгія	56	0,027	7,827	0,994	0,039
3	Китай	56	0,027	3,157	1	0,039
4	Данія	33	0,017	2,009	0,6	0,344
5	Фінляндія	56	0,027	3,157	1	0,039
6	Франція	56	0,027	3,157	1	0,039
7	Німеччина	56	0,027	3,157	1	0,039
8	Італія	55	0,026	7,36	0,987	0,051
9	Японія	56	0,027	3,157	1	0,039
10	Нідерланди	56	0,027	3,157	1	0,039
11	Південна Корея	56	0,027	3,157	1	0,039
12	Сінгапур	54	0,026	7,369	0,978	0,064
13	Швеція	56	0,027	32,197	0,993	0,039
14	Швейцарія	56	0,027	3,157	1	0,039
15	США	56	0,027	3,157	1	0,039

Джерело: складнено на підставі [124, с. 640]

З табл. 2.1. видно, що в мережах цифрових технологій центральність за ступенем (degree centrality), центральність за близькістю (closeness centrality) та центральність власного вектора (eigenvector centrality) формують технології 1 рівня: використання інтернету (UI), автоматизація та робототехніка (AR), інтернет речей (IoT), технологія 5g та два типи патентів (патенти на технології цифрового зв'язку та патенти на комп 'ютерні технології).

Технології 2 рівня представлені таким: 3D-друком (X3Dp) для всіх трьох типів центральності, а також технологічною основою (TF) за показником центральності за посередництвом (betweenness centrality). На окрему уваги слід звернути увагу на результати штучного інтелекту (AI), що займає лідируючі позиції з трьох типів центральності. Нижче представлена табл. 2.2 цифрових технологій із найвищими показниками центральностей.

Таблиця 2.2

Таблиця центральностей мережевого аналізу цифрових технологій

№ з/п	Тип цифрової технології	Централь-ність за ступенем	Централь-ність за близкістю	Централь-ність за посередніст ю	Централь-ність власного вектору	Централь-ність за Боначичем
1	Використання Інтернету	20	0,0769	7,0714	0,9863	0,102
2	Патенти (у т.ч. на цифрові технології зв’язку)	20	0,0769	1,5714	1	0,102
3	Патенти на комп’ютерні технологііі	20	0,0769	1,5714	1	0,102
4	Технологічна основа	10	0,0435	0,1429	0,5704	0,1429

5	Штучний інтелект	16	0,0588	3,5	0,8934	0,2245
6	Інтернет речей	20	0,0769	1,5714	1	0,102
7	Автоматизація та робототехніка	20	0,0769	1,5714	1	0,102
8	3D друк	15	0,0556	0,4286	0,8182	0,0204
9	Технологія зв’язку 5g	20	0,0769	1,5714	1	0,102

Джерело: складено на підставі [124, с. 640]

Мережевий аналіз цифрових технологій сприяє розумінню формування, мети та важливості цифрової трансформації у глобальному виді та масштабі окремо взятої держави. Особливість використання штучного інтелекту підтверджує необхідність детального вивчення суспільно-політичної спільноти з позиції наукової спільноти й етатичних підходів. Власне кажучи, поглиблена концептуалізація штучного інтелекту стає одним із головних завдань для академічної спільноти та експертів у галузі державної політики. Усвідомлення концептуального взаємозв’язку технологій, а також розуміння ключових типів цифрових технологій дозволяють зосередити політичні зусилля та увагу суспільства на досяжних цілях. Виділення пулу взаємопов’язаних технологій дозволяє нам розширити сферу досліджень конкуренції країн та міжнародних відносин щодо концепції цифрової трансформації для забезпечення національної безпеки.

Виявлення дев’яти провідних країн у межах концепції взаємозв’язку цифрових технологій дозволяє переосмислити існуючу конкуренцію між країнами з урахуванням «цифрової» компоненти. Цифрові технології стають одним із ключових ресурсів як внутрішнього розвитку держави, так і її позиції та ролі на міжнародній арені. Мережева структура країн також надає можливість вивчати технологічні альянси та змагання країн у галузі цифрових технологій, які можуть забезпечувати різний вплив на сферу

національної безпеки. Більше того, виявлення «прихованих» лідерів (Швеція) та країн, що «наздоганяють» лідерів в упровадженні цифрових технологій (Бельгія, Індія), відкриває нові можливості для порівняльного аналізу країн та їхньої політики. Аналіз виявлених показників, а також національної політики може надати ще більше інформації щодо глобальних трансформаційних наслідків цифровізації.

Відповідно, за підсумками першого мережного аналізу можемо зазначити таке:

1. Визначити основний фокус – конкретний тип цифрових технологій, на аналізі якого будуватиметься основна частина емпіричного дослідження: технологія штучного інтелекту.

2. Окреслити перелік країн-лідерів цифрової трансформації: Китай, Фінляндія, Франція, Німеччина, Японія, Нідерланди, Республіка Корея, Швейцарія, США та Швеція.

Для цілей цього дослідження не буде проводитися аналіз Китаю й Японії з огляду на відсутність достатніх даних щодо цих країн через мовні обмеження.

Другий мережевий аналіз передбачає розгляд країни як центрів (вузлів), що мають спільні зв’язки, виражені у показниках торгівлі (обміну) цифровими технологіями. Власне, центром виступає конкретна країна. При цьому зв’язок у мережах спрямований – від країни-продавця до країни-покупця (реципієнта).

Для аналізу використовувалася база даних Світової організації торгівлі за класифікацією EBOPS 2010 (доступні дані з 2005 по 2020 роки), а саме: індикатор «Збалансована міжнародна торгівля послугами EBOPS 2010 (2005–2020) – (Набір експериментальних даних)». Матриця даних для мережевого аналізу містить показники за конкретною країною (інформація навдена в рядках), та показники торгівлі між країнами (інформація наведена в стовпцях). Матриця дозволяє встановити зв’язки під час торгівлі від країни продавця зліва до країни покупця праворуч. Для валідизації результатів

використовувалися показники центральностей за даними за 2020 р. (дані з дата-сета).

За результатами другого мережевого аналізу були виявлені лідери торгівлі цифровими технологіями, що підвищили рівень безпеки в таких країнах: Бельгія, Фінляндія, Франція, Німеччина, Польща, Румунія, Швеція, Швейцарія, Великобританія, США. Таблиця 2.3 країн із найвищими показниками центральностей за 2020 р. представлена нижче.

Як бачимо, за результатами двох незалежних мережевих аналізів можна назвати країни, які демонструють лідируючі позиції у використанні та забезпеченні розвитку цифрових технологій. Ураховуючи, що країни демонструють високі показники центральностей на різних дата-сетах, можна стверджувати, що результати виділення країн є стійкими.

Таблиця 2.3

Таблиця центральності країн-лідерів торгівлі цифровими технологіями

№ з/п	Назва країни	Центральність за ступенем	Центральність за близкістю	Центральність за посередністю	Центральність власного вектору
1	Бєльгія	56	0,026	16,246	1
2	Фінляндія	55	0,026	15,053	0,982
3	Франція	53	0,025	12,791	0,963
4	Німеччина	55	0,026	14,009	0,985
5	Польща	55	0,026	19,72	0,986
6	Румунія	55	0,026	24,73	0,97
7	Швеція	55	0,026	14,331	0,979
8	Швейцарія	49	0,023	11,997	0,912
9	Англія	54	0,026	33,571	0,969
10	США	50	0,023	23,133	0,912

Джерело: складнено на підставі [124]

Таким чином, для цілей цього дослідження будуть використані країни, які демонструють лідируючі позиції за підсумками двох мережевих аналізів,

а саме: США, Швеція, Німеччина, Фінляндія та Франція.

З метою надання пояснень щодо потенціалу використання результатів мережного аналізу було здійснено додатковий регресійний аналіз (опис та результати представлені у додатку 5). Логіка аналізу спрямована на виявлення чинників, які можуть пояснити становище країни у торговій мережі цифрових технологій. При цьому нас цікавлять фактори, пов'язані з питаннями безпеки або їх купіруванням, можливістю запобігання загрозам. Іншими словами, варто прагнути визначити можливості дослідження ролі цифрових технологій та дифузії інновацій (що змістовно відображає показники центральності) у логіці національної безпеки.

Держави та уряди можуть розвивати цифрові технології (особливо технології подвійного призначення) як реакцію на внутрішні та зовнішні загрози. Відтак, важливим є виявлення зв'язку чинників загроз із показниками, умовно, технологічної центральності, що може продемонструвати механізм взаємодії державного та публічного секторів у сфері забезпечення цифровізації. З огляду на це висувається гіпотеза щодо визначення потенціалу забезпечення розвитку цифрових технологій для підвищення рівня національної безпеки.

Для перевірки цієї гіпотези може бути використана лінійна регресія. Як залежна змінна виступає показник центральності за посередництвом з другим мережевим аналізом (торгівля технологіями, цифровими технологіями та послугами). Незалежними змінними виступають: дві змінні торгівлі зброєю (постачальник й одержувач); дві змінні, пов'язані з соціальними протестами (протестна мобілізація та насильницька спрямованість протесту) – вони розглядаються як внутрішні загрози національній безпеці соціального характеру; тероризм – як внутрішня та/або зовнішня загроза людського характеру; ймовірність насильницького конфлікту – як внутрішня та/або зовнішня загроза соціального характеру; природні катастрофи – внутрішні/зовнішні небезпеки природного характеру; режим (V-dem) та ефективність дій уряду, що представляє логіку інституційних можливостей

реагування на загрози та розвиток цифрових технологій.

У результаті було збудовано дві моделі регресійного аналізу: модель 2015 р. та модель 2020 р. (У логіці відповідності з другим мережним аналізом). У результаті для моделі 2015 р. істотною є торгівля зброєю, як країною-постачальником, так і країною-одержувачем. Щодо торгівлі зброєю, то результати можуть свідчити про особливості використання цифрових технологій подвійного призначення. Власне кажучи, технології подвійного призначення можуть виступати також елементами торгівлі зброєю. Альтернативним поясненням можуть бути особливості торгових шляхів, оскільки торгівля цифровими технологіями процесуально схожа з торгівлею зброєю (як у рівні торговельних відносин, так і в логіці міжнародних політичних процесів). Щодо тероризму, механізм оцінювання може полягати в такому: держави, які постраждали від терористичних загроз або побоюються цих загроз, розвивають технологічну складову валсної економіки (торгівля технологіями пов’язана з певним рівнем розвитку НДДКР та застосування цифрових технологій), розглядаючи цифрові технології як елемент протидії терористичним загрозам.

Модель 2020 року («доковідна» модель) має відмінні результати. Торгівля зброєю демонструє зв’язок лише з країною-постачальником. Зазначене може пояснюватися специфікою торговельних відносин (зміна/закриття контрактів, зміна торгових шляхів та ін.). Крім того, варто враховувати вплив санкційної політики (після 2014 і 2022 років), яка дуже змінила торговельні маршрути поширення цифрових технологій, особливо у питаннях озброєння.

Варто також зважати на вагомість показника масові протести та режим країни, чи є виборча демократія. Щодо акцій соціальних протестів, то результати можуть пояснюватися збільшенням масової протестної активності, у зв’язку з чим результати відмінні від моделі 2015 р. Альтернативним поясненням може бути підвищена увага держав до акцій протестів. Власне кажучи, органи державної влади на центральному рівні

управління (національні уряди) почали розглядати протести як загрози, які потенційно можна усунути або контролювати за допомогою цифрових технологій. Зазначене може бути викликане ще й доступністю, поширеністю та результативністю самих цифрових технологій. Так, якщо на початку 2010-х технологічні рішення були на стадіях розробки та тестування, то станом на сьогодні, отримавши змістовні результати й оцінивши можливості та перспективи використання цифрових технологій, можна розглядати їх як певні рішення проблеми протестної активності. Режими виборчої демократії й електоральної автократії, також засвідчують значимість зв'язку в моделі 2020 р. Зазначене складно однозначно інтерпретувати з огляду на те, що характеристики режиму визначаються великою кількістю факторів. Однак можна стверджувати, що результати вказують на базис для подальших досліджень щодо впливу режимних характеристик застосування цифрових технологій і роль держав у торгових зв'язках цифрових технологій для забезпечення власної та глобальної безпеки.

Підкреслимо, що зазначений аналіз знаходиться за рамками основного дослідження і містить гіпотезу. Її метою є визначення (1) потенційних можливостей пошуку механізмів оцінювання та проведення мережевого аналізу, а також (2) можливих напрямів посилення аргументації значущості та ролі показників цифрової центральності у забезпеченні нацбезпеки. Сутнісно, показники центральностей змістовно відображають як дифузію інновацій, так і можуть слугувати індексом технологічної центральності. Пошук механізмів оцінювання, що пояснюють позиції країн у мережевій структурі та їх роль у виникненні та реагуванні на загрози (якщо розглядати цифрові технології як елементи можливостей держави створювати/запобігати таким загрозам) значно розширює існуючі дискусії як у предметному полі досліджень безпеки, так і в логіці державної політики цифровізації.

Перед тим, як перейти до опису емпіричної моделі другої частини цього дослідження та безпосередньої реалізації, необхідно виділити додаткове завдання: концептуалізація технології штучного інтелекту в

напрямку забезпечення національної безпеки.

Існують різнохарактерні концепції розуміння штучного інтелекту, але в широкому сенсі даний вид цифрових технологій визначають як «інтелектуальні системи, що відзначаються здатністю аналізувати й удосконалюватися» [299]. Сутрнісно, це різновид набору інструментів, методів та конкретних алгоритмів [224]. Різні програми та методи – від нейронних мереж та моделей глибокого машинного навчання) до розпізнавання мови та/або образів та генетичних алгоритмів, обробка природної мови та машинний зір – об'єднані «парасольковим» поняттям технологій штучного інтелекту, на що звертає увагу держава та система її управління [291]. Штучний інтелект також визначається як система, здатна незалежно інтерпретувати зовнішні дані та навчатися на них для досягнення конкретних результатів за допомогою гнучкої адаптації [282].

У той же час, наявні наукові дослідження, за якими «штучного інтелекту не існує». Наприклад, так уважають [184; 207], що штучний інтелект є історичними конструкціями, подекуди рудиментом на попередніх стадіях соціального та наукового розвитку. Розглядаючи штучний інетететект або як окрему категорію інтелекту, що відрізняється від «природного» інтелекту, або як різновид інтелекту, що є невід'ємною властивістю фізичних осіб (людей), або штучних об'єктів (наприклад, роботів), слід зважати на те, що ні перший аспект, ні другий неможливо розглядати в межах соціальної філософії, адже інтелект – це системне явище, а не властивість окремої одиниці. У цьому контексті погоджуємося із ученими, які звертають на це увагу [245; 282]. У межах наукових розробок, що проводяться в межах наук соціального та політико-правого блоку, цілком допустимим є існування «парасольного» поняття технологій штучного інтелекту, що (поняття) передбачає визначальну сукупність підходів, інструментів, і алгоритмів, оскільки основна відмінна риса штучного інтелекту – соціальний вплив загалом і соціально-політичні ефекти зокрема. Власне кажучи, для досліджень соціальних і державно-політичних процесів немає значення,

наскільки «штучний» чи «природний» інтелект, і який сам «інтелект» [338], розглядаючи цей феномен через розуміння інтелекту як основного явища з людьми і машинами як його агентів [184].

Незважаючи на складність у розумінні та змістовному наповненні технології штучного інтелекту, держави цілком «успішно» вступили в новий етап «конкуренції озброєнь» щодо використання таких технологій [144; 206; 305]. Крім того, подекуди технології штучного інтелекту щодо його потенціалу та можливостей порівнюються з ядерною зброєю [275], і навіть наявні дискусії щодо допустимості застосування штучного інтелекту в галузі ядерного стримування [228]. Якщо проаналізувати існуючі наукові розробки та практичні результати технології штучного інтелекту у сферах охорони здоров'я, логістики, транспорту, комунікації, економіки тощо, можна виявити, що уряди різних країн приділяють все більше уваги технологіям штучного інтелекту. Вже понад 20 країн мають національні програми у сфері цифровізації та штучного інтелекту [138]. До речі, подібна програма у сфері цифровізації та штучного інтелекту США була підписана у січні 2019 р. президентом США Д. Трампом. Відповідна національна програма розвитку штучного інтелекту впроваджується в економіку, сферу безпеки та соціальну сферу.

Відповідно до звіту «Building an AI World» [там само] національні стратегії у сфері використання штучного інтелекту включають як мінімум вісім напрямків (векторів) реалізації державної політики:

1) дослідження;

2) розвиток талантів;

3) актуальні навички та знання, що будуть важливими в середньостроковій перспективі;

4) індустріалізація технологій штучного інтелекту;

5) етичні стандарти штучного інтелекту;

6) дані та цифрова інфраструктура;

7) штучний інтелект в державному управлінні;

8) інклюзивність та соціальне благополуччя.

Уряди різних країн використовують неоднакові підходи до забезпечення розвитку технологій штучного інтелекту. Спільним є те, що штучний інтелект включається до ключових факторів розвитку та конкурентоспроможності держав. Що ще важливіше, це одне з найбільш зростаючих джерел міжнародної конкуренції (як між державами, так і між публічними та приватними інституціями).

Тематичне ядро проблематики алгоритмізації та штучного інтелекту у соціально-політичній сфері [120] розглядає такі питання:

– застосування ускладнених алгоритмів у державному секторі [255];

– допустимість відправлення правосуддя за допомогою алгоритмів [111; 162; 234; 243; 287];

– алгоритмічний процес прийняття політичних рішень [164; 237; 280; 318; 354];

– проблеми «чорної скриньки» алгоритмів та етико-ціннісна проблематика [145; 183; 236; 251], включаючи упередженість, збалансування, а саме неможливість ефективного аналізу унікальних ситуацій, відсутність морально-моральних орієнтирів [321] та ін;

– застосування алгоритмів у військових цілях [128; 275; 355] та/або як інструмент стримування зовнішньої агресії чи збройних конфліктів (прикладом може бути дискусія про використання штучного інтелекту в питаннях моніторингу та розвитку проєктів у галузі ядерного озброєння та бойового чергування ядерних систем);

– алгоритмічні рішення та штучний інтелект у правоохоронній діяльності [247; 327], у забезпеченні соціальної безпеки [174] та прогнозуванні злочинності [252 ; 260];

– штучний інтелект як питання глобальної безпеки з урахуванням конкуренції між найбільш впливовими та технологічно розвиненими країнами [118; 295].

Розгляд досвіду США щодо врегулювання питань штучного інтелекту

[117] дає підстави стверджувати, що розуміння ролі такого інтелекту ґрунтується на ініціативі адміністрації Президента Д. Трампа, який зазначив, що штучний інтелект має слугувати американському народу (Artificial Intelligence for the American People) [там само]). З цією метою було цілеспрямовано визначено основні етапи та напрями розвитку цифрових технологіїй, у т.ч. штучного інтелекту. У свою чергу, План федеральної участі у розробці технічних стандартів та пов'язаних із ними інструментів «Лідерство США в галузі штучного інтелекту» [333], розроблений Національним інститутом стандартів та технологій, визначає дев'ять основних напрямів стандартів використання штучного інтелекту:

1) концепції та термінологія;

2) дані та знання;

3) взаємодія з людьми;

4) показники;

5) мережа;

6) методологія тестування продуктивності та звітності;

7) безпека;

8) управління ризиками;

9) надійність.

У межах цих стандартів вказується, що хоча визначення штучного інтелекту різняться між собою, для цілей цього плану технології та системи цього інтелекту вважаються такими, що включають програмне забезпечення та/або обладнання, яке може «навчитися» самостійно вирішувати складні проблеми, робити прогнози або виконувати завдання, що вимагають людського сприйняття (наприклад, зір, мова та дотик), сприйняття, пізнання, планування, навчання, спілкування чи фізичну дію. У цій сфері наявні різні приклади різноманітні, що швидко розширюються. Так, з'являються помічники штучного інтелекту, системи комп'ютерного зору, біомедичні дослідження, системи безпілотних транспортних засобів, передове ігрове програмне забезпечення та системи розпізнавання осіб, а також застосування

штучного інтелекту як в інформаційних технологіях, так і в операційних технологіях [там само].

Окремо слід відзначити «Огляд засобів управління деякими цифровими технологіями, що розвиваються», адже Бюро промисловості та безпеки США у 2018 році [294] визначило, що до штучного інтелекту належать такі технології:

1) нейронні мережі та машинне навчання (наприклад, моделювання мозку, прогнозування часових рядів, класифікація);

2) еволюція та генетичні обчислення (наприклад, генетичні алгоритми, генетичне програмування);

3) навчання з підкріпленням;

4) комп'ютерний зір (наприклад, розпізнавання об'єктів/суб'єктів у темряві під час значної швидкості);

5) експертні системи (наприклад, системи підтримки рішень, системи навчання);

6) обробка мови та звуку (наприклад, розпізнавання мови та виробництво);

7) обробка природної мови (наприклад, машинний переклад);

8) планування;

9) обробка аудіо та відео технології (наприклад, клонування голосу, дипфейки);

10) хмарні технології штучного інтелекту або набори його мікросхем.

Автори даного огляду ставлять технології штучного інтелекту в один ряд з машинним навчанням і нейронними мережами (як прояв ускладнених математико-статистичних алгоритмів) [там само].

Щодо розуміння штучного інтелекту безпосередньо у сфері забезпечення ситеми безпеки, необхідно звернутися до звітів Комісії національної безпеки зі штучного інтелекту США [325], зокрема проміжної доповіді від листопада 2019 р. [219]. Так, у розділі «Що ми маємо на увазі під «штучним інтелектом»?» визначено, що штучний інтелект – це здатність

комп’ютерної системи вирішувати проблеми та виконувати завдання, які в іншому випадку складно було б реалізувати за допомогою людського інтелекту. Технології штучного інтелекту розвивалися протягом багатьох десятиліть, включаючи розпізнавання об’єктів/суб’єктів, машинне навчання, комп’ютерний зір, розуміння природної мови та розпізнавання мови. Ці технології використовуються для розширення можливостей людей і машин, допомагаючи їм приймати рішення вищої якості та з більшою швидкістю. У зростаючому, але все ще обмеженому спектрі сфер застосування машинного обладнання, воно може досягати показників, подібних до людських або перевершувати людські, зокрема, під час аналізу великих обсягів даних, виявлення закономірностей і виконання масового пошуку корисних відповідей, оцінок і рекомендацій. Ці системи вдосконалюються в міру переходу від експертних систем, заснованих на явних моделях, до систем машинного навчання, що можуть навчатися на досвіді та підвищувати свою продуктивність, у тому числі ті, які можуть навчатися на досить великих та надійних наборах даних. Це системи, призначені для вирішення завдань та досягнення певних цілей, із компетенціями, які в деяких відносинах паралельні когнітивним процесам людини: сприйняття, міркування, навчання, спілкування, прийняття рішень та дії. Таким чином, можна зробити висновок, що влада США визначає технологію штучного інтелекту максимально широко (часто поєднуючи з машинним навчанням і нейронними мережами), відзначаючи еволюційну природу цих технологій (постійний розвиток і вдосконалення) і їх класифікацію.

Більш предметний розгляд штучного інтелекту в контексті безпосередньо дій (оборони, безпеки, військових операцій) представлено у звіті Дослідницької служби Конгресу США «Штучний інтелект та національна безпека» у серпні 2020 р. [115], де розглядаються різні підходи та викликані таким розмаїттям складності, починаючи від систем із когнітивними функціями як у людей, так і закінчуючи автоматизованим озброєнням. Однак сам звіт містить ідентичне, з наведеним вище, ємне

визначення штучного інтелекту, виходячи з різноманіття практичного (прикладного) застосування його технологій.

Завершуючи закордонну концептуалізацію технологій штучного інтелекту, можемо звернути увагу на звіт ООН «Мілітаризація штучного інтелекту» [324] (2019 р.), де вказується, що штучний інтелект не є єдиною технологією, а є скоріше сукупністю теорій, методів, технологій та прикладних систем для стимулювання та розширення людського інтелекту. Окремо розглядається призма практичного військового застосування та впливу як на систему безпеки, так і на стратегію держав та міжнародну стабільність.

У межах цього дослідження (включаючи збір даних та методологічну валідність) під технологією штучного інтелекту варто розуміти алгоритмічні та комп'ютерні системи (у тому числі програмне забезпечення та/або обладнання), які, навчаючись (самовдосконалюючись), можуть вирішувати складні проблеми, робити прогнози або виконувати завдання, що вимагають людського сприйняття, пізнавати, планувати, навчатися, спілкуватися або здійснювати фізичну дію, обов'язково у сфері безпеки або безпосередньо у військовій сфері.

Ще раз повторимо: у рамках цього дослідження ми не фокусуємось на військово-технічному вимірі штучного інтелекту, а на багаторічному розвитку автоматизованих систем (управління) військового призначення. Справді, різні автоматизовані системи у військовій сфері успішно застосовуються вже багато десятиліть. Ці успіхи завдячують своїм існуванням розвитку кібернетики та відповідним дослідженням кінця першої половини – середини XX ст. Однак сучасний етап після всіх змін у розвитку штучного інтелекту є особливим. Уперше в розпорядженні і держав, і дослідників, і недержавних (самоврядних) акторів є обчислювальні можливості штучного інтелекту, так і досвід, якого не було раніше. Більш досконалі системи самонаведення, стеження, геопросторові дані – це лише частина застосування досягнень останніх десятиліть. Так, штучний інтелект

зберігає спеціалізацію (і, ймовірно, зберігатиме), але вже зараз він вийшов за межі завдань дорогих та негнучких АСУ, комп'ютери «навчилися» «бачити, чути, розуміти» (за умов невизначеності), справлятися з безпрецедентно великими обсягами інформації. Власне кажучи, штучний інтелект у сфері безпеки – це (вже) не тільки й не стільки автоматика у складних системах (кінетичного) озброєння та управління військами, яка, як і раніше, цілком надійно забезпечує швидкість та точність ведення бойових дій. Відтак, потребує більш детального розгляду емпірична модель узгодження елементів системи публічного управління у сфері національної безпеки в умовах цифровізації.

2.2. Аналіз загроз упровадження моделі публічного управління у сфері національної безпеки в умовах цифровізації

При формуванні емпіричної моделі публічного управління у сфері національної безпеки в умовах цифровізації варто враховувати вимірювані індикатори та параметри [179]. При цьому, робота з індикаторами та показниками мала враховувати баланс між повнотою та доступністю даних [там само, с. 467]. Показник узгодженості (консистентності) нацбезпеки (security consistency) у межах цієї моделі формується за допомогою різниці між показниками загроз (threats) та можливостями технологій штучного інтелекту (AI capability) реагувати на такі загрози. Зазначене можна подати у вигляді блок-схеми (рис. 2.4).

Вплив алгоритмів штучного інтелекту (як окремого типу цифрових технологій) на національну безпеку, у свою чергу, можна представити також у межах блок-схеми, що містить аналітичні параметри процесу прийняття рішень у сфері забезпечення нацбезпеки. Показник узгодженості (консистентності) нацбезпеки демонструє, як держава здатна оцінювати

загрози (показник загроз) і чи має вона необхідний рівень можливостей для їхнього відображення (показник можливостей).

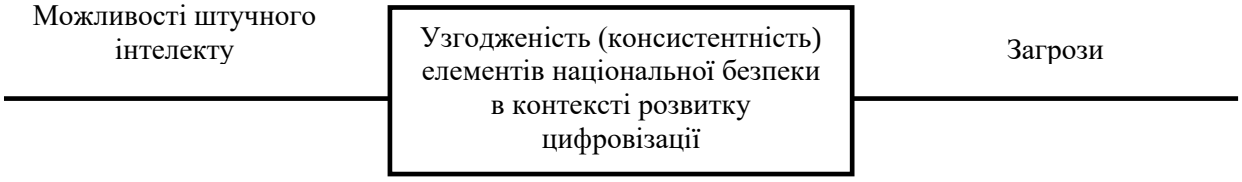

Рис. 2.4. Блок-схема показника узгодженості (консистентності) елементів національної безпеки в контексті розвитку цифровізації

Таким чином, формула (2.1) обчислення індикатора узгодженості нацбезпеки із впливом цифрових технологій має такий вигляд:

$$\text{Security Stability} = \text{AI Capability} - \text{Threats Evaluation} \qquad (2.1)$$

Індикатор можливостей штучного інтелекту розраховується за принципом визначення композитних індексів. У межах даного дослідження за основу береться методичний підхід вимірів «Global capability index» [179] та «Composite Index of National Capability» [167]. Зазначений підхід представляє собою формування єдиного індикатора загалом по країні, який є сумою показників конкретних сфер, поділену на кількість даних сфер. Такий підхід дозволяє врахувати велику кількість проксі показників, які пов’язані та впливають на систему національної безпеки країни. При цьому формування умовного індексу при однонаковій роботі з даними й індикаторами надає можливий прогноз для порівняльного аналізу моделей країн (про який буде йтися під кінець цього підрозділу). Вибір такого підходу обумовлений специфікою даного дослідження тому, що: 1) у межах нього висловлена гіпотеза щодо комплексного аналізу змін; 2) у цьому дослідженні національна безпека розглядається із позиції процесного підходу, адже поза увагою не має залишатись сам процес цифровізації як багатоскладового (комплексного) феномену. З огляду на це, для повнішого досягнення результату, доцільно ґрунтуватись на зазначений підхід

формування композитних індексів. При цьому змістовне розуміння процесу формування показників дозволяє гарантувати досяжність мети та завдань дослідження.

Виходячи з концептуальних засад розуміння штучного інтелекту та цілей створення показника його можливостей (AI capability) можна виділити чотири області/сфери:

1. Технологічна (Technological): передбачає врахування технологічних аспектів штучного інтелекту, а саме: застосування технології у державному управлінні та сфері забезпечення національної безпеки [179]. Спочатку в нього включалися і показники точності алгоритмів, і результати проходження тестів (Turing Test, Loverace Test тощо [246]). Однак у рамках цього дослідження вказаних двох індикаторів можна відмовитися, оскільки за ними були відсутні дані по всіх країнах, крім США (див. попередній підрозділ). У результаті пропонуємо використовувати показник застосування технології (UT – use of technology), який відображає готовність та застосовність штічного інтелекту в публічному та державному управлінні з урахуванням актуальності військової сфери. Ця сфера є відображенням технологічних можливостей держави.

2. Економічна (Economic Environment): передбачає врахування особливостей фінансування технології штучного інтелекту в контексті загального бюджету (для України «військового» бюджету). Варто розуміти, що сфера нацбезпеки може мати різні джерела фінансування, включаючи засекречені статті бюджету, фінансування за рахунок інших статей та розділів тощо. Тому вимушено ґрунтуємось на обмежених публічних даних щодо фінансової підтримки технології безпосередньо у військовому бюджеті України. Відображає фінансово-економічні можливості технології, без фінансування й економічного стимулювання розвиток технології та особливо її застосування у сфері забезпечення нацбезпеки малоймовірне. У результаті використовується показник військових витрат (MF – military fundings), що є ставленням військових витрат на штучний інтелект із загальними

військовими витратами. Такий показник дозволяє повноцінно, але з урахуванням фокусу, аналізувати економічну складову впливу цифровізації на систему публічного управління у сфері національної безпеки.

3. Управління (Governance Environment): ураховує кількість державних компаній, пов'язаних із технологією штучного інтелекту, та існування правової санкції на використання такого інтелекту у військовій сфері. Відображає готовність держави розвивати технологію та застосовувати її можливості. У цій галузі враховуються два показники: 1) наявність державних компаній (SC – state companies) із розробки та застосування технологій штучного інтелекту; 2) правова санкція (LA – legal authorization) на використання штучного інтелекту у військовій сфері. Безумовно, можна (і, більше того, варто) ураховувати більшу різноманітність інституційних проявів публічного та державного управління. Проте з метою проведення ґрунтовного дослідження, зазначених проксі показників достатньо, оскільки вони охоплюють як елемент легіслатури, і наявність розробок та інституційних можливостей застосування технологій;

4. Соціальна (Social Environment): передбачає визначення аспектів зайнятості населення у сферах розробки та застосування технології штучного інтелекту, а також кількість стартапів, що фокусуються на цифрових технологіях. Відображає залучення громадськості, а також можливість держави мобілізувати високопрофесійні кадри. У межах цього блоку також ураховуються два показники: 1) вакансії (JO – job openings), як співвідношення зайнятості-відкриті вакансії на кількість працездатного населення; 2) стартапи (RS), пов'язані зі штучним інтелектом. Логіка оцінювання даних показників обґрунтовується наявністю ресурсів і людського капіталу, необхідного для розробки та застосування цифрових технологій у сфері нацбезпеки, а також можливості впровадження державно-приватного партнерства за умови залучення стартапів з боку держави.

Зазначимо, що вибір та формування проксі показників може зазнати подальшої критики. Безумовно, при подальшому доопрацюванні теми та поглиблення знадобиться додатковий перегляд показників й індикаторів моделі. Однак на даний момент показники спираються на існуючі методи афіляції, мають єдине логічне обґрунтування, повноцінно розкривають різні аспекти як питань нацбезпеки, так і технологічної складової. При цьому будь-яка модель не є «об'єктивною реальністю», а лише потенційним й умовним відображенням феноменів і процесів у певний момент часу. Слід усвідомлювати, що це обмеження, яке не варто намагаєтися контролювати як на рівні однакового протоколу роботи з даними, так і на рівні більш детальної інтерпретації результатів (не генералізуючи/масштабуючи результати та не заявляючи про однозначність виявлених процесів, демонструючи деяку гнучкість, пропонуючи кілька пояснювальних механізмів).

Агрегування зазначених областей/сфер є заключним етапом формування індикатора можливостей технології штучного інтелекту (AI capability), на якому ґрунтуються ці області: технологічна та економічна отримують вагу «0.25» з 1, а область управління – вагу «0.3» у зв'язку з соціально-політичною значимістю цієї галузі у питаннях нацбезпеки. За схожими мотивами соціальна сфера має вагу «0,2», незважаючи на значущість громадянського суспільства та суспільної реакції, у сфері забезпечення безпеки населення «знає лише те, що держава вважає за можливе знати». Іншими словами, роль суспільства у питаннях можливості технології у сфері безпеки буде найменш значущою поряд з іншими областями/вимірюваннями.

Детальний опис підрахунку показників наведений у додатку 2. Там же представлені описові статистики показників та кореляційні матриці для кожної країни. Для всіх країн властивий позитивний коефіцієнт кореляції показників індикатора можливостей штучного інтелекту. Зазначене і те що, що це дані представлені у діапазоні від 0 до 1 зміцнюють логіку

представленої формули. Так, є як теоретичне обґрунтування ваг, а й емпіричне підтвердження допустимості такого встановлення ваг.

Кореляція індикаторів зміцнює логіку формування показника можливостей штучного інтелекту – маніфестація єдиної концепції підкріплюється даними вісім країн.

Формула (2.2) обчислення індикатора можливостей штучного інтелекту (AI capability) має такий вигляд:

$$\text{AI capability}=(0.25\cdot UT+0.25\cdot MF+0.3\cdot(SC+LA)+0.2\cdot(JO+RS))4 \qquad (2.2)$$

У формулі (2.2) обчислення індикатора можливостей штучного інтелекту (AI capability) представлений показник UT як показник застосування/використання штучного інтелекту в публічному та державному управлінні, а також у військовій сфері, що відноситься до «технологічної» сфери. Показник MF (фінансування штучного інтелекту у військовій сфері) відноситься до «економічного» блоку. Показник SC є показником державних підприємств, організацій у сфері штучного інтелекту, а LA – це показник наявності правових санкцій на застосування технології штучного інтелекту у військових цілях. Останні показники MF і LA відносяться до області «управління». Крім того, наявні ще два показники, що відносяться до «соціальної» сфери, а саме: JO як показник зайнятості у сфері штучного інтелекту, і RS – це показник стартапів у сфері штучного інтелекту.

Продемонструємо розрахунок можливостей штучного інтелекту (AI capability) на конкретних практиках, що були поширені у Швеції у 2019 р. Так, показник застосування/використання штучного інтелекту в публічному та державному управлінні, а також військовій сфері (UT), що відноситься до технологічної сфери, є бінарним та відповідає «1» на підставі звіту «Штучний інтелект у шведському бізнесі та суспільстві» [120]. Показник фінансування штучного інтелекту у військовій сфері Швеції (MF) набуває значення «0.0029», оскільки розраховується ставленням фінансування штучного інтелекту у військовій сфері та секторі безпеки на загальні

військові витрати. Згідно з офіційною статистикою Швеції (розділ R&D у Швеції присвячений технології штучного інтелекту [120], а також офіційному звіту [120]) було виділено фінансування в обсязі 17.39 млн. При цьому, загальні військові витрати, відповідно до бази SIPRI [309], за 2019 р. становили 5920.1 млн. по всіх країнах усі фінансові дані призводилися до єдиного значення валюти США за чинним курсом тимчасового періоду. Відповідно розрахунок відносин дозволив встановити значення показника фінансування штучного інтелекту у військовій сфері Швеції. У продовження варто відзначити, що показник області управління включає два бінарні підпоказники. Перший показник державних підприємств у сфері штучного інтелекту (SC). Станом на 2019 р. він набув значення "1", адже було створено державні компанії з розробки штучного інтелекту та технологій подвійного призначення із системами штучного інтелекту (зокрема, компанію Universes [336], що займається автоматизацією та розвитком штучного інтелекту). Другий показник – наявність правової (-их) санкції (-й) на застосування технології штучного інтелекту у військових цілях (LA), що також мав значення «1» на підставі національного звіту Національного підходу до штучного інтелекту Швеції [262].

Два показники соціальної сфери Швеції, що передбачає використання штучного інтелекту – показник зайнятості у сфері штучного інтелекту (JO) та показник стартапів у сфері штучного інтелекту (RS) – також бінарні й отримали значення «0» та «1» відповідно. За показником зайнятості, на жаль, не було встановлено достовірних офіційних даних, тому показник отримав значення «0». Показник стартапів у сфері штучного інтелекту у Швеції, у свою чергу, ґрунтувався на масштабній базі даних з аналітики технологічних компаній Crunchbase [169], де зазначалася не лише афіліація з країною, а й фінансування та всі дані щодо реєстрації стартапу.

У результаті застосування формули з розподілом ваг та розподілом на заявлені 4 області (блоки) було отримано значення можливостей технології штучного інтелекту (AI capability) у Швеції за 2019 р., що дорівнює «1.05».

Цей приклад демонструє загальну логіку розрахунку та спрямований на формування розуміння можливостей формули (2.2).

Формування індикатора оцінки загроз спирається на підходи вузькоспеціалізованого предметного поля досліджень військового озброєння та військових загроз. Оцінка загроз передбачає оцінку та ранжування загрози, а також відповідне призначення зброї (двоетапні моделі) або оцінку сприйняття загрози, розрахунок індексу загрози та призначення зброї (трьохетапні моделі). Створення повноцінної системи реагування та протидії загрозам виходить за рамки даного дослідження, у зв'язку з чим зазначені підходи приймаються як основний методичний підхід [166; 172; 229; 239; 259].

У цьому дослідженні основна логіка є оцінкою загрози і співвідношення цих загроз з об’єктами та секторами безпеки, що захищаються у законодавстві. Виходячи з логіки відповідності, формула розрахунок представляє собою відношення розрахунку загроз на об’єкти та сектори безпеки. Таким чином, оцінка загроз враховує показник сприйняття загрози та характеристику/тип загрози. При цьому дослідники підкреслюють високу роль оцінювання в моделі показника значення захисту активів (protection value), який призначається особою, яка приймає рішення і знаходиться в диапазоні між 0 і 1 [239]. Такий показник необхідний для врахування розподілу пріоритету загроз із боку політичних акторів та осіб, які ухвалюють рішення у сфері забезпечення національної безпеки. Рекомендована модель також матиме показник значущості (PV) як елемент пріоритету з боку держави.

У свою чергу, активи/об’єкти, що захищаються – це те, на що, власне, спрямовані загрози технології штучного інтелекту. Усвідомлюючи це обмеження неможливості практичного розрахунку загальної кількості активів/об'єктів, що захищаються, ураховуємо ті галузі (сектори), які визнаються державою, як ті, що захищаються (наприклад, сектори й об’єкти критичної інфраструктури).

Ураховуючи секторальний підхід аналізу сфери забезпечення нацбезпеки, запропонований Копенгагенською школою, може також запроваджуватися показник – фактор загрози (TF). Цей показник дозволяє сфокусувати процес визначення чинників окремих категорій. Більш детальний опис та обґрунтування розрахунку формули наведено у додатку 3.

Формула розрахунку загроз (2.3) із метою дослідження може мати такий вигляд:

$$TE = \frac{(PV \cdot (TP + TT))}{(DA \cdot TF)} \qquad (2.3)$$

Формула розрахунку загроз містить показники значущості (PV), сприйняття загроз (TP), показник характеру/типу загрози (TT), показник кількості об’єктів (DA), що захищаються, і показник факторів загроз (TF). Іншими словами, логічний зміст формули можна представити таким чином: оцінка загроз (TE) є відношенням суми показника сприйняття загроз (TP – як загрози представлені на рівні нормативно-правових актів) та показника характеру/типу загрози (TT – як загрози представлені у звітах, релевантній літературі) помножена на показник значущості (PV – як особи, яка приймає рішення та політичні актори, які оцінюють важливість/значимість загроз) до показника кількості об’єктів, що захищаються (DA – об’єкти/активи на які спрямовані загрози) на показник факторів загроз (TF – оцінка та ранжування секторів безпеки до яких відносяться загрози).

Відмінна ознака формули (2.3) – це те, що уряди (потенційно) повинні враховувати та співвідносити загрози з тим, на що останні спрямовані (на соціальну сферу, економічну, екологічну тощо). Детальний опис розрахунку формули представлений у додатку 3. Там же представлені описові статистичні дані показників та кореляційні матриці для кожної країни. Для всіх країн властивий позитивний коефіцієнт кореляції показників індикатора оцінки загроз, за винятком Німеччини та Фінляндії. У обох країнах

негативна кореляція демонструється показником ТР (показник характеру/типу загроз). Зазначене пояснюється специфікою внутрішньої системи національної безпеки і частковою обмеженістю даних щодо цих країн. Однак у подальших дослідженнях та при розширенні вибірки країн, може бути проведено додатковий аналіз чутливості та тестування показників індикатора оцінки загроз з особливою увагою до показника ТР для підвищення валідності. Зазначене можна виразити у вигляді блок-схеми оцінки загроз (рис. 2.5).

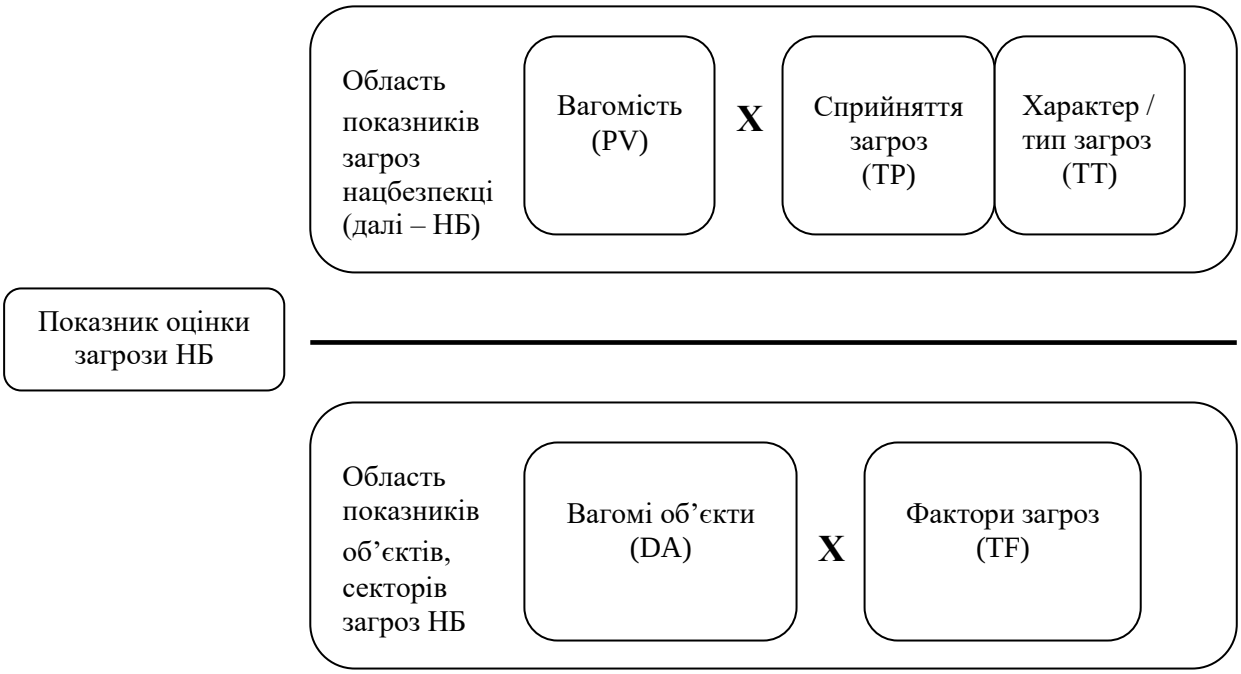

Рис. 2.5. Блок-схема – показник оцінки загрози національній безпеці в умовах цифровізації

Джерело: складено на підставі [125]

Дорнечно надати розрахунок формули на прикладі Швеції за 2019 р., аналогічно, як і з прикладом можливостей штучного інтелекту. Область показників загроз включає три показники: значимість (PV), сприйняття загроз (TP) та характер загроз (TT). Показник значущості (PV) формується з наступних характеристик: технологія штучного інтелекту в стратегії національної безпеки країни, окремий державний орган з проблематики

штучного інтелекту, національна стратегія з штучного інтелекту, сформульоване визначення штучного інтелекту в національній стратегії з цифрової трансформації, державні підприємства з розробки технології штучного інтелекту у військовій сфері та/або у сфері безпеки. Кожна характеристика подається за бінарнім вимірюванням (0 – відсутня, 1 – присутня) і розраховується з розподілом ваг, у результаті сам показник значущості набуває значення від «0» до «1». Характеристика наявності окремого державного органу, що займається проблематикою штучного інтелекту, має вагу «0.3», адже якщо в рамках системи державних органів у структурі забезпечення безпеки створено спеціальний орган, присвячений технології штучного інтелекту, то можна стверджувати, що держава визнає значний пріоритет даної технології. Для прикладу Швеції, за даними у 2019 р. всім характеристикам може бути присвоєно значення «1», оскільки Стратегія національної безпеки Швеції визнає технологію штучного інтелекту як одну з пріоритетних, а в 2019 р. було сформовано окреме відомство – AI Sweden [120], прийнята й упроваджується національна стратегія Швеції зі штучного інтелекту [262], він регламентований у стратегії з цифрової трансформації Швеції [192], а також створені та фінансуються державні програми розвитку систем штучного інтелекту.

Очевидно, що загальнодержавне сприйняття загроз (ТР) формується на підставі стратегій та інших нормативно-правових актів країни, які можуть визначати три елементи:

1) показник освіти (розраховується виходячи з показників результатів країни за рейтингом PISA виключно за напрямом математики, тому що математична освіта є фундаментальною для розробок та застосування технології штучного інтелекту);

2) показник нормативного регулювання – це питома вага нормативно-правових актів (далі – НПА), що визначають у тій чи іншій мірі загрози з боку технології штучного інтелекту, розраховується таким чином: кількість НПА зі згадуванням технології штучного інтелекту на загальну кількість

НПА на рік) та показник внутрішніх патентів (враховувалися лише внутрішньодержавні патенти за тематикою «Штучний інтелект». Якщо для показника освіти використовується база даних PISA з математики, то за 2019 р. рейтинг Швеції становив 502 бали з максимуму 600 балів. Відповідно, показник освіти набував значення «0,83». Показник нормативного регулювання розраховується, виходячи з національної бази нормативно-правових актів Швеції [313] за ключовими словами за конкретний рік. Відповідно, у 2019 р. у Швеції було прийнято та видано 66 релевантних нормативних актів (за тематикою штучного інтелекту) із 1336 усього прийнятих правових актів за звітний період. Відповідно, показник нормативних актів набув значення «0,049». Розрахунок патентів ґрунтувався на базі даних Всесвітньої організації інтелектуальної власності [347], при цьому доречно враховувати саме внутрішні патенти. У 2019 р. Швецією було зареєстровано 17 патентів на тематику штучного інтелекту із загальної кількості рівної 161 патенту. Відповідно, показник внутрішніх патентів набув значення «0,10». Зазначені показники можна підсумувати, відтак, показник сприйняття загроз набуває значення «0.99». Це дуже високий показник, що майже дорівнює 1.

Характер/тип загрози (ТТ) ґрунтується на дослідженнях, індексах та показниках звітів, експертних оцінок. Цей показник може бути представлений як демонстрація конкретного (обчислюваного) показника характеру/типу загроз. Однак на даний момент відсутні стійкі статистичні показники безпосередньо релевантних технологій штучного інтелекту [153; 155; 230]. З огляду на проаналізовані дані може бути визначено бінарний показник:

0 – тип/характер загрози, що був відсутній у країні у цьому періоді;

1 – тип/характер загрози був присутній (зафіксований/ задокументований) у країні у звітному періоді, згідно з наступним переліком типів/характеру загроз штучного інтелекту [116; 127; 264]:

1. Загрози критичній інфраструктурі;

2. Кіберзагрози / Кібератаки, що здійснюються за допомогою технологій штучного інтелекту (вони розширюють вектори загроз, виявляючи та експлуатуючи слабкі місця системи);

3. Компанії з дезінформації (зокрема Deepfakes);

4. Порушення прав людини (мається на увазі, порушення персональних даних, загрози біометричним даним тощо).

Відповідно до зазначеного переліку за кожен конкретний рік може формуватися показник від «0» до «1». Якщо у досліджуваному році було зафіксовано якийсь тип загроз, то виставляється «1», якщо не було – «0».

На прикладі Швеції, загрози критичній інфраструктурі можуть бути визначені у державному звіті за 2019 р. [125]. Крім того, кіберзагрози та кібератаки визначалися у звіті Міністерства закордонних справ Швеції [Nordic Foreign and Security Policy], компанії з дезінформації вказувалися у звіті Міністерства підприємництва та інновацій, а порушення прав людини були прописані Міністерства іноземних справ нації. Таким чином, за 2019 р. показник типу загроз набував значення «1».

Нагадаємо, що зазначені три показники відносяться до області показника загроз. Область показників об’єктів/секторів загроз представлена двома показниками: об’єкти, що захищаються (DA) і фактори загроз (TF). Об’єкти, що захищаються/активи (DA) – те, на що, власне, спрямовані загрози технології штучного інтелекту. Ураховуючи специфіку даного дослідження, з практичної точки зору, неможливо вирахувати загальну кількість активів/об’єктів, що захищаються, адже бази даних щодо тих же об’єктів критичної інфраструктури у значній кількості країн світу є обмеженими в доступі. Тому враховуватися може чисельний бінарний показник, що охоплює кількість згадувань в НПА країни терміну «штучний інтелект», або дані, що захищаються, дані державних компаній, персональні дані громадян тощо. Для Швеції може бути виділено 8 об’єктів/активів, виходячи з національного законодавства (розвіддані, державні дані, персональні дані, автономно керовані автомобілі та техніка, автономне

озброєння, об’єкти інфраструктури інформаційної сфери, космічні операції та цифрова інфраструктура з кібероперaціями). Кожен об’єкт/актив оцінювався за допомогою бінарних значень: наявності чи відсутності загроз. У свою чергу, показники загроз можуть оцінюватися по п’яти секторах безпеки, що визначена Копенгагенською школою, з ранжуванням від «0» до «3». Тобто за рівнем: 0– відсутня; 1 – наявна локальна загроза; 2 – наявна регіональна загроза; 3 – наявна міжнародна загроза. Фактори загрози (TF) ураховуються як питома вага відношення суми шкали оцінювання на максимальну кількість оцінок сфер безпеки. Для прикладу Швеції (згідно з отриманними даними за 2019 р.), показник фактора загроз набуває значення «0.8». Таким чином, застосування формули (2.3) дозволяє розрахувати оцінку загроз для Швеції у 2019 р., що набуває значення «0.77» [125].

Зазначений приклад розрахунку як можливостей штучного інтелекту, так і оцінювання загроз спрямований на формування розуміння та загальної логіки розрахунків. Детальна характеристика наведена у додатках 3 та 4. Розрахунок проксі показників дозволяє стверджувати про сумісність показників та допустимість застосування такого підходу до формування показників. Додаткове тестування чутливості моделі, має бути наведено на прикладі інших країн-партнерів України в реалізації її європейських і євроатлантичних інтеграційних прагнень, що забезпечить підтвердження валідності рекомендованої моделі публічного управління у сфері нацбезпеки. Зазначимо ще раз, що будь-яке моделювання не є демонстрацією беззаперечної істини, тому потрібно підходити виважено до інтерпретації отриманих результатів. При цьому слід розуміти, що як на рівні теоретичного обґрунтування, так і на методичному рівні з тестуванням рекомендована модель публічного управління у сфері нацбезпеки допустима і дозволяє досягти поставленої мети та завдань дослідження.

Зазначимо, що узгодженість елементів національної безпеки, як результат моделі публічного управління, що реалізується в умовах впливу цифрових технологій, є умовним способом вимірювання ступеня, в якому

показники можливостей штучного інтелекту й оцінювання загроз співвідносяться разом як загальне та часткове. Власне кажучи, показник узгодженості елементів нацбезпеки й цифровізації, наприклад, приймаючи значення «0» означає ідеальну узгодженість, при цьому лише відображає як уряди оцінюють можливості визначати загрози, але не означає механізмів як реагувати на них. Цілком можливо, що уряди публічно не заявляють про можливі загрози, чому й рекомендована модель публічного управління, побудована на відкритих даних, ніяк не може відобразити, або уряди просто не надають політичного значення таким загрозам, тобто ніяк не відображають їх у НПА, звітах тощо. Вказане, безумовно, є обмеженням, але воно відноситься до будь-якого виду моделювання (адже, як зазначалося вище, певні бази даних мають обмежений доступ у цілях безпеки). Таким чином, отримані результати можуть демонструвати необхідність обґрунтування альтернативних механізмів публічного управління у сфері гарантування національної безпеки в умовах впливу цифровізації та її технологій. Зупинимося на особливостях верифікації та тестування запропонованої моделі на прикладах окремо взятих країн.

Незважаючи на теоретичне обґрунтування та практичну реалізацію моделі публічного управління у сфері нацбезпеки необхідна її верифікація та тестування. Необхідність обумовлена як раціональною вимогою до внутрішньої верифікації, так і зазначеною вище специфікою самої сфери нацбезпеки, а саме: обмеженнями доступу до даних.

Для верифікації та тестування моделі публічного управління у сфері нацбезпеки може бути реалізовано її чисельне дослідження (simulation analysis, за на прикладом наведеним у [250]). Логіка кількісного дослідження спрямована на перевірку чутливості моделі [187], при цьому потрібно зважати на такі питання: що, якщо якась частина даних не відповідає реальності, є хибною або зовсім відсутня; наскільки це сильно вплине на результати. Отже, тестування моделі публічного управління у сфері нацбезпеки в умовах впливу цифрових технологій із допомогою

прогнозування спрямовано на отримання відповідей на зазначені питання.

Кількісне дослідження моделі реалізовувалося поетапно у відповідності до кожного показника [187], тобто до кожного показника окремо ставиться питання дійсності даних. Реалізовується це таким чином: 1) для кожного показника створюються підроблені; 2) відтворюється модель з усіма вихідними показниками, але замість тестованого показника випадковим чином використовуються значення з хибними даними. При цьому важливо, щоб модель будувалась із використанням мінімального значення хибних даних (тобто допустимий мінімум) та окремо з максимальним значенням хибних даних (аналогічно «допустимий максимум»); 3) у результаті після кожного прогнозування має бути отримано новий результат моделі, який порівнювався з первинним, для отримання остаточного.

Таким чином, був протестований кожний показник з моделі публічного управління у сфері національної безпеки в умовах впливу цифрових технологій. При порівнянні (у тому числі з мінімальним, і з максимальним допустимим значенням за кожним конкретним показником) може бути зроблено висновок про стійкість моделі до даних конкретного показника. Слід зазначити, що при порівнянні рішення про стійкість цієї моделі має враховуватися розподіл змодельованого (з урахуванням прогнозу) фінального показника в межах стандартного відхилення. Іншими словами, якщо розподіл знаходився в межах одного стандартного відхилення, то приймається рішення про стійкість моделі до варіативності значень даних конкретного показника.

За підсумками моделювання з отриманими даними може бути спрогнозовано відповідну модель публічного управління у сфері нацбезпеки в умовах впливу цифрових технологій (додаток 4), а саме:

1. Модель стійка до загроз і таких показників: «фінансування у військовій сфері» (Military fundings – MF) з індикатора «можливостей штучного інтелекту» (економічна сфера); сприйняття загроз (Threat

perception – TP) з індикатора «оцінки загроз».

2. Модель чутлива до загроз і таких показників: технологічної сфери з індикатора «можливостей штучного інтелекту» (UT – use of technology), але тільки у бік максимальних значень; соціальної сфери з індикатора «можливостей штучного інтелекту» (JO (job openings) + RS (стартапи)), але у бік максимальних значень; фактори загроз (threat factors - TF) з індикатора «оцінка загроз» як до мінімальних, так і до максимальних значень.

3. Модель, що передбачає подальше оцінювання загроз і показників, які підлягають тестуванню, оскільки їхнє мінімальне і максимальне значення, що приймалося, було присутнє в первинній моделі за звітний період, а саме: сфера управління (SC (state companies) + LA (legal authorization)) з індикатора «можливостей штучного інтелекту»; тип/характер загроз (TT), об’єкти/активи (DA), що захищаються, та значність/цінність об’єктів, що захищаються (PV) з індикатора оцінки загроз.

4. Модель демонструє стійкість до більшості показників і загроз. Однак слід звертати особливу увагу на джерела даних щодо показника «фактори загроз» (threat factors – TF) з індикатора «оцінка загроз». Зазначений показник може давати значну помилку під час побудови моделі публічного управління у сфнері національної безпеки. Тому при роботі з даними країн за кожним показником ці дані повинні проходити додаткову верифікацію. Схожа, але менш загрозлива ситуація є і з показниками «технологічної та соціальної сфери» з індикатора «можливостей штучного інтелекту», де модель чутлива лише до максимальних значень показників. До цих показників додатково має перевірятися перебільшення даних із доступних джерел.

Безпосередня реалізація емпіричної моделі публічного управління у сфері нацбезпеки для конкретно обраної країни може пройти як окремим, так і за єдиним протоколом. На першому етапі має визначатися тимчасове охоплення, релевантне для кожної країни. При визначенні тимчасового охоплення в аналізу може бути взято:

1) основні нормативно-правові акти у сфері забезпечення національної безпеки (стратегії національної безпеки, закони, декрети, доктрини тощо, що визначають систему безпеки держави);

2) основні нормативні документи інформаційно-технічної сфери з фокусом на цифровізацію, алгоритмізацію, автоматизацію політики та державного управління (з урахуванням концепції електронного уряду, аж до регулювання конкретних типів цифрових технологій);

3) тимчасове охоплення з урахуванням кількох урядів/адміністрацій для динаміки змін.

Після формування тимчасової таблиці даних може бути розпочато безпосередній збір даних за кожним показником моделі публічного управління у сфері національної безпеки в умовах впливу цифровізації. Обов'язковою умовою збору даних був аналіз як національних НПА й офіційних статистичних даних, так і міжнародних звітів, баз даних тощо за аналізованою тематою щодо конкретно взятої країни. У результаті для кожної країни може бути сформовано дата-сет, де до кожного значення показника робиться позначка джерело даних (для верифікації). Дані можуть бути доступні у відкритому репозиторії GitHub за стабільним посиланням окремими файлами по кожній країні.

При побудові дата-сету по кожній країні має бути проведено розширену роботу з національними НПА та офіційними даними статистики. Якщо при обгрунтуванні дат-сету враховується лише основні акти держав, дані для моделі публічного управління у сфері нацбезпеки накопичуються внаслідок аналізу всіх суспільно-політичних ріщень. Так, для виявлення перспектив застосування штучного інтелекту в публічне та державне управління, а також у військову сферу (показник UT), для уточнення наявності правової санкції на використання штучного інтелекту у військовій сфері (показник LA), виявлення типу/характеру загроз (показник TT), встановлення об'єктів/активів (показник, що захищаються) PV) і для розрахунку питомої ваги НПА, що визначають загрози з боку штучного

інтелекту (елемент Regulation (Reg) у показнику сприйняття загрози – TP) враховуються всі нормативно-правові акти з офіційних сайтів урядів/легіслатур окремо взятої країни [242]. Аналогічно, розширений аналіз доступних НПА може проводитися за всіма показниками. Наприклад, розрахунку показника фінансування (military fundings – MF) враховуються як «загальні» статті бюджету, так і специфічні, вузьконаправлені звіти (для моделі США враховувалися, зокрема, National Defence Authorization Act for Fiscal Year). Однак у разі відсутності даних на національному рівні – мають ураховуватися дані міжнародних організацій, як це було з показником патентів для Швеції (питома вага кількості внутрішніх патентів – елемент DP показника сприйняття загрози), де для всіх країн використовувалася база Міжнародної організації інтелектуальної власності [347].

На наше переконання, проведення дослідження за такою логікою дозволить на системній основі виявити та простежити зміни, які відбуваються безпосередньо на національному (внутрішньому) рівні країни. Використання загальних (наднаціональних) документів потрібне лише в разі відсутності (або не публічності) внутрішніх джерел. Для побудови, тестування та валідизації моделі публічного управління у сфері нацбезпеки всі обчислення можуть проводитись у безкоштовному програмному середовищі для статистичних обчислень.

2.3. Сучасний стан функціонування механізмів публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні

Аналіз наукових напрацювань щодо формування та класифікації механізмів публічного управління у сфері національної безпеки в умовах цифрової трансформації дав підстави виокремити в їхньому (механізмів) складі організаційний, правовий, інформаційний і ресурсний механізми. Як

зазначалося вище, вони чинять взаємний вплив один на одного, тому складно не розглядати їх саме з позиції застосування комплексного підходу. Інакше поза увагою можуть залишитись латентні проблеми, що можуть актуалізуватись під впливом сприятливих умов, трансформувавшись у загрози. Отже, вважаємо за доцільне зупинитися на сучасному стані функціонування механізмів публічного управління у сфері нацбезпеки в умовах впливу цифрових технологій, зокрема, розгляді із застосуванням комплексного підходу.

Як відомо, цифрові технології реалізуються у декількох формах: 1) соціальній, що передбачає акцентування уваги на самому населенні, яке є одержувачем послуг та користувачем інформації, а також її ретрансляторами; 2) фізичній, що може зумовлювати розвиток цифрового й інформаційного суспільства, вимогою якого є якомога ширше застосування новітніх інструментів та цифрових технологій, необхідних для отримання та передачі інформації, покращення рівня свого добробуту, соціально-економічного розвитку територій тощо; 3) цифровій або віртуальній, яка підсилює функціонування двох вищевказаних форм цифрових технологій шляхом розробки й упровадження програмного забезпечення, сервісів та ін. у ті чи інші сфери суспільної життєдіяльності.

Розгляд наукової літератури також дозволяє підкреслити важливість виокремлення типів сучасних цифрових технологій, що розвиваються під впливом тіє або іншої їхньої форми набувають. Серед типів цифрових технологій виділяють такі: технології зв’язку; технології зберігання; технології аналітики; технології виготовлення; технології візуалізації; інтерактивні технології; технології інтерфейсів «людина – машина»; сенсорні технології. Вони використовуються по різному публічними (державними та приватними) інституціями, адже неоднаковою є мета та методика впровадження цифрових технологій. Зважаючи на предмет дослідження, уважаємо за доцільне зупинитись на аналізі особливостей застосування цифрових технологій саме в державному секторі, а також на

умовах, необхідних для цього (організаційно-правових, ресурсних тощо).

В Україні було розроблено та затверджено чимало стратегій національної безпеки, кожна з яких не відзначається комплексністю ні у визначенні ризиків і загроз, що впливають на таку безпеку, ні у механізмах їхнього попередження та реагування на них. На жаль, складності ситуації додає те, що неповнота правового регулювання спостерігається від початку проголошення незалежності України (табл. 2.4).

Так, якщо говорити про першу Стратегію національної безпеки України (2007 р.), то в цьому правовому документі, на перший погляд, начебто правильно робився акцент на визначенні місця України у світі, що змінюється, а також на неефективності гарантій її безпеки. Крім того, у стратегії визнано нездатність України протистояти новітнім викликам національній безпеці, що пов'язані із застосуванням інформаційних технологій в умовах глобалізації, насамперед кіберзагрозам [81, п. 3.3]. З цією метою визначено основні завдання політики нацбезпеки у внутрішній сфері [там само, п. 4.3], серед яких виокремлено економічну, соціальну, інформаційну та інші сфери безпеки.

Слід констатувати, що розробники першої Стратегії у сфері нацбезпеки все ж таки найбільше занепокоєння висловили щодо геополітичних трансформацій і щодо перетворення нашої держави на «сіру зону безпеки» [там само, Розділ 1 «Загальні положення»]. Не цього потрібно було боятися розробникам стратегії нацбезпеки України, а саме впливу поширення зброї масового ураження, міжнародного тероризму, нелегальної міграції, ескалація міждержавних і громадянських конфліктів тощо. Усі ці загрози стали інтенсивними, охопивши нові регіони й держави, що (загрози) за своїми негативними наслідками набувають глобального впливу.

Крім того, не можемо погодитись із розробниками Стратегії національної безпеки України (2007 р.) [там само], що на той час найбільш нагальними залишалися внутрішні виклики національній безпеці. Це ще раз підкреслює однобічність у визначенні загроз у сфері національної безпеки

України, що поступово призводило до зниження рівня її безпеки, підходящого для реалізації зовнішньої агресії рф.

Таблиця 2.4

Основні нормативно-правові акти, що визначають засади публічного управління у сфері національної безпеки України

№	Назва нормативно-правового акту у сфері національної безпеки України
1.	Декларація про державний суверенітет України
2.	Постанова Верховної Ради Української Радянської Соціалістичної Республіки «Про проголошення незалежності України»
3.	Заява про без'ядерний статус України
4.	Конституція України (1996 р.)
5.	Указ Президента України від 12.02.2007 р. № 105 «Про Стратегію національної безпеки України»
6.	Указ Президента України від 08.06.2012 р. № 389/2012 «Про нову редакцію Стратегії національної безпеки України»
7.	Постанова Кабінету Міністрів України від 26.11.2014 р. № 671 «Положення про Міністерство оборони України»
8.	Указ Президента України від 26.05.2015 р. № 287/2015 «Про Стратегію національної безпеки України»
9.	Постанова Уряду України від 28.10.2015 р. № 878, якою затверджено «Положення про Міністерство внутрішніх справ України»
10.	Постанова Кабінету Міністрів України від від 16.12.2015 р. № 1052 «Про затвердження Положення про Державну службу України з надзвичайних ситуацій»
11.	Закон України «Про засади внутрішньої і зовнішньої політики»
12.	Закон України «Про оборону України»
13.	Закон України «Про Службу безпеки України»
14.	Закон України «Про національну безпеку України»
15.	Указ Президента від 14.09.2020 р. № 392/2020 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»

Джерело: складено на підставі [60]

Безперечно, на момент затвердження аналізованої стратегії (2007 р.) в Україні накопичилось чимало внутрішніх проблем, пов'язаних із корупцією, викривленням демократичних процедур, гальмуванням процесів кадрового оновлення на всіх рівнях державного управління, неспроможністю держави виконувати свої обов'язки щодо захисту прав і свобод громадян, підтримання

рівня довіри населення до органів державної влади тощо. Важливо підкреслити, що в цій стратегії розробники передбачали вплив вищезазначених проблем, як можуть становити підґрунтя для посилення політичніої радикалізації, зростання екстремістських настроїв і рухів, що загрожують національному суверенітету і територіальній цілісності України [там само]. У 2007 році в межах аналізованої стратегії також акцентувалось на «виникненні самопроголошених квазідержавних утворень на територіях суверенних держав, поява небезпечних прецедентів визнання іншими державами деяких із цих утворень, що може стати стимулом для процесів регіонального сепаратизму» [81, п. 3.1]. Проте такі перестороги так і залишились на папері, їхнім попередженням не займались належним чином на всіх рівнях державного управління. Можна, звісно, говорити про те, що реалізації першої стратегії у сфері нацбезпеки перешкодила наступна стратегія, розроблена в цій сфері, яка є «проросійською». Однак між цими стратегіями національної безпеки різниця становила 5 років – це мінімальний термін для короткострокового стратегічного планування. Відтак, Україна мала необхідний час для впровадження «однобічної, безперспективної» стратегії 2007 року, на зміну якій було прийнято не менш недосконалу Стратегію національної безпеки 2012 року.

Перед тим як перейдемо до аналізу її положень відзначимо, що невирішені внутрішні проблеми, окреслені у Стратегії національної безпеки України (2007 р.), і неврахування зовнішніх загроз, потягло за собою появу нових і кристалізацію старих проблем. Зауважимо, що вчасне та комплексне їх визначення й реагування на них становило би базис для попередження трагічних для України подій, організатором яких є держава-агресорка, починаючи з 2014 р. Власне кажучи, потрібно говорити про те, що необхідним є вчасне результативне реформування системи державного управління, забезпечення розвитку сучасного військово-оборонного комплексу, здатного протистояти зовнішній збройній агресії, а також розвитку інформаційного та цифрового суспільства, яке б могло протистояти

інформаційним впливам, дезінформації тощо. Ось на що мала б бути зорієнтована *перша* Стратегія національної безпеки України у 2007 році. Крім того, сьогодні потрібно говорити про включення до стратегічних засад правового регулювання в цій сфері, зокрема, аспектів впливу цифрових технологій на національну безпеку.

У продовження умовного плану дослідження відзначимо, що у 2012 році на заміну першої стратегії було розроблено та затверджено нову, з якої прибрали всі згадки про інтеграційні прагнення України, зокрема, європейські й євроатлантичні. Цікаво, що в п. 4.2.3 Стратегії нацбезпеки України (2007 р.) було визначено, що одним із основних завдань політики національної безпеки у зовнішньополітичній сфері є створення умов для інтеграції нашої держави в єдиний європейський політичний, економічний, правовий простір, у тому числі шляхом розвитку секторального співробітництва з ЄС [81]. Однак у 2012 рці було внесено зміни до цієї Стратегії у п. 4.2.6, де визнавалась важливість дотримання Україною політики позаблоковості [там само]. На підставі зазначеного можемо вважати, що розробники першої стратегії нацбезпеки України намагались забезпечувати її стабільний розвиток насамперед економічними засобами й уникати аспектів міжнародної взаємодії у межах військового та блокового векторів. Отже, можемо зробити такий проміжний висновок: у першій і наступній Стратегіях національної безпеки України була низка положень, що протирічили один одному, зокрема, визнавалась неефективність гарантій безпеки для неї, і при цьому вказувалось на необхідність пошуку шляхів та механізмів посилення міжнародних гарантій безпеки України [там само, п. 4.2.6, абз. 5 Розділу 1 «Загальні положення»]. На жаль, вирішенню цих проблеми організаційно-правового характеру не судилося збутися. Навіть незважаючи на те, що у Стратегії національної безпеки України (2007 р.) визнавалась можливість її реалізації на третьому етапі (2016 і наступні роки), яка відзначається коригуванням цієї стратегії на основі оцінки ефективності її впровадження.

Ще раз зазначимо, що в Стратегії національної безпеки України 2012 року [82] взагалі уже неможливо відшукати такого роду положень, які б стосувались реалізації нашою державою євроатлантичних інтеграційних прагнень. В аналізованому правовому документі визнається проблема погіршення регіонального безпекового середовища навколо України, але не в її середині. Подібна завуальованість масштабних проблем є свідченням небажання тогочасних високопосадовців застосовувати комплексний підхід до забезпечення системи безпеки в Україні.

Вирішити вищенаведені проблеми правового регулювання у сфері національної безпеки, на яку значною мірою впливають цифровізація загалом і її технології зокрема, мала б Стратегія національної безпеки України, затверджена указом Президента України від 26.05.2015 р. № 287/2015 [83]. На відміну від першої стратегії ця не мала пафосних назв, і розроблялась як результат зреалізованої революції гідності. Саме з цих слів починається преамбула Стратегія національної безпеки України (2015 р.). Крім того, привертає увагу теза аналізованої стратегії, згідно з якою рф визнається країною, що перешкоджає волі Українського народу до європейського майбутнього шляхом окупації українських територій і ревізії світового порядку [там само]. Як і в перші стартегії, у стратегії нацбезпеки України (2015 р.) також наголошується на загрозах безпековому середовищу – зовнішніх і внутрішніх. Проте не зрозумілою є логіка формулювання вітчизняним законодавцем цих загроз. Власне, установлено, що «російська загроза, що має довгостроковий характер, інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України обумовлюють необхідність створення нової системи забезпечення її національної безпеки» [там само]. Виникає запитання, чому «російська загроза» прирівнюється до «інших докорінних змін у безпековому середовищі». Загроза ніяк не можа розглядатись у контексті докорінних змін; це не синоніми, загрози можуть зумволювати виникнення певних змін (правових, організаційно-функціональних, структурних, кадрових тощо). У

той же час, бачимо, що вітчизняний законодавець знову пішов шляхом невхтування принципів фундаментальної науки у формуванні механізмів публічного управління у сфері національної безпеки. Поза увагою залишився негативний досвід розробки та впровадження попередніх двох стратегій у сфері нацбезпеки (2007 і 2012 років).

У «Загальних положеннях» Стратегії національної безпеки України (2015 р.) установлено, що вона спрямована на реалізацію до 2020 року. Цей документ також є прикладом короткострокового стратегічного планування, як і попередні дві аналізовані стратегії. На жаль, починаючи з 2014 року Україна перебуває в перманентному стані функціонування (не говорячи взагалі про розвиток), і її державному апарату складно надавати середньострокові прогнозні оцінки щодо стану та перспектив забезпечення національної безпеки. Ураховуючи це, можемо відзначити, що однією зі основних цілей функціонування України (яка не викликає занепокоєння на центральному рівні управління) є забезпечення її інтеграції до ЄС та формування умов для вступу в НАТО, що було закріплено в Стратегії нацбезпеки України (2015 р.) [83, Розділ 2 «Цілі Стратегії національної безпеки України»]. Крім того, у Розділі 2 цієї стратегії визначено такі цілі: 1) мінімізація загроз державному суверенітету та створення умов для відновлення територіальної цілісності України; 2) гарантування мирного майбутнього України; 3) утвердження прав і свобод людини і громадянина, забезпечення нової якості економічного, соціального і гуманітарного розвитку [там само]. У той же час, є очевидним, що ці цілі Стратегії національної безпеки України (2015 р.) не були досягнуті, як й інші задекларовані підцілі: 1) реалізація якісно нової державної політики, спрямованої на ефективний захист національних інтересів в економічній, соціальній, гуманітарній та інших сферах; 2) комплексне реформування системи забезпечення національної безпеки, створення ефективного сектору безпеки й оборони України [там само]. На наше переконання, тільки одна підціль була досягнута, пов’язана з новим зовнішньополітичним

позиціонуванням України у світі. Дійсно, починаючи з 2022 року наша країна асоціюється з війною, техногенними катастрофами, руйнацією, значною міграцією тощо.

Розробники Стратегії нацбезпеки України (2015 р.) додали до актуальних загроз нацбезпеки такі: 1) несформованість сектору безпеки й оборони України як цілісного функціонального об'єднання, керованого з єдиного центру; 2) відсутність ефективних зовнішніх гарантій безпеки України; 3) діяльність незаконних збройних формувань, незаконне використання вогнепальної зброї [83, п. 3.2]. Як бачимо, ці всі загрози та проблеми визнавались і в попередніх стратегіях національної безпеки України (2007 і 2012 років). Проте так і не відбулось урахування на практиці й усвідомлення справжньої природи цих загроз і їхньої спрямованості – незалежність і суверенітет України.

Безумовно, викликає здивування, чому на період розробки та затвердження Стартегії національної безпеки України (2015 р.) так і не було забезпечено реалізацію по ключовим пунктам попередніх стратегій (2007 і 2012 років), а саме: інституційна спроможність; протидія корупції; депрофесіоналізація та деградація державної служби; забезпечення економічної, соціальної, енергетичної, екологічної й інформаційної безпеки. Виникає логічне запитання, навіщо розробляти нову стратегію, яка не відрізняється по ключовим показникам від попередньої стратегії, цілі якої так і не були досягнуті. Це є прикладом нераціонального використання ресурсів (фінансових, людських, інформаційних та інших) і неврахування принципів фундаментальної науки щодо стратегування, конфліктології, ризикології, інституціоналізму, теорії поля та політичної комунікації тощо.

Стратегія національної безпеки України (2015 р.) [83] визначила такі основні напрями державної політики національної безпеки України:

1) відновлення територіальної цілісності України;

2) створення ефективного сектору безпеки й оборони;

3) підвищення обороноздатності держави;

4) реформування та розвиток розвідувальних, контррозвідувальних і правоохоронних органів;

5) реформування системи державного управління, нова якість антикорупційної політики;

6) інтеграція в ЄС;

7) особливе партнерство з НАТО;

8) забезпечення національної безпеки у зовнішньополітичній сфері;

9) забезпечення економічної безпеки;

10) забезпечення енергетичної безпеки;

11) забезпечення інформційної та кібербезпеки;

12) забезпечення безпеки критичної інфраструктури;

13) забезпечення екологічної безпеки.

Очевидно, що подібне формулювання напрямків політики національної безпеки України було наявне у Стратегії національної безпеки України (2007 і 2012 років). Відтак, з упевненістю можемо стверджувати, що не відбувалось повноцінне досягнення цілей політики національної безпеки у період 2007 – 2020 років, окреслених у відповідних Стратегіях національної безпеки України у 2007 р., 2012 р. і 2015 р. Досягнуто було в повній мірі те, що реалізація Стратегії національної безпеки потребувала спрямування щорічно на бюджетне фінансування сектору безпеки й оборони не менше 5 відсотків від ВВП, і такі кошти виділялись (див. наукові роботи С. Домбровської, Є. Нікіпєлової та ін. [26]). Усе це засвідчує дієвість функціонування ресурсного механізму публічного управління у сфері нацбезпеки, зокрема, у частині його фінансового забезпечення. Варто розуміти, що ресурсний механізм публічного управління у зазначеній сфері охоплює не тільки фінансовий складник, а й кадровий та інформаційний. Щодо інформаційного забезпечення публічного управління в досліджуваній сфері, то його оцінено з позиції включеності інформаційної безпеки та кібербезпеки як вектору реалізації Стратегії національної безпеки України. Зважаючи на сучасні умови триваючого воєнного стану в Україні, відзначимо, що складно оцінити

кадровий потенціал у межах ресурсного механізму публічного управління у сфері національної безпеки України через обмеженість відомостей у цій сфері.

Варто зазначити, що, на відміну від раніше затверджених стратегій національної безпеки, Стратегія національної безпеки України (2015 р.) [83] не містила чіткої вказівки на місце та роль цифрових і новітніх технологій у цій сфері. Акецнтувалась увага саме на забезпеченні інформаційної та кібербезпеки, що є необхідним, але цього не достатньо. І доречно зазначити, що в аналізованому стратегічному акті визнається важливість підтримки економічної безпеки, що, у свою чергу, є неможливим без інноваційного та сталого розвитку, а також цифрової трасформації основних сфер суспільної життєдіяльності.

На погляд вітчизняних нормативорців, на період дії Стратегії національної безпеки України (2015 р.) [83] забезпечення інформаційної безпеки можливе було в межах таких пріоритетів (наперед завбігаючи, зауважимо, що формулювання деяких з них є некоректним):

– забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії. Не зрозуміли є, що це за наступальні заходи політики, імовірно, йдеться про «проактивну» і «реактивну» політику та її заходи, спрямовані на забезпечення інформаційної безпеки;

– створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них. Потребує конкретизації (а точніше персоніфікації) суб’єктний склад, покликаний реалізовувати моніторинг й оцінювання загроз інформаційного характеру, а також реагування на них;

– протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю, захист національних цінностей і зміцнення єдності українського суспільства. Знову ж таки незрозуміло, хто має це реалізовувати (Мінкульт, Мінцифри, РНБО України тощо);

– розробка і реалізація скоординованої інформаційної політики органів

державної влади. Насправді це завдання є одним зі складних у реалізації, тому що й досі наявне дублювання сфер компетенції між центральними органами виконавчої влади щодо взаємоузгодженого забезпечення інформаційної політики;

– виявлення суб'єктів українського інформаційного простору, що створені та/або використовуються рф для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності. Виконання цього завдання, насамперед, належить до сфери СБУ і Кіберполіції, і, зважаючи на обмеженість інформації у цій сфері, складно надавати об'єктивні оцінки щодо стану реалізації цього завдання. За свідченням дослідників С. Домбровської, О. Крюкова, В. Новікова, А. Помази-Пономаренко, С. Пороки, у 2023 р. Україна посіла перше місце у світі в списку країн, чиї комп'ютери найбільше схильні до хакерських атак (наприклад, у звітному періоді відбулось 29 таких атак). У 2023 р. у США було зреалізовано 14 кібератак, більшість з яких були на замовлення Ірану та КНР [27, с. 120, 134–135]. Питання протидії інформаційно-гібридним війнам перебувають у центрі уваги США, ЄС, рф, Китаю та інших країн. У зазначеному напрямку рівень протидії інформаційно-гібридним війнам у цих країнах не однаковий через ступінь їхнього розвитку у технологічному плані [56]. Погоджуємось з ученими, що на сучасному етапі основним інструментом під час протистояння інформаційним загрозам є соціальні мережі, що пов'язано з інформатизованістю суспільства, через захоплення цифровими технологіями [27, с. 129];

– створення і розвиток інститутів, що відповідають за інформаційно-психологічну безпеку, з урахуванням практики держав – членів НАТО. У цьому контексті наявні різнохарактерні наукові думки, чи потрібно створювати нову інституцію, чи покласти обов' язок щодо протидії дезінформації на вже існуючі органи державної влади. Цінною, на наше переконання, є позиція О. Новікова та А. Помази-Пономаренко [69], які відзначають, що корисно досліджувати й виважено аплікувати позитивний

закордонний досвід у сфері протистояння загрозам гібридної війни. У цьому контексті науковці пропонують ураховувати досвід США щодо створення та функціонування інформаційної контргібридної пропагандистської структури [там само];

– удосконалення професійної підготовки у сфері інформаційної безпеки, упровадження загальнонаціональних освітніх програм із медіакультури із залученням громадянського суспільства та бізнесу. Щодо даного пріоритету забезпечення інформаційної безпеки України можемо зазначити таке: низка дослідників пропонують напрямки медіатизації інформаційної сфери, з якими можна погоджуватись або ні. Проте з упевненістю можемо наполягати, що рух у цьому напрямку потрібен, і його забезпечують, зокрема, експерти Ради національної безпеки і оборони України, а також Мінцифри тощо. Свідченням цього є розроблений фахівцями Центру протидії дезінформації при РНБО України освітнього курсу «Дезінfакеція твого інфопростору» [27, с. 191–192].

Аналіз наукових напрацювань у сфері забезпечення національної безпеки України та впливу на це цифрових технологій та інформації дає підстави стверджувати про важливість деталізації умов застосування механізмів протистояння інформаційним загрозам і загрозам, пов’язаним із використанням та розвитком цифрових технологій (рис. 2.6).

Отже, з 2015 року в Україні на законодавчому рівні прийнято відповідні закони та нормативно-правові акти, які регулюють відносини у кіберпростору та гарантування інформаційної безпеки. Відповідно до прийнятого законодавства політика інформаційної та кібербезпеки в Україні покладена на низку органів державної влади, а саме: на Державну службу спеціального зв’язку та захисту інформації України, Державну поліцію України, Службу безпеки України, Міністерство оборони та Генеральний штаб Збройних Сил України. У кожному з цих органів є відповідні підрозділи. Наприклад, у структурі кримінальної поліції діє Департамент кіберполіції, який забезпечує реалізацію державної політики у сфері протидії

кіберзлочинності, організовує та проводить відповідно до законодавства оперативно-розшукову діяльність.

Рис. 2.6. Умови застосування механізмів протистояння інформаційним загрозам і загрозам, пов’язаним із використанням цифрових технологій

Джерело: складено на підставі [27, с. 120, 134–135; 69]

У той же час, 2016 рік засвідчив низку слабких місць стратегічної комунікації, зокрема у секторі безпеки і оборони, згідно з даними Українського національного інституту стратегічних досліджень [27, с. 179–180]. Для усунення цих недоліків, таких як «суттєва відсутність документів, що регламентують зв’язок», та для забезпечення створення системи стратегічних комунікацій розроблено та прийнято низку законодавчих документів, які забезпечують створення та функціонування системи

стратегічної комунікації в секторі оборони та безпеки. Так, наприкінці 2016 року Україна ухвалила Доктрину інформаційної безпеки [60]. До речі, у 2021 році буде затверджена Стратегія інформаційної безпеки, що передбачає комплексну взаємодію на основі Конституції України, законів України, Стратегії національної безпеки України [там само].

Слід констатувати, що в 2020 році на заміну вищевказаним стратегіям була розроблена та затверджена чергова Стратегія національної безпеки України «Безпека людини – безпека країни» [84]. Розробці цієї стратегії передувало прийняття Закону України «Про національну безпеку України» у 2018 році, що містить визначення поняття стратегії національної безпеки України як документа, що визначає актуальні загрози національній безпеці та відповідні цілі, завдання, механізми захисту національних інтересів, а також є основою для планування і реалізації державної політики у сфері національної безпеки [60, ст. 1]. На погляд вітчизняного законодавця, стратегія у сфері нацбезпеки є документом довгострокового планування [60, абз. 2 ч. 3 ст. 25]. При цьому у абз. 1 ч. 3 ст. 25 Закону України «Про національну безпеку України» установлено, що планування у сферах національної безпеки й оборони поділяється на довгострокове (понад п’ять років), середньострокове (до п’яти років) та короткострокове (до трьох років) [там само]. На жаль, установлення таких термінів для реалізації планування у сфері нацбезпеки суперечить фундаментальним принципам стратегування, за якими короткострокове планування відбувається терміном до 5 років, середньострокове – терміном до 10 років, а довгострокове – терміном понад 10 років. Така підміна понять аж ніяк не сприяє досягненню поставленої мети в стратегії національної безпеки України. На ці аспекти слушно звертають увагу вчені С. Домбровська, С. Крук, О. Крюков, Є. Нікіпєлова, В. Новіков, А. Помаза-Пономаренко, С. Порока та ін. [25; 27; 38; 53–56].

Принагідно відзначимо, що відповідно до ч. 1 ст. 26 Закону України «Про національну безпеку України» стратегія національної безпеки України

має розроблятися за дорученням Президента України протягом 6 місяців після його вступу на пост [60]. У той же час, Стратегія нацбезпеки України була розроблена та схвалена із запізненням, тобто без належного дотримання цієї правової норми. Як відомо, вступ на пост шостого Президента України відбувся 20.05.2019 року (саме тоді відбулась його інагурація), а от стратегія національної безпеки України була затверджена указом Президента України від 14.09.2020 року. Насправді в України та її високопосадовців не було зайвого часу на розкачування та відтягування у прийнятті надважливих управлінських рішень у сфері підтримки національної безпеки. Прагнення держави-агресорки відомі були ще у 2014 році. І на центральному рівні потрібно було належним чином розшифровувати та реагувати на наративи рф [27].

У продовження умовного плану дослідження відзначимо, що чинна Стратегія національної безпеки України (2020 р.) ґрунтується на таких основних засадах, як стримування, стійкість і взаємодія. З одного боку, це ті засадничі принципи, що перегукуються з тими, що були закріплені в Стратегіях національної безпеки України 2007 і 2015 років. Звісно, в останніх стратегіях ці принципи визначені не один в один із чинною стратегією, але сутнісно співпадають. У той же час, зауважимо, що деталізація принципів стримування, стійкості та взаємодії є не зовсім вдалою. Погоджуємось із науковцями, які вказують на важливість корегування положень Стратегії національної безпеки України «Безпека людини – безпека країни», зокрема, у частині визначення приципів забезпечення нацбезпеки [27; 38; 53–56]. Власне, незрозумілим є принцип стійкості, що, на думку нормо творців, означає «здатність суспільства та держави швидко адаптуватися до змін безпекового середовища й підтримувати стале функціонування, зокрема шляхом мінімізації зовнішніх і внутрішніх уразливостей» [84]. Складним для уявлення є процес визначений у Стратегії національної безпеки, згідно з якої вона має ґрунтуватись на категорії ідеального порядку – *здатності* суспільства та держави швидко адаптуватися до змін безпекового

середовища. Подібні протиріччя від самого початку визначення положень архіважливого стратегічного документа дають підстави для висловлення критичного ставлення по відношенню до документа в цілому.

Наступний момент, що зумовлює появу зайвих наукових дискусій, стосується визначення національних інтересів у чинній Стратегії національної безпеки України (2020 р.). Так, у п. 5 цієї стратегії встановлено, що пріоритетами національних інтересів України та забезпечення національної безпеки є:

– відстоювання незалежності та державного суверенітету;

– відновлення територіальної цілісності у межах міжнародно визнаного державного кордону України;

– суспільний розвиток, насамперед розвиток людського капіталу;

– захист прав, свобод і законних інтересів громадян України;

– європейська й євроатлантична інтеграція [84].

Однак те, що визначено національними інтересами у Стратегії нацбезпеки України (2020 р.), відноситься до принципів і цілей політики національної безпеки у Стратегіях національної безпеки України 2007 і 2015 років. Усе це, на наше переконання, засвідчує той факт, що відсутня «інституційна пам’ять» під час розробки документів стратегічного планування у сфері національної безпеки.

Крім того, стратегія нацбезпеки як підзаконний акт не має суперечити Конституції України та іншим законам. У абз. 10 ч. 1 Закону України «Про національну безпеку України» [60] визначено, що національні інтереси є життєво важливими інтересами людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян. Розгляд законодавчого визначення національних інтересів дає підстави стверджувати, що йому певною мірою протирічить визначення національних інтересів у Стратегії національної безпеки України (2020 р.). Йдеться про те, що законодавець задекларував основі національні інтереси, а

нормотворці Стратегії нацбезпеки України відступили від вимог спеціального законодавства, і на власний розсуд трактували, що відноситься до національних інтерсів. Наприклад, європейської й євроатлантичної інтеграції серед національних інтересів немає у Законі України «Про національну безпеку України» [60]. Також у цьому законі акцентується увага на демократичному розвитку, а також на створенні безпечних умов життєдіяльності та забезпеченні добробуту громадян. Однак демократичний розвиток – не синонім суспільного розвитку, це категорії науки політології, соціології, економіки. Зрозуміло, що представники цих галузей науки вкладають різне значення в ці терміноконструкції «демократичний розвиток» і «суспільний розвиток». Вищевказане дає змогу наполягати на узгодженні норм Закону України «Про національну безпеку України» (2018 р.) і Стратегії національної безпеки України (2020 р.) [60; 84]. Цікавим є погляд С. Пороки, який обґрунтовує необхідність прийняття оновленої Стратегії нацбезпеки України саме з урахуванням виваженого визначення національних інтересів як засадничих принципів забезпечення національної безпеки [73]. На нашу думку, формулювання положень Стратегії нацбезпеки України (2020 р.) [84] потрібно здійснювати у зовсім іншому ключі, зокрема, визначити й обгрунтувати механізм реалізації цієї стратегії.

Щодо визначення цифрових технологій у сфері забезпечення національної безпеки в межах аналізованої Стратегії нацбезпеки України (2020 р.) [84], то в ній, на відміну від стратегії 2015 року, наявне згадування таких технологій. Підтвнердженням цього є положення Розділу ІІІ «Основні напрями зовнішньополітичної та внутрішньополітичної діяльності держави для забезпеченя її національних інтересів і безпеки»:

– держава повинна виконувати лише необхідні функції (безпекову, зовнішньополітичну, соціальну та регуляторну);

– Україна має здійснити цифрову трансформацію, забезпечити надання адміністративних послуг через безпечне «єдине вікно» із використанням сучасних інформаційних технологій, поширювати цифрову грамотність;

– основним завданням розвитку системи кібербезпеки є гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації [84, п. 50, п. 51, п. 52].

Уважаємо, що констатація щодо реалізації державою найважливіших функцій є слушною: це покликано забезпечити раціональне використання «портфеля» ресурсів для забезпечення належної суспільної життєдіяльності. Проте дотримання цього принципу на практиці виявляється ускладненим. Стосовно здійснення цифрової трансформації, то принцип «єдиного вікна» упроваджується в Україні і доволі успішно, але не можна беззаперечно стверджувати про досягнення значних позитивних результатів у цій сфері. Для прикладу, розглядаючи звітну інформацію Мінцифри щодо стану вдосконалення роботи центрів надання адміністративних послуг [23], можна виявити, що це вдосконалення стосувалося незначної кількості напрямів, які не зовсім стосуються саме впровадження цифрових технологій. Зокрема, йдеться про облаштування пандусів, але не усувається безбар'єрність у використанні цифрових технологій особами, які мають обмежені фізичні можливості.

Відтак, можемо наполягати на тому, що саме в цьому напрямку потрібно рухатися, щоб забезпечити інклюзивність і включеність населення у процеси державної політики, що можливо зреалізувати за допомогою цифрових технологій. Погоджуємося із твердженням, що «безпека для людини» є підґрунтям «для безпеки, яка виходить із боку суспільства» [8; 69–71]. До речі, чинна правова база України визначає публічні (адміністративні) послуги й інформаційну безпеку як сектори критичної інфраструктури, адже в межах цих секторів забезпечується виконання життєважливих функцій (див. Закон України «Про адміністративні послуги» (2012 р.) і «Про критичну інфраструктуру» (2021 р.) [78; 79].

РОЗДІЛ 3
НАПРЯМИ ВДОСКОНАЛЕННЯ МЕХАНІЗМІВ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ВПЛИВУ ЦИФРОВИХ ТЕХНОЛОГІЙ

3.1. Шляхи розвитку механізмів публічного управління у сфері національної безпеки України в умовах впливу цифрових технологій

На підставі проведеного аналізу стану функціонування механізмів публічного управління у сфері національної безпеки в умовах впливу цифрових технологій можемо відзначити, що Україна може протидіяти інформаційним загрозам, кібервійнам і негативному впливу зазначених технологій. Це можливо зреалізувати в таких напрямках:

1. Удосконалення власної нормативно-правової бази, ураховуючи міжнародні стандарти у сфері стратегічного планування і виваженого використання технологій (зокрема, штучного інтелекту).

2. Розвивати канал дво- і багатостороннього співробітництва із зарубіжними країнами щодо впровадження цифрових технологій.

3. Створювати відповідні організаційні структури або розширювати можливості вже наявних публічних інституцій у сфері національної безпеки з метою протистояння негативному впливу цифрових технологій.

Щодо першого пункту, то вважаємо, що він має передбачати визначення в межах оновленої Стратегії національної безпеки України механізму її реалізації, який включає таке:

1. Опис проблем, які обумовили її прийняття, і нормативно-правових актів, що діють у відповідній сфері.

2. Аналіз поточного стану справ, тенденцій й обґрунтування щодо необхідності розв’язання виявлених проблем.

3. Стратегічні цілі.

4. Завдання, спрямовані на досягнення поставлених цілей, етапи їх виконання, очікувані результати.

5. Етапи реалізації стратегії.

6. Порядок проведення моніторингу, оцінки результатів реалізації стратегії та звітування.

7. Ресурси, необхідні для реалізації стратегії.

8. Операційний план реалізації стратегії.

Крім того, доцільно узгодити положення оновленої Стратегії національної безпеки України (на період до 2030 року) із нормами інших правових актів, насамперед, Законом України «Про національну безпеку України» [60] у частині визначення національних інтересів, а також зовнішніх і внутрішніх загроз у цій сфері.

Стосовно цифрових технологій, то їх вплив на сферу нацбезпеки також важливо конкретизувати в межах оновленої Стратегії національної безпеки України (на період до 2030 року). На наше переконання, допомогти в цьому контексті може врахування положень чинного законодавства у сфері цифровізації. Серед основних нормативно-правових актів можемо виокремити Закон України «Про стимулювання розвитку цифрової економіки в Україні» (2021 р.), постанову Уряду України «Про схвалення Національної економічної стратегії на період до 2030 року» (2021 р.), розпорядження Уряду України «Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів щодо її реалізації» (2021 р.) [60] тощо.

У межах цієї оновленої стратегії слід визначити ефекти застосування цифрових технологій у сфері національної безпеки та їх наслідки, що впливають на трансформацію цієї сфери. У цьому контексті набуває актуальності визначення процесу того, як цифрові технології проникають у сферу забезпечення нацбезпеки та які зміни відбуваються у самій системі безпеки держави. На емпіричному рівні, звужуючи рамку трансформації до елементів змін та наслідків, можна виявити хвилеподібну динаміку взаємодії цифрових технологій зі сферою забезпечення національної безпеки та

обґрунтувати емпіричну модель для вимірювання такої динаміки змін. Окремо можна виділити можливості масштабування емпіричної моделі публічного управління у сфері нацбезпеки, яку можливо застосовувати для аналізу різних типів цифрових технологій.

Спираючись на заявлену проблематизацію, у цьому дослідженні теоретично можливо представити опис процесу того, як цифрові технології (на прикладі технології ШІ) проникають у сферу забезпечення нацбезпеки, а також які зміни відбуваються в самій системі безпеки держави. Результати показують, що відбувається максимізація можливостей системи національної безпеки за рахунок упровадження передових цифрових технологій. Отримані результати демонструють, що держави можуть активно застосовувати напрацювання великих баз даних (у контексті національного та міжнародного масштабів) у сфері безпеки. Таким чином, формується тенденція щодо підпорядкування та сек'юритизації розвитку (development) у сфері забезпечення національної безпеки [25; 27; 282].

Оцінка та сприйняття загроз у контексті цифрових технологій з боку держав нелінійна (див. додатки 2–6), вона має хвилеподібний характер через дію різних зовнішніх і внутрішніх факторів. Динаміка змін у всіх аналізованих моделях країн не однакова, проте має кілька подібних етапів. Так, у звітному періоді стабілізується показник можливостей ШІ, а показник оцінки загроз до цього періоду демонструє стрімке зростання (див. додаток 2). При цьому показник узгодженості (консистентності) безпеки демонструє відмінності серед держав щодо початку проникнення цифрових технологій у сферу забезпечення нацбезпеки, а також загальною динамікою. Поки одні країни активно нарощують потенціал трансформації систем національної безпеки (наприклад, США та Швеція), інші країни демонструють зворотний тренд – посилення побоювань та ризиків таких змін (наприклад, Німеччина та Фінляндія).

На другому рівні проблематизації – в інструментальній (методичній) площині – має бути розроблено, протестовано та валідизовано емпіричну

модель змін та оцінки системи безпеки держави під впливом цифрових технологій (на прикладі технології ШІ). Емпірична модель має оціночний характер і спрямована на формування концепції оцінки системи нацбезпеки (не лише оцінка загроз, а й виявлення можливостей) та створення емпіричного підходу до вимірювання сфери забезпечення безпеки держави. Запропонований підхід дозволяє оцінити динаміку розвитку (еволюції та трансформації) системи нацбезпеки держави під впливом технологій штучного інтелекту.

Спроба «об’єктивного» аналізу динаміки демонструє деякі переваги. По-перше, можемо окремо спостерігати зміни як в офіційних оцінках загроз у сфері нацбезпеки, а також у визначенні можливостей цифрових технології (у контексті публічного сприйняття реалізованих досліджень, апробації та впровадження різних алгоритмічних систем штучного інтелекту). По-друге, можемо з урахуванням окремих часових відрізків аналізувати те, як розвивають цифрові технології, як вони проникають у систему нацбезпеки. Наприклад, стрімкий розвиток технології ШІ у період з 2006 по 2012 рр. у США дозволив цій державі скерувати загальносвітові технологічні перегони, наслідки яких виходять за науково-дослідні та технологічні рамки. По-третє, окремий акцент на оцінці загроз у сфері нацбезпеки дозволяє аналізувати політичне ставлення до цифрових технології, що розширює існуючу дискусію у предметному полі сек'юритизації цих технологій з огляду на їх вплив на сферу безпеки. По-четверте, представлена модель має інтерпретаційну гнучкість, ураховуючи, що зібрані дані представляють різні галузі (соціальна, економічна, політична) і з більшим тимчасовим охопленням. По-п'яте, модель може бути корисною для проведення порівняльних досліджень країн. Наступні дослідження будуть спрямовані на посилення крос-модельного порівняльного аналізу як за єдиним показником узгодженості індикаторів безпеки, так і за окремими індикаторами можливостей ШІ та оцінки відповідних загроз (див. додатки 3, 4).

Особливо відзначимо масштабованість моделі, що передбачає

потенційну можливість щодо заміни технології ШІ на будь-яку іншу цифрову технологію (наприклад, хмарні обчислення, технології зв'язку п'ятого покоління тощо) і формування емпіричної моделі узгодженості (консистентності) нацбезпеки з урахуванням конкретної цифрової технології. Мається на увазі, що сфера нацбезпеки, коефіцієнти якої будуть збережені і для іншого типу цифрової технології, дозволяє простежити динаміку змін системи безпеки держави, але вже щодо конкретного типу технології. Тому дослідження має бути сфокусовано на тестуванні можливостей моделі публічного управління у сфері нацбезпеки та перевірці її інтерпретаційних можливостей, на які впливають цифрові технології.

Уважаємо, що в межах оновленої стратегії нацбезпеки України доречно закріпити два сценарії реалізації заходів щодо забезпечення на належному рівні цієї безпеки – оптимістичного та песимістичного. Щодо першого сценарію, то він передбачає оцінювання загроз, пов'язаних із впливом цифрових технологій на національну безпеку, яке має випереджати наявні рішення щодо протидії таким загрозам. Незважаючи на специфічність, неоднозначність та стрімкість розвитку цифрових технологій, зокрема технології штучного інтелекту, більшість держав встигають як мінімум на інституційному рівні визначати та закріплювати можливості реагування на такі загрози. Іншими словами, можна спостерігати актуалізацію феноменів, коли держава у сфері безпеки на початковому етапі визначає можливості реагування на загрози більш ємно (повно та варіативно), ніж характеризує самі загрози. Однак це поширюється не на всі держави. В аналізованих моделях публічного управління у сфері національної безпеки в умовах впливу цифрових технологій подібне спостерігається у всіх країнах, крім Німеччини. Модель Німеччина є єдиною, де до 2019 року показник оцінки загроз у цій сфері перевищує показник визначення можливостей. Саме тому можемо вказати, що на вітчизняних теренах німецький досвід може враховуватись лише в період після 2019 року, тому що до цього часу модель Німеччини не відповідає повноцінно заявленим прагненням дослідження.

Інтерпретація результату тестування першого варіанту дозволила визначити «ставлення» орагінів влади до змін у сфері нацбезпеки, опосередкованих цифровими технологіями. Держави визначають роль і місце технологій пропорційно їх потенціалу можливостей. Тому органи державної влади успішно інтегрують ці технології, збалансовано оцінюючи пов'язані з ними загрози. Ці технології дозволяють швидше адаптувалися до сучасних змін і конструювали систему безпеки таким чином, що можливості реагування перевершують загрози, що оцінюються. Іншими словами, це не «спонтанна трансформація», не реакція на виклики, а планомірна і стратегічна політична діяльність з оцінки потенціалу можливостей у співвідношенні з загрозами. Можна стверджувати, що у країнах Європи й Україні спостерігається збільшення побоювань у питаннях нацбезпеки, тому актуалізується увага на визнаенні потенціалу загроз у цій сфері [25; 27].

Другий (песимістичний) варіант реалізації публічного управління у сфері національної безпеки також передбачає визначення динаміки розвитку цифрових технологій і їхнього впливу на забезпечення нацбезпеки. У той же час, реагування на загрози, пов'язані із негативним впливом цих технологій, є ускладненим, і має спиртися на організаційний принцип функціонування сучасних сил забезпечення безпеки (у т.ч. максимізація військової сили за рахунок використання технологій). Результати моделей частково спростовують припущення про те, що застосування державами цифрових технологій у сфері безпеки буде відбуватися раніше, ніж у суспільстві з'явиться дискусія про ці типи цифрових технологій. Таким чином, не можна однозначно стверджувати, що у всіх країнах прояви застосування цифрових технологій у сфері забезпечення нацбезпеки виявились раніше за суспільну/ публічну дискусію. Незважаючи на те, що моделі США та Швеції підтверджують цю тезу, такі результати не поширюються на всі країни. Можливий пояснювальний механізм такого несподіваного результату (песимістичного), за якого максимізація технологічного потенціалу у сфері нацбезпеки відбувається раніше, ніж починається формування механізмів

публічного управління, проте важливо в цьому плані опертивно скористатись технологіями штучного інтелекту, перед тим, як вони будуть використані з військовою метою, хочай й розроблялися як цивільні/комерційні рішення.

На жаль, неоднозначність результату (щодо моделей двох сценаріїв розвитку подій) не дозволяє нам однозначно стверджувати, що держави прагнуть максимізації потужності та безпеки за рахунок цифрових технологій. Потенційним поясненням такого розмаїття в моделях публічного управління в реагуванні на негативний вплив цифрових технологій і в рівнях країн (див. підрозділ 2.1) може бути визнана та обставина, що частина держав побоюються загроз і ризиків у цій сфері сильніше, ніж бачать потенціал для застосування зазначених технологій. Відтак, країни намагатимуться спочатку отримати доказову базу переваг, а лише потім починати впроваджувати та застосовувати цифрові технології. Їх різноманіття може пояснюватись існуючими можливостями технологічного розвитку (development) та потенціалом людського капіталу (наявністю або відсутністю висококваліфікованих кадрів для впровадження технологій) [25; 27; 282].

Запропоновані варіанти розвитку подій щодо порівняльного аналізу показників сприйняття загроз і типу цифрових технологій конструювалися навколо консенсусу про те, що та сама загроза може по-різному сприйматися державою, а тому різним буде механізм реагування на неї. При цьому слід розуміти, що стосовно цифрових технологій існує сильна невизначеність, яка формує побоювання серед теретиків і практиків публічного управління. Результати аналізу наукових напрацювань показують, що в різні періоди навіть у межах однієї країни показник впливу цифрових технологій на сферу нацбезпеки може коливатися. Отже, сприйняття та реагування на загрози в цій сфері державами не може бути лінійним. Зазначене підтверджує існуюче обмеження сфери забезпечення нацбезпеки, що кожна держава по-різному визначає й оцінює загрози. Ми не просто підтверджуємо існуючий консенсус щодо відмінностей у визначенні й оцінці загроз, а й уточнюємо його безпосередньо крізь призму контексту використання цифрових технологій.

Більше того, можна спостерігати, що по-різному визначаються й оцінюються одні й ті ж загрози щодо різних часових періодів. Причому зазначене свідчить, що з часом сприйняття однієї й тієї загрози має «знижуватися».

Таким чином, виявлення відмінностей в оцінці загроз підтверджує теоретичне припущення, що емпірично існують відмінності серед держав в оцінці та сприйнятті загроз, пов'язаних з розвитком цифрових технологій. Це дозволяє виявити певну специфіку щодо цифрових технологій, що розширює дискусію про трансформаційний ефект цифрових технологій. На цій підставі можна продемонструвати, що такі перетворення не є лінійними. Держави адаптуються до загроз у сфері цифровізації та її трансформації, а також намагаються пропорційно оцінювати потенціал їхнього впливу на найважливіші сфери суспільної життєдіяльності. У свою чергу, цифрові технології виступають і як інструмент (що зміцнює зміни), і як сам фактор, що підвищує рівень національної безпеки. Це важливий результат, який дозволяє, при розширеній інтерпретації, стверджувати, що цифрова трансформація може бути пов'язаною не лише з позитивними змінами, а й з появою обґрунтованих побоювань [17].

Гіпотеза щодо досягнення максимальних показників емпіричної моделі публічного управління у сфер національної безпеки в умовах впливу цифрових технологій ґрунтується на логіці готовності держав до ризиків та викликів із боку цифрових технологій. За наслідками аналізу гіпотеза підтверджується частково. У цьому контексті можливо спостерігати у всіх моделях пубічного управління у сфері нацбезпеки приблизно однаковий тренд, а саме: показник можливостей ШІ вирівнюється та стабілізується на одному рівні протягом кількох років, що означає, що органи держави починають практичне застосування технології з пропорційним розумінням можливостей і меж застосовності. У свою чергу, показник оцінки загроз у сфері цифрових технологій може отримати стрімке зростання, що може свідчити про високу оцінку ризиків і загроз з боку держави, коли реципієнти починають отримувати все більше інформації та знань про вплив цифрових

технологій, а також супутніх ризиків. У певний період показник узгодженості безпеки може демонструвати зростанн, із приблизно схожою поступальною динамікою зростання та різким стрибком у інші періоди, оскільки в цей час, по-перше, держави можуть спостерігати, по суті, реальні наслідки застосування цифрових технологій, а по-друге, реалізовути посилення політизації та сек'юритизації цифрових технологій [18].

Отримані результати не завжди можуть відображати попередньо визначені очікувані результати. Вони різні для України, США та Швеції, відповідно для яких притаманна практика щодо застосування підходу, за якого головними суб’єктами в забезпеченні нацбезпеки під впливом цифрових технологій є уряд. Однак така практика відсутня в Німеччині, що зумовлено рішенням щодо її децентралізації з метою формування потужних федеральних земель, а не центрального рівня. У всіх аналізованих країнах показник можливостей технології штучного інтелекту досягає схожого максимального значення останніми роками, чого не скажеш по відношенню до України. Більше того, на неї цифрові технології чинять усе більше негативний вплив, чому сприяє рф. Відтак, набуває актуальності розробка показника узгодженості національної безпеки з рівнем розвитку цифрових технологій. Його динаміка є хвилеподібною й досить унікальною для кожної країни, за винятком США та Швеції. Всупереч теоретичним очікуванням, різкий стрибок показника узгодженості безпеки в 2016-2017 р. в Україні, також спостерігається в інших країнах (зокрема, у Франції). У цей період в інших країнах світу спостерігався спад показника узгодженості безпеки через зростання ризиків щодо застосування цифрових технологій, їх сек’юритизації технології й поступальною (не постпішальною) легітимізацією суспільством самого факту використання ШІ в бік інформаційного обмеження (секретності) [17].

Зважаючи на це, видається можливим надання відповіді на заявлене основне дослідницьке питання щодо динаміки застосування цифрових технологій органами державної влади у сфері забезпечення національної

безпеки двома основними тезами. По-перше, динаміка застосування механізмів публічного управління в цій сфері є нелінійною, а хвилеподібною і відбиває як національні особливості концептуалізації національної безпеки, так і внутрішню специфіку відносин держав до конкретного типу цифрових технологій. Незважаючи на певні побоювання, уряди країн встигають пропорційно внутрішнім особливостям системи безпеки оцінювати ризики та вигоди від використання цифрових технологій, і на підставі такої оцінки працювати над їх упровадженням. Іншими словами, результати демонструють, що у країнах відсутні як «алармістські» побоювання, так і поблажливість до питань технологічних змін у системі національної безпеки. По-друге, у країнах присутні загальні тренди як у часовій площині (наприклад, схожі терміни прийняття національних стратегій і програм зі штучного інтелекту), так і за кінцевою динамікою визначення можливостей технології штучного інтелекту – наближення до максимальних значень. Це може свідчити або про результативне функціонування системи міжнародного співробітництва як у сфері національної безпеки, так і у сфері цифрових технологій, або про розвиток та посилення конкуренції між країнами щодо розробки та продажу технології штучного інтелекту. Розуміння реального механізму реагування й управління в цій сфері, швидше за все, вимагає об’єднання зазначених варіантів: країни продовжують напрацьовувати міжнародне співробітництво та нарощувати власний технологічний потенціал, але конкуренція між ними посилюється.

У свою чергу, порівняльний аналіз дозволяє виявити як подібності в застосуванні механізму реагування й управліня в цій сфері, так і унікальні ознаки для відповіді на додаткове дослідницьке питання. Власне, апробація емпіричної моделі оцінювання системи національної безпеки держави на основі виміру узгодженості цієї безпеки з інноваційним розвитком країни продемонструвала деякі обмеження. Слід зазначити, що сама логіка узгодженості безпеки демонструє, що чим меншим є показник, тим більш «узгодженою» буде система безпеки держави. Іншими словами, виходячи з

логіки дослідження (ураховуючи індикатор можливостей ШІ та індикатор загроз), можна відзначити, що чим більше у держави можливостей і чим більше вона визначає для себе загроз, тим вищою є ймовірність того, що показник узгодженості системи безпеки з інноваційним розвитком буде дорівнювати нульовому значенню [282]. Однак на рівні інтерпретації й аргументації необхідно враховувати складнощі з оцінкою загроз, пов'язаних з інноваційним розвитком у сфері цифрових технологій. Наприклад, держава може просто «не бачити» загрозу (навмисне чи випадково), але остання існуватиме реально. Навпаки, держава може зайво політизувати та сек'юритизувати цілі сектори безпеки (й акторів у цих секторах), у результаті модель публічного управління демонструватиме високий індикатор оцінки загроз у сфері цифрових технологій, але фактично ці загрози не матимуть реального втілення. У свою чергу, аналогічні флуктуації можуть відбуватися і з індикатором можливостей ШІ (коли держава перебільшує його можливості). Також значним обмеженням може бути відсутність необхідної інформації. Окремо слід зазначити, що зараз складно говорити про існування порогових значень у рівні впливу цифрових технологій на сферу національної безпеки, які були б оптимальними для показника узгодженості цієї безпеки з впливом зазначених технологій [18].

Запропонована модель публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні не розглядає цілеспрямовано військові програми щодо використання технологій ШІ, у тому числі через те, що відомості про такі програми мають закритий характер (наприклад, для отримання та (або) збереження переваги в реальному чи потенційному конфлікті з рф). Будь-яка модель публічного управління, зокрема претендує на відображення складності реального світу, – це неминуче спрощення реальності. Використані у запропонованій моделі публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні параметри описують не тільки реальність афктичний стан справ, скільки її відображення (і розуміння), елементи якого

містяться в офіційних документах (чинній Стратегії національної безпеки України (2020 р.), Стратегії інформаційної безпеки України (2021 р.) [60; 84]).

Окремо слід вказати на обмеження масштабованості та генералізації результат моделі публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні. По-перше, результати дослідження стосуються насамперед оптимістичного сценарію реалізації публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні. При цьому підкреслюється, що результати перспектив упровадження пропонованої моделі небезпечно поширювати з огляду на зацікавленість держави-агресорки. Отримані результати можна співвідносити з країнами зі схожою зміною інститутів та політичних процесів. Допустимо використовувати результати як певне узагальнення для країн, які мають однакову інституційну основу як у питаннях безпеки, так і на рівні процесу прийняття управлінських рішень. Проте, результати не можна генералізувати на велику вибірку країн. Безумовно, результати не поширюються на державу-агресорку, а також на держави з менш якісними інститутами (як на рівні режимних відмінностей, так і у питаннях національної безпеки). При генералізації та масштабуванні результатів рекомендується коригувати модель публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні для забезпечення однаковості підходу, що застосовується в міжнародних безпекових інституціях. По-друге, дослідження орієнтоване на інноваційні країни, тому результати можуть стосуватися лише розвинених щодо цифрових технологій держав.

У вибірці країн для побудови моделі є блокові (тобто країни-члени НАТО, ЄС). У зв’язку з цим для повноцінного та системного аналізу необхідно враховувати як нормативно-правові акти національного рівня України, так і наднаціонального рівня. У цьому конкретному дослідженні було визначено необхідність виявлення й аналізу безпосередньо внутрішніх змін у системі публічного управління у сфері національної безпеки в умовах

впливу цифрових технологій в Україні. При цьому ми прагнули досягти порівнянності моделей публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні і за кордоном (на рівні критеріїв, що застосовувались під час мережевого та регресійного аналізу). Зважаючи на це, виявлено, що у переважній більшості аналізу підлягали саме національні нормативно-правові акти у сфері національної безпеки та розвитку цифрових технологій. Зазначене формує ще одне обмеження цього дослідження, яке можна подолати у майбутньому (у післявоєнний період): результати аналізу стосуються безпосередньо внутрішньої політики держави у питаннях національної безпеки та впливу на неї цифрових технологій. Облік наднаціональних і міждержавних нормативно-правових актів дозволить розширити отримані результати та можливі у подальших дослідженнях.

Самостійним обмеженням може бути концептуалізація та операціоналізація технологій штучного інтелекту. Незважаючи на те, що в дослідженні наведено вичерпний аналіз системного та синергетичного підходів до розуміння публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні, розвиток технології ШІ продовжується. З огляду на це, відзначимо, що концептуалізація напрямків розвитку публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні може коригуватися у відповідності до вимог часу та суспільства. Більше того, сама сфера національної безпеки може внести корективи у визначення того, які цифрові технології будуть відноситися до ШІ, які обмеження та межі застосування на них поширюються тощо. Адже ШІ – це ніщо інше, як система «запит – відповідь».

Отже, виходячи з цілей і завдань дослідження, нами сформульовані два варіанти розвитку механізмів публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні.

Перший варіант формулюється щодо моделювання процесу застосування цифрових технологій у сфері нацбезпеки. Виходячи з логіки

емпіричної моделі (співвідношення показника оцінки загроз у сфері розвитку цифрових технологій і цифрових можливостей реакції на такі загрози), можна припустити, що за оптимістичного сценарію модель публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні показник загроз не перевищуватиме показник можливостей реагування на них. Обґрунтуванням є специфічність цифрових технологій, неоднозначність їх застосування та стрімкість розвитку. Проте за оптимістичного сценарію аналіз й оцінювання загроз від цифрових технологій («традиційних» загроз, а неи гібридних) має випереджати наявні управлінські рішення щодо протидії цим загрозам. Тестування гіпотези щодо оптимістичного сценарію дозволить виявити вектори державної політики до змін у сфері національної безпеки, опосередкованих цифровими технологіями. Конкретизуючий механізм дозволить уявити, як держава та її апарат визначають роль і місце цифрових технологій (оцінка загроз дозволить продемонструвати побоювання держав, а також потенціал можливостей – те, як держава та її апарат здатні реагувати на загрози, пов’язані з розвитком цифрових технологій). Що стосується підтвердження гіпотези песимістичного сценарію, то можемо стверджувати, що спостерігаємо збільшення побоювань у питаннях національної безпеки та впливу на неї цифрових технологій. Органи влади все більше уваги звертають на потенціал загроз у сфері розвитку цифрових технологій (як безпосередньо з боку цифрових технологій, так і в питаннях, де технології мають бути інструментом усунення загроз). У разі спростування гіпотези песимістичного сценарію, навпаки, органи влади успішно інтегрують цифрові технології, збалансовано оцінюючи загрози та вчасно реагуючи на них. У такому випадку можна буквально продемонструвати, що держава та її апарат адаптувалися до сучасних змін і сконструювали систему національної безпеки таким чином, що можливості реагування перевершують загрози, що оцінюються [17; 18]. Більш конкретно, гіпотеза може бути сформульована таким чином:

1. Оцінка загроз розвитку цифрових технологій і їх впливу випереджатиме можливості реагування на загрози

Тимчасове охоплення емпіричної моделі публічного управління у сфері національної безпеки в умовах впливу цифрових технологій дозволяє сформулювати гіпотезу в термінах динаміки змін. Організаційний принцип сучасних сил забезпечення безпеки (збройних сил, правоохоронних органів, спеціальних служб тощо) виявляється у максимізації військової могутності за рахунок використання цифрових технологій. Відповідно, логічно припустити, що застосування державними органами цифрових технологій у сфері забезпечення нацбезпеки матиме місце раніше, ніж у суспільстві розпочнеться змістовна дискусія щодо цих типів цифрових технологій. Органи державної влади, якщо вони дійсно прагнуть максимізації можливостей у сфері забезпечення нацбезпеки, повинні починати розробляти та приймати управлінські рішення та впроваджувати технології швидше і раніше, ніж суспільство буде включено до зазначеної дискусії. Основна публічна дискусія щодо застосування технології штучного інтелекту у сфері забезпечення безпеки розпочалася приблизно з 2010 р. у формі обговорення побоювань, пов’язаних з витоком персональних даних або неналежного їх використання. Перевірка гіпотези надасть не лише розуміння динаміки, а й дозволить оцінити «включеність» органів державної влади у потенціал технологічної зміни системи нацбезпеки. Іншими словами, можливо виявити те, наскільки проактивно діють органи влади: наскільки вони прагнуть залучати та застосовувати цифрові технології (з огляду на тривалість технологічного циклу з моменту прийняття управлінських рішень до безпосередньої практичної реалізації) з випереджаючими темпами до того, як суспільство зверне увагу на суттєві ризики та можливості впровадження цифрові технології (зокрема, ШІ). У разі підтвердження гіпотези можливо стверджувати, що державні органи справді прагнуть максимізації потужності та безпеки за рахунок цифрових технологій. Тобто зміни, що спостерігаються (наприклад, цифрова трансформація) мають бути підтримані і навіть

ініційовані органами державної влади центрального рівня. Однак, якщо гіпотеза буде спростована, то може існувати кілька механізмів пояснення. Основний механізм полягатиме в тому, що держава та її апарат побоюються загроз і ризиків сильніше, ніж бачать потенціал для застосування цифрових технологій. Тому органи влади мають прагнути спочатку отримати доказову базу умовних переваг від розвитку цифрових технологій, а лише потім починати впроваджувати та застосовувати ці технології. Альтернативним поясненням може бути перерозподіл фокусу органів влади, тобто максимізація може і відбувається, але за рахунок інших цифрових технологій чи за рахунок інших стратегій і тактик. Таким чином, другий варіант розвитку механізмів публічного управління передбачає, що дослідження може бути сформульований таким чином:

2. Динаміка застосування цифрових технологій у сфері забезпечення національної безпеки та системі публічного управління

Другий варіант розвитку механізмів публічного управління у сфері національної безпеки в умовах впливу цифрових технологій формулюється щодо порівняльного аналізу моделей реалізації цих механізмів (стійкої моделі до загроз; чутливої моделі до загроз тощо). У дослідженнях національної безпеки є консенсус щодо того, що різні держави (та їх уряди) не оцінюють загрози однаково. Одна й та ж загроза у сфері розвитку цифрових технологій може по-різному оцінюватись та інтерпретуватися державами. Незважаючи на те, що основна робота з даної тематики (дослідження Волферса) відноситься до «традиційних» підходів до національної безпеки і може вважатися «застарілою», але питання невизначеності загроз є дуже актуальним. Незважаючи на існуючі дискусії про правильне та належне розуміння нацбезпеки, сприйняття загроз (і його зміст) – це і наукова, і практична проблема. Іншими словами, у цій гіпотезі варто спиратиося на змістовну складову доказу про те, що держави по-різному визначають й оцінюють загрози системи безпеки. Емпірична модель даного дослідження дозволяє аналізувати оцінку та сприйняття загроз

кожною державою окремо й оцінити таке сприйняття. Однак, незважаючи на відмінності в оцінці загроз системі національної безпеки, навколо цифрових технологій існує невизначеність у сфері такої безпеки, що формує зайві побоювання. Тому варто допускати, що в країнах, які аналізуються (й у т.ч. в Україні), оцінки загроз не будуть однорідними, і цим оцінкам будуть притаманні підвищені побоювання. Тестуючи цю гіпотезу, варто прагнути виявити існування невизначеності щодо оцінки загроз, ускладнену специфікою цифрових технологій у сфері нацбезпеки. З одного боку, виявлення відмінностей в оцінці загроз у сфері нацбезпеки підтвердить теоретичне припущення, що емпірично існує, про відмінності серед держав в оцінці та сприйнятті загроз. З іншого боку, це дозволить продемонструвати, чи існує специфіка щодо цифрових технологій у сфері нацбезпеки. У разі підтвердження гіпотези можливо буде спростувати теоретичне уявлення про невизначеність в оцінці загроз і продемонструвати ставлення держав до цифрових технології. Це значно розширить дискусію про трансформаційний ефект цифрових технологій. Якщо ж гіпотеза буде спростована, можна буде підтвердити існуючу теорію про невизначеність оцінки загроз, а також продемонструвати, що ставлення органів державної влади до цифрових технологій не відрізняється від будь-яких інших феноменів тощо.

3. Сприйняття загроз і типів загроз, пов'язаних із впливом цифрових технологій, досягатиме максимальних значень

У свою чергу, порівняльний аналіз також дозволить протестувати припущення про високу готовність держав до ризиків та викликів з боку цифрових технологій. Можна допустити, що у всіх аналізованих країнах, як лідерах у сфері інформаційних технологій, спостерігатимуться високі значення показників емпіричної моделі публічного управління у сфері забезпечення національної безпеки, що свідчить про те, що держави (1) високо оцінюють ризики та загрози з боку цифрових технологій, а також (2) стрімко впроваджують цифрові технології у сферу забезпечення безпеки для протидії сучасним викликам, пов'язаним із розвитком цих технологій. При

тестуванні гіпотези щодо оптимістичного варіанту розвитку механізмів публічного управління у сфері нацбезпеки стане можливо стверджувати про існування цифрових перетворень. Стрімкість упровадження цифрових технологій, а також висока оцінка ризиків та викликів у цій сфері демонструють адаптивність та готовність урядів до сучасних викликів безпеки, пов'язаних із цифровізацією.

Отже, у роботі пропонуються шляхи розвитку правового, організаційного, інформаційного та ресурсного механізмів публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні в межах насамперед оптимістичного сценарію. У цьому контексті, по-перше, наполягається на розвитку правового механізму публічного управління в цій сфері шляхом удосконалення чинної Стратегії національної безпеки в напрямку доповнення її положеннями щодо ролі цифрових технологій у системі публічного управління. По-друге, обґрунтовано розвиток організаційного механізму публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні за рахунок виваженого впровадження технологій штучного інтелекту та діджиталізації діяльності сектору безпеки й оборони. На цій підставі уточнено індикатор можливостей штучного інтелекту й індикатор оцінки загроз у цій сфері. По-третє, обґрунтовано, що ресурсний механізм публічного управління у сфері нацбезпеки вимагає актуалізації хмарних рішень і послуг у сфері публічного управління в цій сфері, а також розвитку конвергентних систем на заміну традиційних сховищ даних у цій сфері. Крім того, у роботі рекомендовано підвищувати результативність інформаційного механізму публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні за рахунок розвитку цифрового суспільства. Адже воно повсюдно застосовує мобільні додатки й інтерактивні платформи, і повинно отримувати об'єктивну інформацію та високоякісні послуги з метою формування системи безпеки, що виходить і від населення також (у формі вдоволення/невдоволення).

3.2. Підходи до вдосконалення системи публічного управління у сфері національної безпеки України в умовах впливу цифрових технологій

Сучасний стан функціонування системи публічного управління у сфері національної безпеки України в умовах впливу цифрових технологій охарактеризовано, як незадовільний. Причини цього мають різний масштаб поширення та джерело походження. Відтак, визначення підходів до вдосконалення системи публічного управління в означеній сфері має враховувати дану причинно-наслідкову обставину. Вона зумовлює необхідність визначення одним із ключових векторів удосконалення системи публічного управління в означеній сфері оновлення Стратегії національної безпеки України, що (стратегія) має враховувати тенденцію до негативного застосування цифрових технологій з метою зниження рівня безпеки в державі.

З огляду на це можемо відзначити, що вдосконалення системи публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні має відбуватись із застосуванням системного та синегретичного підходів. Дана гіпотеза висловлена через стрімкий і складно прогнозований розвиток цифрових технологій, що може так само неочікувано впливати на систему публічного управління. Її вдосконалення також передбачає модернізацію інституційного й організаційного забезпечення цієї системи з позиції систематизованих типів цифрових технологій, пов’язаних із ними ризиків і соціально-політичних ефектів цифровізації. Серед цих ефектів особливе місце може бути відведено ефектам технології великих даних (big data), що становлять цінність і для приватного сектору, і для державного сектору через масштаби впливу на ці сектори загалом і на сферу забезпечення національної безпеки зокрема. Крім того, удосконалення системи публічного управління у сфері нацбезпеки має

усунути цифрові бар'єри для того, щоб підвищити рівень цифрової довіри населення до діяльності органів публічної влади. Останнє вимагає забезпечення балансу між конфіденційністю персональної інформації та розвитком системи національної безпеки. Без довіри населення не буду забезпечено національну безпеку на високому рівні, адже населення не буде визнавати загальнодержавної ідеології, дотримуватись її, і, більше того, виявляти невдоволення, непокору, хаос, апатію тощо. Усе це становить загрозу для системи безпеки із середини, і цим не має скористатись ворог. У цьому контексті можемо відзначити, що потрібно в оновленій Стратегії національної безпеки України передбачити методику оцінювання та ранжування ризиків у цій сфері з позиції визначення серед них місця цифрових технологій (рис. 3.1).

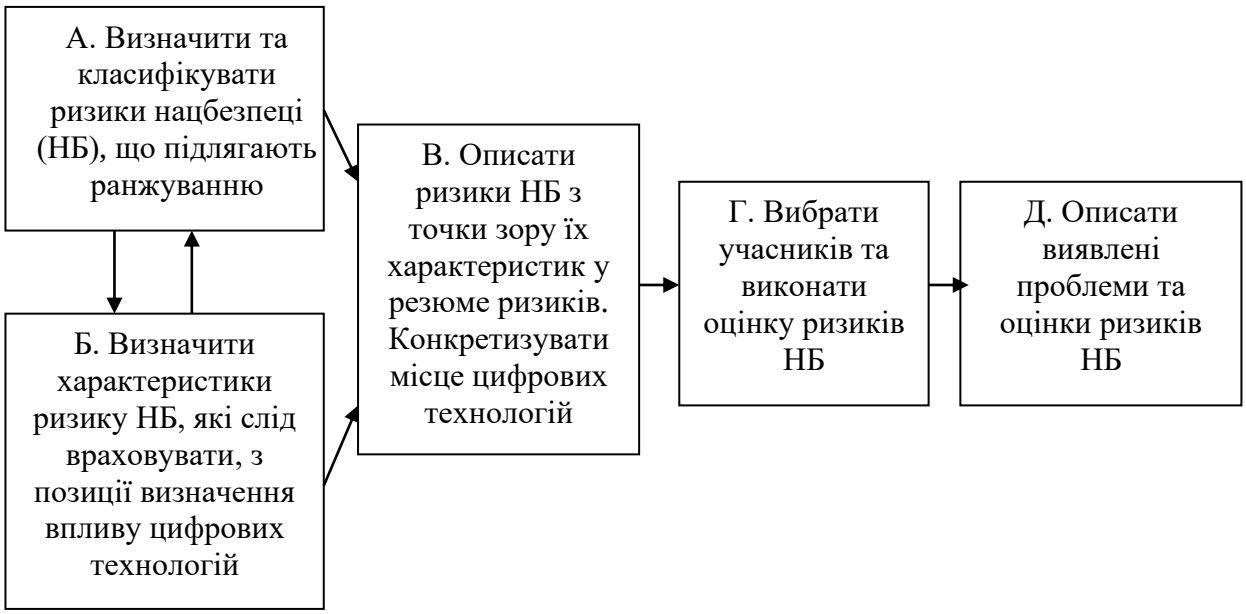

Рис. 3.1. Етапи деліберативного (дорадчого) методу ранжування ризиків національної безпеки в умовах впливу цифрових технологій

Джерело: авторська розробка

Аналіз усіх стратегій національної безпеки України (починаючи з першої) дозволив виявити низку проблем інституційного й організаційного характеру, що з часом не вирішувались, а навпаки кристалізувались. Більше

того, складності ситуації додає те, що цьому спряло неврахування особливостей синергетичного підходу. Відсутність інституційної пам’яті та підлаштування під вплив зовнішніх факторів зумовили те, що в Україні не було Стратегії національної безпеки, у якій би із року в рік дотримувались одного вектора зовнішньої та внутрішньої безпекової політики, загрози визнавали загрозами, а не напрямками тощо. Якби така була виваженість і системність, то Україна була би більш готовою до сучасних гібридних викликів, що трансформуються в небезпеки, серед яких особливе місце займають цифрові технології.

Слід відзначити, що деліберативний метод ранжування ризиків у сфері національної безпеки включає п’ять етапів (див. рис. 3.1). Перші два етапи дозволяють концептуалізувати ризик як такий, одночасно визначаючи, які ризики нацбезпеки варто ранжувати та які характеристики слід використовувати для опису цих ризиків. Потім ризики національній безпеці оцінюються з точки зору виявлених ознак безпековості / загрозливості й визначаються в зведених таблицях ризиків, які відображають найкращу практику передачі інформації про ризики, що можуть становити загрозу для сфери безпеки. Ці таблиці, що резюмують ризики нацбезпеки, використовуються для інформування цільових груп, яким вони скеровуються для розробки ранжування ризиків. На завершальному етапі по суті здійснюється ситуаційний аналіз із застосуванням методів Delphi та stakeholders engagement, що дозволяє виявляти відповідні проблеми з отриманих рейтингів. Деліберативний метод рекомендовано застосовувати з огляду на те, що в наявних Стратегіях національної безпеки України відбувалась підміна понять у визначенні викликів, загроз і небезпек у сфері нацбезпеки [81–84].

У продовження відзначимо, що мета деліберативного методу ранжування ризиків нацбезпеки полягає в тому, щоб надати обґрунтовану оцінку наявних ризиків, що можуть становити небезпеку. У цьому контексті кілька етапів цього процесу є корисними, з точки зору інформування про

характеристики, які визначають ризики та загрози для національної безпеки.

Зазначений підхід представляє інтерес при аналізі процесу відбору ризиків та загроз, а також формування їх класифікації. Деліберативний метод іноді порівнюється з національним репрезентативним оглдяами, і тому використовується у різних методологічних варіаціях для збору даних. Обидві варіації порівнюють набір ризиків країни загалом, а не ризик окремого респондента. Крім того, використовуються ті самі оцінки основних ризиків нацбезпеці для інформування учасників, щоб всі вони розглядали узгоджений набір ризиків у рамках єдиної структури [38]. Наразі ідея про широке залучення експертів до процесу прийняття управлінських рішень з позиції збільшення негативних ризиків має місце на існування, особливо якщо це експерти є безпековими аналітиками. У той же час, під час проведення відповідних консультацій і ситуаційних аналізів у групах часто залучаються співробітники самих органів державної влади, що може як підвищувати, так і знижувати об’єктивність оцінки [там само]. Відтак, потрібно говорити про обмеження даного методу стосовно оцінки ризиків нацбезпеки (за необхідності), тому що подекуди виправданим є використання моделі Zero Trust (нульової довіри) у системах безпеки. Провідну роль відіграють експерти та співробітники органів державної влади, які, ґрунтуючись на власному досвіді, приймають рішення про наявність або відсутність ризику та його можливий розвиток.

На цій підставі можемо вказати, що, окрім синергетичного підходу, потрібно застосовувати системний під час вирішення проблем, пов’язаних з оцінюванням ризиків. Системний підхід передбачає застосування верифікаційного кількісного методу дослідження, які ґрунтуються на історичному, компаративному та іншому аналізі, необхідному для наукового прогнозування векторів забезпечення національної безпеки держави, у тому числі обґрунтовуючи необхідність побудови технократичної системи оцінки її ризиків для запобігання «колапсу держави». Наприклад, за допомогою статичного закону розподілу аналізується структура терористичних актів із

використанням цифрових технологій або надається ширша добірка випадків використання емпіричних методів для подібних досліджень, де історичний аналіз використовується для прогнозування ризиків системи безпеки. При цьому використовуються різні засоби формування підсумкової позиції щодо оцінки ризиків національної безпеки, зокрема, методика NRA (National Risk Assessment). Вона охоплює використання логарифмічної структурованої діаграми ризиків (risk diagram) на основі агрегованої оцінки впливу (aggregated impact). На окрему увагу заслуговує застосування індикативних методів до оцінки ефективності публічного управління, де вже безпосередньо заявлено про необхідність нової, інструментальної парадигми такого управління як «датазалежного» і «цифрозалежного» процесу прийняття рішень [282]. Розглядаючи способи вибору індексів, індикаторів і показників різного рівня оцінок у зазначеній сфері, можемо вказати, що статичні інструменти є необхідними для формування інструментальної парадигми оцінки публічного управління. Зокрема, ця методика може бути використана стосовно сфери національної безпеки з урахуванням можливості виникнення непередбачених ризиків та загроз через вплив цифрових технологій, які можуть розвиватися в рамках уже існуючих трендів. Під впливом пандемії COVID-19 з'явилися окремі тренди використання цифрових технологій у різних сферах суспільної життєдіяльності [66].

Інтерес урядів до збирання, поширення й інтерпретації інформації сприяє появі цілої «індустрії індикаторів», призначеної для фільтрації даних у політичній системі. Чимало органів влади використовують інформаційні та цифрові технології для «запобіжного» управління для відстеження показників у режимі реального часу, у тому числі для моніторингу складних кризових ситуацій як пандемія COVID-19, збройний конфлікт тощо. Подібна підвищена увага до прийняття управлінських рішень на основі даних ставить важливі питання про здатність уряду реагувати на нову та часто суперечливу інформацію та вплив цифрових технологій. Це, у свою

чергу, може викликати активізацію «режиму ручного управління», що не повинен мати систематичного характеру, інакше буде нівелюватись демократичний режим у державі [69].

Різкий стрибок у появі нових цифрових технологій та інновацій призвів до того, що в рамках системно-логічного аналізу з'явилася група досліджень щодо використання «запобіжних» механізмів у прогнозуванні ризиків нацбезпеці та нових інноваційних технологій. Наприклад, випереджальне управління розуміється як можливість розширеної дискусії навколо нових, заснованих на знаннях цифрових технологій (knowledge-based technologies), або як розробка сценаріїв розвитку науково-технологічного прогресу, що згодом «апробуються» у фокус-групах з респондентами [135]. Тим не менш, існує певний перетин цієї групи досліджень з окремими елементами деліберативного аналізу, який є основним підходом у даному випадку, і знаходить опосередковане відображення, наприклад, через використання механізмів Public Engagement [там само]. У цьому плані цікавими видаються концепції «адаптивного» управління та «запобіжної» демократії [28; 38; 69], у межах яких здійснюються спроби розширення підходів до оцінки ризиків в рамках єдиної системи публічного управління. «Адаптивне» управління визнає, що хоча люди в основному є раціональними соціальними акторами, їх знання недосконалі, нерівномірно розподілені, і вони застосовують різні критерії оцінки різних інституційних умов залежно від комунікацій чи прозорості. Допомогти забезпечити «об'єктивність» управління може виважене застосування новітніх технологій. «Адаптивне» управління ґрунтується на системному підході, на відміну від «рефлексивних» підходів щодо технологічних переходів та концепції залежності від попереднього розвитку (Path Dependence) [270; 271].

«Випереджальне» публічне управління (або «проактивне») є теорією, яка використовує підходи з гнучкою структурою прийняття рішень на основі різних проекцій майбутнього, щоб підготуватися до змін та

скоригувати рішення у бік мінімізації загроз [28, 38; 53–56]. У даному випадку «випереджальне» публічне управління розглядається як система інститутів, правил і норм, які дозволяють використовувати прогноз із метою зниження ризиків та підвищення здатності реагувати на події на ранніх, а не пізніх стадіях їх розвитку [28, 38; 53–56]. Рекомендуються гнучкі дії, які можна розбити на модулі (блоки) і реалізувати в міру необхідності залежно від ступеня розвитку майбутнього [там само]. Показники та індикатори змін пропонується відстежувати на систематичній основі, а рішення щодо реалізації «запобіжних» стратегій і заходів адаптації слід розглядати у світлі реальних тенденцій [там само]. Також пропонується використовувати модель «дорадчої» демократії, а також теорії поля та теорії складності, фокусуючись на нарощуванні потенціалу для реагування на непередбачувані або важко передбачувані виклики шляхом розробки індикаторів і показників ефективності для «випереджального» визначення ризиків [там само]. «Випереджальна» публічне управління передбачає більш активну участь громадськості у формуванні майбутнього, використовуючи форсайт і підхід «бажаного майбутнього» [там само]. Даний підхід спрямований на прогнозування сценаріїв майбутнього та використання їх для покращення бачення та створення кращої реальності.

Таким чином, «випереджальне» публічне управління в сучасному стані є всією інституційною системою управління, тоді як історично перші підходи до управління в рамках «адаптивних» теорій були зосереджені лише на окремих аспектах або лише на одній системі ресурсів. Сучасне «випереджальне» публічне управління особливо застосовується до глобальних системних проблем таких, як боротьба зі злочинністю, проявами тероризму, реагування на збройну агресію, з урахуванням тисяч місцевих проблем. Більше того, такий вид публічного управління розширився за своїм змістом, і включає соціальний та антропологічний контекст [28, 38; 53–56], оскільки має справу зі складними людськими взаємодіями, які раніше розглядалися як перешкоди на шляху реалізації адаптивного публічного

управління. Ці перешкоди носять скоріше інституційний, ніж технічний характер, оскільки інститути будуються на основних передумовах і переконаннях, законах, політиці та нормах поведінки, що глибоко укорінилися в соціально-економічних системах, на які все більше впливають цифрові технології, ставлячи таким чином публічне управління у відповідну залежність.

Останнім часом стосовно проблеми оцінювання ризиків національної безпеки, зокрема, пов’язаних з розвитком цифрових технологій, з’являються підходи в рамках системно-логічного аналізу військових стратегій та інших джерел про використання окремих «випереджальних» елементів оцінки ризиків, які за своєю природою розуміються як гібридні, тобто такі, що поєднують штучне та природне походження [53–56; 270; 271]. У цих публікаціях поки немає чіткого розмежування між оцінками ризиків національної безпеки та стратегічним плануванням, але вже заявляється, що оборонна політика та політика безпеки має мати громадянський характер у плані визначення стратегічних орієнтирів та процесів адміністрування [38; 71]. Відтак, необхідними є дослідження з виходом на інформаційне управління й аналіз геостратегічної та геопросторової комплексної соціально-економічної ситуації. Даний напрям доречно реалізовувати з позиції зростання геостратегічної та геопросторової інформації. У цьому контексті можливо стверджувати про синергію такої інформації та даних, що зумовлює необхідність у їх врахуванні в межах системи публічного управління. Необхідність побудови чіткої системи оцінювання ризиків вбачається як елемент єдиної державної політики у сфері управління національною безпекою, від якої залежить і соціально-економічний розвиток країни, що здійснюється на основі випереджаючого сценарного аналізу, так й імітаційного моделювання з використанням апарату функціональних знакових орієнтованих графів. При цьому потрібно зважати на актуалізацію використання штучного інтелекту при оцінці ризиків. Передбачається, що ШІ змінить процес прийняття рішень у сфері оборони

та безпеки чотирма основними способами. По-перше, за рахунок можливості «когнітивного маневру» із використанням передиктивної аналітики для більш раннього втручання та нейроаналітики. По-друге, змушуючи людей виходити «з циклу» для прийняття рішень, і застосовуючи модель Zero Trust у цілях безпеки. По-третє, надаючи рекомендації, що веріфікуються з часом, хоча можуть бути важко зрозумілими. По-четверте, у короткостроковій перспективі, надаючи безпрецедентну оперативність і реакривність процесам прийняття рішень, що містять опис ментальних моделей, на яких ґрунтують рішення, щоб забезпечити можливість порівняння з автоматизованою (нейроаналітикою) аналітикою. У цьому контексті відзначимо, що оновлена Стратегія національної безпеки України має враховувати дані способи впливу цифрових технологій (у т.ч. ШІ) на сектор безпеки й оборони.

Питання оцінювання ризиків національної безпеки тією чи іншою мірою позначені в науоквій літературі та знайшли розвиток у формуванні нових теорій щодо «передбачення» різних аспектів публічного управління (див. [25; 27; 28; 38; 53–56]). Сучасна ж оцінка ризиків національної безпеки може здійснюватися переважно в рамках деліберативного методу ранжування ризиків, до якого на певних етапах застосовуються методи Delphi, Foresight і Stakeholders Engagement. Це покликано забезпечити дослідження ризиків нацбезпеки не обмежуючись однією зі сфер функціонування публічного управління. Представлені методи все активніше акцентують увагу на необхідності вибудовування комплексної системи «випереджаючого» публічного управління як складного процесу прийняття рішень на основі великих обсягів даних (big data), сформованих на підставі результату оцінок стану індикаторів та показників верхнього та нижнього рівнів. Такий процес на «випередження» виникнення ризику та розвитку сценаріїв найбезпечнішого майбутнього спрямований на визначення ефектів від впливу цифрових технологій, серед яких big data належить одне з визначальних місць.

Слід розуміти, що стратегічне планування здійснюється, з одного боку, відповідними інститутами та соціальними суб'єктами. З іншого боку, на користь соціальних інститутів та людей, тобто для соціальних суб'єктів. У цьому контексті важливо вказати, що соціальні суб'єкти як суб'єкти стратегічного планування повинні враховувати особливості розвитку неживих цифрових технологій. Це додає особливого значення ролі соціальних суб'єктів, адже вони виступають до того ж представниками суспільства, на яких ці технології також в різній мірі впливають. Відтак, потрібно розглядати аспекти діяльності соціальних суб'єктів як суб'єктів стратегічного планування з позиції застосування інструментів і механізмів публічного управління.

Застосування індикативних оцінок як підхід до визначення ризиків національної безпеки, що розглядається в цьому дослідженні, можна віднести до інструментальних підходів і, говорячи ширше, до інструментальних теорій, предмет яких формується під впливом методів Delphi, Foresight і Stakeholders Engagement. Інструментальний характер індикативного підходу у сфері нацбезпеки передбачає таке: 1) характеристику його застосування переважно не до об'єктів фізичного світу, а до опосередкованих предметів, які є продовженням інтелектуальної діяльності людини – цифрових технологій; 2) наявність кількох конструктів у контексті різних експертних підходів до оцінки ризиків національної безпеки; 3) сукупність чіткого набору методів, які застосовуються до певної сфери суспільної діяльності (публічного управління у сфері національної оборони та безпеки) [28, 38; 53–56].

У той же час, потрібно розуміти, що індикативне оцінювання є лише передумовою прийняття відповідних управлінських рішень. В їх розробці та прийнятті бере участь багато акторів, і структура їхньої взаємодії має бути побудована таким чином, щоб індикативні оцінки враховувалися як провідна ланка в аналітиці, на основі якої ці рішення приймаються. Уважаємо, що поєднання теорії індикативних оцінок та акторно-мережевої

теорії, яка задає параметри аналітики, прийнятної для взаємодії акторів, дозволить забезпечити більш ефективну побудову та подальше застосування системи оцінки ризиків національної безпеки в умовах впливу цифрових технологій.

Незважаючи на те, що саме поняття публічне управління чітко не визначене, воно й досі активно обговорюється в науковому середовищі. Це пов'язано, серед іншого, із процесом глобалізації та появою нових акторів, які зменшують поділ між державою та громадянським суспільством у бік забезпечення публічності. Вона зачіпає політичні наслідки соціальних й інституційних змін, оскільки зміщується до нового акценту на соціально-політичні інститути у світі, що постійно змінюється. Власне, публічне управління є результатом завершених дій і формою соціальної координації. Таким чином, концепція мереж публічного управління (Governance Networks) безпосередньо пов'язана з процедурною й орієнтованою на результат логікою, яка збігається з іншими підходами, що використовуються у цій роботі. На даний момент, в її основі знаходиться методика оцінювання ризиків національної безпеки держави на базі Delphi та Foresight, що передбачають урахування експертних висновків і сценарів (оптимістичного та песимістичного).

Публічне управління у сфері самоорганізованих мереж, очевидно, має відбуватись через планування та стратегування. Ці мережі самоформуються і, ґрунтуються на спостереженнях, згодом набуваючи все більшої сили та самостійності. Застосування концепції мереж управління зростає. Зрозуміло, що через це відбуваються певні методичні зрушення, які лише посилюватимуться в майбутньому. У цьому контексті існує необхідність розуміння даного тренду, щоб спробувати визначити та зрозуміти ці мережі, зробити картування механізмів управління та визначити державних та приватних суб'єктів (акторів), які беруть участь у глобальних процесах і національних процесах забезпечення системи безпеки. При цьому можна визначити деякі позитивні моменти для ініціювання досліджень у сфері

публічного управління, з точки зору мережі, а саме:

а) мережі мають значний потенціал для активного публічного управління, оскільки кілька суб'єктів здатні швидше виявляти нові можливості та проблеми, а також виробляти гнучкі відповіді, що відповідають складності та різноманітності фіксованих умов;

б) мережі є важливими інструментами об'єднання інформації, знань та оцінок, які пов'язані з політикою. Актори цих мереж, як правило, мають відповідні знання для прийняття такого роду рішень, і коли знання всіх зацікавлених суб'єктів об'єднуються, вони є важливою основою для прийняття раціональних управлінських рішень серед можливих варіантів;

в) мережі створюють рамки для досягнення консенсусу або принаймні для врегулювання конфліктів між заінтересованими сторонами;

г) мережі знижують ризики стійкості, оскільки коли суб'єкти беруть участь у процесі, вони з більшою ймовірністю будуть надавати підтримку.

У новій теорії управління (New Public Management) вважається, що мережі мають рівні можливості для позитивного, а також негативного впливу на управлінський потенціал [223; 228; 266]. Таким чином, важливо визначити, як формуються ці мережі, хто їх формує, і як вони функціонують, оскільки вони мають такий самий безпосередній вплив на публічне управління. Чим більше ми знаємо про мережі, тим краще розуміємо динаміку публічного управління та його відносини з урядом, неформальними механізмами та приватними суб'єктами. Це також допомагає визначити категорії для аналізу даних. Зокрема, у дослідженні необхідно встановити групи значущих індикаторів, індексів та показників для відстеження трендів зміни ризиків національної безпеки в умовах впливу цифрових технологій.

Процес прийняття рішень у системі публічного управління реалізуються на основі зв'язків між суб'єктами та об'єктом, з яким вони мають справу. Говорячи про управління й оцінку ризиків нацбезпеки, стратегічні аспекти входять у сферу аналізу як важливі елементи, які мають

бути окреслені, тому що багато з того, що вирішено (а також те, що ще не виявлено в ході аналізу) має прямий вплив на таке:

1) те, як стратегії розробляються та виконуються;

2) стратегічні результати.

Розуміння процесу змісту та стратегічних результатів відповідно до логіки стратегії як практики представляється логічним способом вивчення багатьох питань. Зокрема, у цьому випадку можливе поєднання оцінок ex post та ex ante у рамках методики оцінки ризиків національної безпеки держави. На наше переконання, шляхом мережевого аналдізу механізмів публічного управління, виявлення та розуміння дій відповідних суб'єктів, складання груп індикаторів, а також розробки пояснень цих питань, одночасно надаються відповіді на стратегічні питання. Це особливо цінно для стратегічних результатів, оскільки публічне управління та стратегічні результати взаємопов'язані [25; 38; 71]. Крім того, визначення стратегічних результатів не повинно обмежуватись економічними результатами, а також соціальними й екологічними результатами.

У зв'язку з цим індикатори та показники оцінювання ризиків національної безпеки в умовах впливу цифрових технологій є ключовими інструментами такої аналітики, вони дозволяють розглядати та вимірювати різні аспекти безпеки країни чи регіону. Крім того, у цьому напрямку може бути використано в аналітичних системах «нейроаналітичний компонент» прийняття рішень для виявлення загроз, оцінки рівня вразливості та визначення ефективності заходів щодо забезпечення нацбезпеки.

Перерахуємо деякі основні категорії індикаторів та показників, які можливо використовувати для оцінювання ризиків національної безпеки:

1. Мілітарні індикатори:

– військовий бюджет (обсяг фінансування збройних сил);

– чисельність збройних сил (кількість активних військовослужбовців та військової техніки);

– арсенал ядерної та хімічної зброї (наявність та кількість такої зброї);

– військові операції (активність збройних сил у конфліктах).

2. Економічні індикатори:

– ВВР, рівень інфляції (стабільність фінансової системи та низький рівень інфляції стимулюють розвиток цифрових технологій та інноваційної діяльності);

– зовнішньоторговельний баланс (стан торгових відносин з іншими країнами);

– зайнятість та безробіття.

3. Соціальні індикатори:

– демографічні показники (населення, народжуваність, смертність);

– рвень освіти (рівень грамотності та доступу до освіти загалом, а також цифрової грамотності серед населення);

– рівень бідності та нерівності (рівень життя та соціальна нерівність. Населення з низьким рівнем доходу буде більш схильним дот вияву апатії, невдоволення та ін., що загрожує системі безпеки в країні);

– охорона здоров’я (доступ до медичних послуг та здоров’я населення, наявність можливостей безбар’єрного доступу до медичних послуг).

4. Політичні індикатори:

– політична стабільність (оцінюється рівень політичних, суспільно-політичних та інших конфліктів у країні, а також нестабільності на рівні вищої влади);

– рівень корупції (оцінюються заходи щодо протидії виявам корупції в державному та приватному секторах, а також у суспільстві загалом);

– громадянські права та свободи (дотримання прав людини та громадянських свобод, їхній захист).

5. Кібербезпека:

– кібератаки та супітні інциденти (кількість і характер кібератак);

– рівень кіберзахисту (ефективність заходів щодо захисту інформаційних систем).

6. Екологічні індикатори:

– екологічні катастрофи та стан реагування на них;

– забруднення навколишнього середовища (рівень забруднення повітря, води та ґрунту, що оцінюється із використанням цифрових технологій);

– зміна клімату (вплив зміни клімату на безпеку).

Індикативний підхід до застосування цих індикаторів при аналізі національної безпеки країни полягає в тому, щоб: а) постійно збирати та обробляти масиви даних, що відносяться до цих індикаторів; б) індекси, що отримуються, по кожному з індикаторів ранжувати для кожної, отримуючи рейтинг за відповідними індексами; в) за допомогою кореляційного аналізу ранжувань знаходити дублюючі індекси й усувати дублювання; в) виявляти тренди у ранжуваннях та встановлювати коридори допустимої динаміки; г) у випадках виходу за межі коридорів фіксувати настання ризиків і загроз національній безпеці.

Її індикатори та показники, які вибираються залежно від конкретних потреб оцінки ризиків, можуть бути адаптовані до конкретної ситуації та стратегій національної безпеки (у нашому випадку до оновленої Стратегії національної безпеки в Україні). Індикатори відіграють ключову роль у стратегічному плануванні, оскільки вони дозволяють оцінити прогрес у досягненні стратегічних цілей і відстежити зміни в середовищі публічного управління. Зважаючи на вказане, можна виділити таку послідовність використання індикаторів у процесі стратегічного планування у сфері національної безпеки в умовах впливу цифрових технологій:

1. Визначення стратегічних цілей і завдань:

– перший етап у стратегічному плануванні – це визначення стратегічних цілей і завдань. Такі цілі можуть бути пов’язані з розвитком бізнесу, зростанням організації, покращенням якості послуг та іншими аспектами.

2. Вибір ключових індикаторів:

– на цьому етапі обираються індикатори, які найкраще відображають прогрес у досягненні стратегічних цілей. Індикатори мають бути конкретними, вимірюваними, досяжними, релевантними та пов’язаними з часовими рамками (критерії SMART).

3. Установлення базових значень:

– для кожного обраного індикатора фіксуються початкові (базові) значення. Це дозволяє мати точку відліку для вимірювання прогресу.

4. Установлення цільових значень:

– визначаються бажані цільові значення кожного індикатора. Цільові значення пов’язані з кінцевими результатами і дозволяють оцінити, чи досягнуто стратегічні цілі.

5. Моніторинг та вимір:

– під час реалізації стратегії індикатори регулярно моніторяться та вимірюються. Дані збираються й аналізуються з урахуванням базових і цільових значень.

6. Аналіз й інтерпретація:

– отримані дані аналізуються для визначення, як зміни в індикаторах впливають на досягнення стратегічних цілей. Це також включає оцінку факторів, що впливають на прогрес.

7. Коригування стратегії:

– якщо аналіз індикаторів вказує на невідповідність очікуваним результатам, стратегія може бути скоригована. Це може включати перегляд цілей, тактик, ресурсів або термінів.

8. Звітність та комунікація:

– результати моніторингу й аналізу індикаторів подаються у вигляді звітів. Звіти можуть бути використані для інформування стейкхолдерів та прийняття рішень.

9. Поліпшення процесу:

– стратегічне планування є циклічним процесом. Досвід і результати моніторингу можуть бути використані для покращення стратегії та процесу

планування у майбутньому.

Індикатори, що використовуються у стратегічному плануванні у сфері нацбезпеки, допомагають державним інституціям, науковим установам та іншим зацікавленим суб'єктам більш ефективно координувати та вимірювати прогрес у досягненні цілей. Вони також сприяють прийняттю більш інформативних й обґрунтованих управлінських рішень, що є ключовим елементом успішного стратегічного планування в системі публічного управління [25; 38; 71].

Отже, індикативна оцінка ризиків національної безпеки – це методика оцінювання ризиків в зазначеній сфері, що ґрунтується на використанні певних індикаторів або показників, які можуть вказувати на можливі ризики чи потенційні загрози, виклики. Цей підхід еволюціонував з часом, ураховуючи потреби, що змінюються, і можливості у сфері публічного управління ризиками та стратегічного прогнозування.

Умовно можна виділити три основні етапи у розвитку методики індикативної оцінки ризиків національної безпеки:

1. Методи: у початкових стадіях використовуються звичайні індикатори такі, як фінансові показники, статистичні дані та показники ринкової діяльності для передбачення ризиків, пов'язаних з економічною стабільністю, сектором безпеки тощо.

2. Розвиток інтегрованих моделей: потім можуть застосовуватись інтегровані моделі, які поєднують безліч індикаторів та показників для оцінки ризиків. Це передбачає використання статистичних методів, множинних регресій і аналізу часових рядів для більш точного прогнозування.

3. Використання технологій та великих даних (big data): із розвитком цифрових технологій і доступності великих даних індикативна оцінка ризиків у сфері нацбезпеки стала більш точною та комплексною. Аналітики можуть тепер використовувати машинне навчання та алгоритми глибокого навчання для аналізу великих обсягів даних та виявлення латентних

тенденцій.

Індикативний підхід до оцінювання ризиків у сфері нацбезпеки (на основі даних, у т.ч. big data) знаходиться в площині доказової політики. Вона також відома як політика на основі доказів (Evidence-Based Policy – EBP), є підходом до розробки та реалізації державної політики, у межах якої рішення та заходи приймаються на основі ретельного аналізу наукових досліджень та зібраних даних, зокрема щодо ризиків розвитку цифрових технологій. Основний принцип доказової політики полягає в тому, що державні заходи та програми мають бути засновані на наукових фактах, емпіричних доказах і кращих практиках, а не лише на політичних переконаннях чи ідеології. Для прийняття управлінського рішень використовуються актуальні дані, а також оцінка ефективності запропонованих державних заходів. Результати аналізу доказів повинні бути доступними для всіх зацікавлених сторін, включаючи громадян та інших організацій. Це сприяє прозорості та відкритості системи публічного управління, і дозволяє суспільству оцінити його впроваджені заходи. Для забезпечення довіри населення потрібно усувати цифрові бар'єри на шляху оцінювання цих заходів. Відтак, доказова політика повинна передбачати механізм коригування політичних рішень на основі нових даних і досліджень. Це дозволяє покращувати ефективність і реагувати на обставини, що змінюються. Доказова політика має приділяти особливу увагу оцінці результатів державних заходів у сфері національної безпеки та їхнього впливу на суспільство. Цей підхід надає можливість більш ефективно використовувати ресурси, зосереджуючи зусилля на програмних, стратегічних та інших державних заходах, які довели свою ефективність, зменшуючи ризик непотрібних витрат. У цьому контексті потрібно активно впроваджувати такий інструмент, як публічно-приватне партнерство. Особливо цінним його впровадження є в Україні сьогодні, коли її ресурси обмежені та спрямовуються на підтримку системи національної безпеки. Даний інструмент також є важливим під час стимулювання розвитку

інноваційної діяльності загалом і цифрових технологій зокрема [282].

3.3. Концептуальні засади прогнозування розвитку системи публічного управління у сфері національної безпеки в умовах впливу цифрових техеологій

Оцінка ризиків національної безпеки України носить, з одного боку, комплексний міжвідомчий характер, охоплюючи різні напрями оцінки – економічних, інноваційних, інформаційних, техногенних та ін. З іншого боку, варто виділити відсутність єдиної централізованої системи оцінювання серед органів влади, яка б на регулярній основі відповідала за оцінку всіх типів ризиків національної безпеки на основі єдиного організаційно-інформаційного забезпечення. Кожен із органів влади здійснює оцінку ризиків у закріпленій за ним предметній галузі з метою вироблення єдиної державної політики у цій сфері. У той же час, сучасні ризики та загрози національній безпеці часто мають гібридний характер, що робить особливо важливою їхню оцінку у взаємозв'язку один з одним на основі глибокого аналізу масивів великих даних (big data).

Національні інтереси, стратегічні національні пріоритети України, цілі та завдання державної політики у сфері забезпечення національної безпеки та сталого розвитку на довгострокову перспективу визначаються Стратегією національної безпеки [60; 81–84]. У свою чергу, Стратегія є базовим документом стратегічного планування, яке регулюється Законом України «Про національну безпеку України». Отже, практична проблема визначення ризиків національної безпеки України є невід’ємною частиною процесу стратегічного планування. У цьому контексті можна відзначити, що одним із важливих підходів у реалізації такого планування є методологія сценарного аналізу на основі розробки та дослідження імітаційних моделей, створюваних на базі апарату знакових графів, що дозволяє використовувати

як вихідні дані як якісного, так і кількісного типу. Основною перевагою цієї методології є можливість оцінки альтернативних шляхів розвитку ситуації в соціальній, економічній та політичній сферах під впливом зовнішніх та внутрішніх загроз; та просторі стратегічних та тактичних управлінських рішень щодо досягнення поставленої мети в умовах невизначеності. Важливою обставиною є той факт, що запропонована методологія враховує зовнішньополітичні реалії останніх 10-20 років й інтегрується з моделлю управління протидією інформаційної агресії (ГеоКІП – геополітичне комплексне інформаційне протиборство).

Модель ГеоКІП, у свою чергу, ґрунтується на кількох важливих припущеннях, які характеризують комплексний погляд на оцінку стану національної безпеки. По-перше, деструктивні інформаційні та цифрові впливи в рамках ГеоКІП спрямовані насамперед на суспільну свідомість та соціум в цілому (первинний вплив), які, у свою чергу, чинять активний вплив на базові показники ефективності та стійкості розвитку як соціально-економічної системи загалом, і окремих її сегментів нацбезпеки (вторинний вплив). Цю тезу багато в чому можна вважати пов’язаною з розглядом мережевої теорії стосовно питань оцінки ризиків національної безпеки (про яку йшлося в роботі вище). По-друге, ця можель передбачає визначення деструктивних інформаційних і цифрових впливів на початковому етапі інформаційної агресії з боку рф як геополітичного противника здійснюється з використанням цілеспрямовано накопиченого початкового інформаційного та технологічного потенціалу країни, що включає інформаційний ресурс, а також системи його відтворення та використання. По-третє, рівень і якість життя населення зумовлені не лише соціально-економічними показниками, а й показниками морально-психологічного стану суспільства, які є головною мішенню деструктивних інформаційних і цифрових впливів у рамках ГеоКІП (рівні поляризації, маргіналізації і люмпенізації суспільства; впевненість у завтрашньому дні). Таким чином, дослідження процесів соціально-економічного розвитку країни дійсно має здійснюватися на основі

закладених у модель об’єктивних закономірностей і сучасних тенденцій з урахуванням різних макроекономічних, ресурсних, технологічних та інших обмежень. Таким чином, наукові підходи до оцінювання ризиків національної безпеки варіюються від методів побудови комплексних та інтегральних показників до методів прогнозування процесів соціально-економічної стабільності та дестабілізації, сценарного аналізу та імітаційного моделювання.

На наше переконання, найбільш перспективний напрямок оцінювання ризиків національної безпеки в умовах впливу цифрових технологій, пов’язаний із застосуванням методів, що базуються на аналізі даних, зокрема, big data. Існує низка міжнародних баз даних та інформаційних ресурсів, які можуть використовуватися для оцінки ризиків національної безпеки, а саме:

1. Статистичні дані: офіційні статистичні органи й урядові агентства збирають дані щодо різних аспектів національної безпеки, таких як злочинність, охорона здоров'я, економіка й оборона в умовах гібридних загроз.

2. Геополітичні та військові дані: ці дані надають інформацію про міжнародні конфлікти, військові операції, арсенали країн та дипломатичні відносини країн.

3. Інформація про кібербезпеку: дані про кіберзагрози й інциденти можуть бути зібрані з джерел таких, як Міжнародний центр кібербезпеки, державні служби у сфері кібербезпеки та інші організації, що спеціалізуються на кібербезпеці.

4. Дані щодо клімату й екології: екологічні дані та прогнози щодо кліматичних змін надають інформацію про можливі екологічні ризики такі, як Всесвітня метеорологічна організація та національні служби з клімату, що можуть бути джерелами даних.

5. Дані про міграцію та демографію, що надає Управління Верховного комісара ООН у справах біженців та національні статистичні бюро.

6. Дані про кримінальну обстановку та правопорядок.

7. Економічні та супутні дані.

Для аналізу стану та ризиків національної безпеки часто використовуються географічні інформаційні системи (ГІС), які дозволяють інтегрувати та візуалізувати дані з різних джерел на картах. Існує кілька міжнародних баз даних та організацій, які надають індикатори та показники для оцінки національної безпеки щодо стану ГІС. Ці та інші джерела надають широкий спектр даних та аналітичних інструментів, які можуть бути корисними для оцінки національної безпеки та розробки політики у цій галузі.

Таким чином, на даний час сформувалися передумови для того, щоб індикативний підхід до оцінки ризиків національної безпеки в умовах впливу цифрових технологій почав активно застосовуватися, можливе використання значного масиву даних за напрямками, які збираються та обробляються. Теоретичні передумови розгортання індикативного підходу становлять практичні заходи в цьому напрямку, спрямовані на опрацювання міжнародної та вітчизняної аналітики, у т.ч. нейроаналітики.

Основне питання застосування індикативного підходу до аналітики ризиків національної безпеки в умовах впливу цифрових технологій полягає в тому, як імплементувати індикативні оцінки ризиків у наявні інформаційні та цифрові системи, що склалися в процесі мережної взаємодії акторів національної безпеки (включаючи не антропогенну частину цих акторів). Підхід до оцінки ризиків національної безпеки на основі даних (індикаторів та показників) вимагає достатньо розвиненої автоматизованої інформаційної системи (АІС) збору та обробки такої інформації, яка може бути як самостійною, так і створена на основі існуючих державних автоматизованих (інформаційних) систем. При цьому така система може включати як закритий контур обробки й обміну даними, так і відкриту частину у вигляді цифрової платформи для роботи з експертною спільнотою. Індикативний підхід є універсальним для всіх держав і може використовуватися незалежно

від національних особливостей стратегічного планування, характерних ризиків і загроз. У той же час, важливим фактором успішного застосування даного походу є певний рівень цифрової зрілості державного управління, який полягає у наявності відповідних електронних систем і підходів при ухваленні управлінських і стратегічних рішень.

Крім того, ключовим фактором є наявність системи збору та обробки масивів різнорідних даних за цілою низкою напрямків. Зокрема, у рамках цього дослідження при кількісному аналізі було розглянуто індикатори та показники економічного, соціального, правового та політичного характеру, з яких у рамках усунення дублювання можуть бути відібрані дані за такими напрямками:

– стабільність держави (Government Stability);

– соціо-економічні умови (Socioeconomic Condition);

– інвестиційний профіль (Investment Profile);

– внутрішні конфлікти (Internal Conflict);

– зовнішні конфлікти (External Conflict);

– корупція (Corruption);

– участь військових у політиці (Military in Politics);

– міжрелігійна напруженість (Religious Tension);

– правопорядок (Law and Order);

– міжетнічна напруженість (Ethnic Tensions);

– демократична підзвітність (Democratic Accountability);

– якість державного управління (бюрократії) (Bureaucracy Quality);

– оборонний бюджет держави в розрахунку на душу населення (National Defense Expenditure Per Capita);

– інтенсивність конфліктних ситуацій (Weighted Conflict Index);

– ефективність законодавчої влади (Legislative Effectiveness).

Зазначені 15 напрямків представляють собою індикатори та показники, складені на основі груп кількісних факторів, що характеризують кожен із напрямків за різними аспектами нацбезпеки, що перебуває під

впливом цифрових технологій. Слід відзначити, що пріоритетними масивами статистичних та інших даних мають бути тимчасові ряди за вказаними 15 напрямами, які вже представлені в агрегованому вигляді, також і по відношенню до стратегічного планування.

В Україні назріла потреба а оновленні та зміні документів стратегічного планування з метою забезпечення національної безпеки в сукупності з необхідністю регулярного оновлення актуальних ризиків і загроз безпеки, що зумовлюють актуальність створення спеціалізованої АІС для реалізації повноважень компетентних органів у встановленій сфері. Для ефективної підтримки процесу оцінювання ризиків національної безпеки АІС має забезпечити автоматизацію таких функцій:

1. Управління джерелами даних (формування протоколів збору та уніфікації неупорядкованих даних).

2. Управління системами даних (централізоване зберігання, зміна, керування та використання баз даних).

3. Узаємодія та подання:

– розмежування доступу користувачів до різних мережевих ресурсів;

– застосування єдиного інтерфейсу користувача для ефективного обміну інформацією між користувачами та модулями. Для досягнення мети та вирішення зазначених завдань розвиток АІС має бути заснований на наступних принципах: забезпечення централізованого збору та одноразового введення інформації, що надходить до АІС від центральних органів виконавчої влади, місцевих органів виконавчої влади, органів місцевого самоврядування, з можливістю подальшого багаторазового використання інформації, що міститься в АІС; переважне використання в рамках АІС первинних даних (індикаторів та показників); скорочення обсягу міжвідомчої та міжрівневої взаємодії з питань отримання даних та виключення дублювання запитів інформації безпосередньо з її джерела;

– забезпечення актуальності, достовірності та несуперечності даних, що містяться в АІС, єдності термінології, нормативно-довідкової інформації,

системи показників, включаючи прозорість методик формування аналітичних показників, та регламентів звітності;

– переважний обмін даними та інформацією між центральними органами виконавчої влади та місцевими органами виконавчої влади в рамках АІС;

– забезпечення відкритості АІС для інтеграції з іншими інформаційними системами за рахунок дотримання єдиних форматів, протоколів та регламентів інформаційної взаємодії між АІС та джерелами інформації;

– забезпечення гнучкості й адаптивності АІС до зміни потреб користувачів в інформації та інструментах її аналізу;

– забезпечення захисту даних, що містяться в АІС, а також розмежування прав доступу до даних АІС;

– єдність стандартів, технологій, форматів для учасників створення та експлуатації АІС;

– безоплатність доступу державних органів влади та органів місцевого самоврядування до інформації, що міститься в АІС;

– облік та об’єднання на функціональній основі поточної бази нормативної правової й аналітичної інформації у сфері стратегічного планування та національної безпеки;

– інтеграція на системному й організаційно-інформаційному рівнях;

– розвиток функціональних можливостей у частині завдань, що розв’язуються, а також типів взаємодіючих інформаційних систем, адаптація до різних умов їх застосування;

– забезпечення захисту інформації на всіх рівнях відповідно до категорії інформації;

– етапність створення АІС;

– комплексне фінансування створення й утримання АІС.

Під архітектурою АІС для збирання й обробки інформації при оцінці ризиків національної безпеки розуміються загальні принципи та логічна

організація інформаційної взаємодії елементів АІС. У цьому контексті можна виділити три рівні архітектури АІС.

1. Рівень джерел даних:

– уніфікація протоколів збору та уніфікації неупорядкованих даних.

2. Рівень системи даних:

– забезпечення централізованого зберігання, зміни, управління та використання баз даних.

3. Рівень взаємодії та подання:

– забезпечення можливості розмежування доступу користувачів до різних мережевих ресурсів;

– застосування єдиного інтерфейсу користувача для ефективного обміну інформацією між користувачами та модулями.

До складу АІС входять такі функціональні рівні: взаємодії та уявлення; система даних та джерела даних. Рівень взаємодії та подання призначений для остаточного збору, систематизації, обробки, зберігання та надання інформації у сфері стандартизації центральним органам виконавчої влади, місцевим органам виконавчої влади й органам місцевого самоврядування, здійснення форматно-логічного контролю інформації, виявлення неузгодженостей і розбіжностей у даних, що надійшли з різних джерел, а також проведення гармонізації інформації, що міститься в АІС і забезпечення інтеграції з інформаційними системами центральних органів виконавчої, місцевих органів виконавчої влади й органів місцевого самоврядування, інформаційними ресурсами інших інформаційних систем, необхідність інтеграції яких у АІС визначається функціональними вимогами до неї.

Збір даних в АІС здійснюється в рамках рівнів систем та джерел даних такими способами:

– через інтерфейси введення даних, доступних для постачальників даних на порталі АІС;

– шляхом здійснення прийому до АІС структурованих електронних

документів, сформованих та переданих з інформаційних систем органів виконавчої влади й органів місцевого самоврядування;

– шляхом інтеграції з типовими регіональними рішеннями у подібних сферах діяльності (зокрема, ситуаційними центрами).

Інформаційні ресурси даних рівнів призначені для систематизації, аналітичної обробки, зберігання та надання інформації, у тому числі з метою підвищення ефективності публічного управління у сфері оцінки ризиків національної безпеки та покращення інформаційно-аналітичного забезпечення діяльності посадових осіб профільних органів виконавчої влади з дотриманням вимог інформаційної та цифрової безпеки, встановлених законодавством України.

Модуль нормативно-довідкової інформації містить репозиторій для ведення реєстрів індикаторів і показників, довідників і класифікаторів, а також призначений для централізованого ведення та розповсюдження реєстрів, класифікаторів та ін., що використовуються у державних та місцевих інформаційних системах, для формування відомостей, необхідних під час прийняття управлінських рішень ризиків національної безпеки.

Інформаційно-аналітичні можливості модулів дозволяють здійснювати зіставлення й аналіз інформації, що міститься в рамках усіх рівнів АІС, а також забезпечувати інформаційно-аналітичну підтримку ухвалення управлінських рішень, у тому числі з використанням візуальних засобів моніторингу, оцінки та контролю даних (зокрема, big data) [249;282].

Модулі АІС є інформаційними ресурсами, що забезпечують доступ до нормативної, статистичної та аналітичної інформації у сфері оцінки ризиків національної безпеки, інструментів аналізу, різних інформаційних сервісів для успішного функціонування секретаріатів відповідних робочих груп. Також передбачено збір, обробку інформації, що надходить з інших державних інформаційних систем і порталів із метою проведення моніторингу, аналізу та прогнозування для розробки нормативно-правових актів і документів стратегічного планування. Розвиток АІС необхідно

здійснювати з урахуванням забезпечення можливості підтримки єдиних форматів, протоколів і регламентів інформаційної взаємодії з іншими державними інформаційними системами для забезпечення наскрізного надходження даних для формування індикативних оцінок.

Програмно-технічний компонент забезпечення національної безпеки та публічного управління відповідно до вимог інформаційної та цифрової безпеки, у тому числі вимог щодо збору й обробки інформації обмеженого доступу відповідно до вимог законодавства України, призначений для виконання функцій захисту АІС від несанкціонованого доступу до закритої частини інформації в рамках підсистеми інтеграції із зовнішніми державними інформаційними системами, антивірусного захисту, контролю захищеності, реєстрації й обліку доступу користувачів, резервування, резервного копіювання та відновлення АІС. Програмно-технічний компонент адміністрування та моніторингу в умовах впливу цифрових технологій забезпечує управління та налаштування програмних й апаратних засобів усіх рівнів АІС, а також здійснення моніторингу їхньої працездатності [161].

Функціональні компоненти АІС призначені на вирішення публічно-управлінських завдань, реалізація яких у АІС накладає додаткові організаційні та функціональні обмеження. Функціональні компоненти АІС розробляються за допомогою функціональності всіх рівнів АІС. Безпосередніми користувачами АІС виступають співробітники профільних органів виконавчої влади, а також громадяни, які виступають як експерти в рамках профільних робочих груп у сфері оцінки ризиків національної безпеки в умовах впливу цифрових технологій.

Модернізація та розвиток архітектури АІС має базуватись на таких принципах:

– використання підходів і технологій, які забезпечують користувачам повноту надання необхідних даних за показниками АІС;

– використання підходів і технологій, що забезпечують як

централізоване, так і децентралізоване зберігання необхідних даних для функціонування АІС;

– використання уніфікованих інтерфейсів та форматів здійснення інформаційної взаємодії між системами, що ґрунтуються на відкритих стандартах міжсистемної взаємодії;

– забезпечення готовності технічної інфраструктури до розвитку АІС щодо розширення її функціональності,

– збільшення обсягів зберігання даних, збільшення чисельності користувачів, розширення складу сервісів, що надаються;

– забезпечення можливості відновлення працездатності системи АІС та даних за мінімально короткий період у разі порушення працездатності.

Крім того, рівні АІС повинні забезпечувати зберігання в єдиному сховищі даних інформації, постійно необхідної для здійснення інформаційно-аналітичної підтримки прийняття рішень органами виконавчої влади у сфері забезпечення національної безпеки й учасниками процесу стратегічного планування, планування діяльності даних органів та здійснення моніторингу, оперативного аналізу та контролю виконання рішень. прийнятих органами виконавчої влади [27; 161].

У системі даних на основі інформації, що надходить із рівня джерел даних, повинні формуватися, постійно зберігатися агреговані дані за аналітичними показниками для оцінки ризиків національної безпеки. Також має забезпечуватись доступ до даних із використанням стандартизованих програмних інтерфейсів. Функціональні вимоги до АІС можуть уточнюватись на етапі технічного проєктування доопрацювання та розвитку системи. Відзначимо, що єдине сховище даних у межах рівня АІС має забезпечувати можливість динамічного розширення складу аналітичних показників, що завантажуються, зберігаються і надаються.

Основним інструментом аналізу в АІС є інформаційні модулі, що формуються для вирішення певної функціональної задачі (оцінки групи ризиків національної безпеки), яка забезпечується централізовано. Крім

того, можливе формування інформаційних модулів для реалізації функціональних завдань конкретних робочих груп у сфері оцінки ризиків національної безпеки. Наповнення таких інформаційних модулів забезпечується відповідною робочою групою із зовнішніх державних інформаційних систем у відповідний модуль або репозиторій даних АІС.

Із метою розвитку інформаційно-аналітичних інструментів АІС у сфері забезпечення національної безпеки в умовах впливу цифрових технологій передбачається:

– широке застосування інструментів, що автоматизують процес підтримки прийняття управлінських рішень, на основі готових технологічних платформ, у тому числі для аналізу досягнення стратегічних та операційних цілей;

– використання методик виявлення даних раніше невідомих, але доступних для інтерпретації знань, необхідних для прийняття рішень, методик змішування та інтеграції даних, статистичного аналізу даних лише на рівні великих баз даних;

– реалізація інформаційно-аналітичних можливостей, у тому числі підтримка інтегрованих інформаційних панелей, засобів прогнозування й імітаційного моделювання, засобів спільної роботи та прийняття рішень із підтримкою різних комунікаційних середовищ;

– підтримка персоналізації, формування профільних робочих столів для державних службовців різних галузей для збору та обробки даних для подальшої оцінки ризиків національної безпеки;

– формування інформаційних модулів, що дозволяють різним категоріям користувачів вирішувати різні функціональні завдання, включаючи надання швидкого доступу до інформації за допомогою цифрових технологій, яка використовується для моніторингу, аналізу, оцінки ефективності діяльності та прийняття управлінських рішень щодо основних управлінських завдань, а також можливостей застосування геоінформаційних рішень з використанням держкадастру, картографії тощо.

Перелік найбільш значущих функціональних завдань для формування інформаційних панелей розглядається та схвалюється в установленому порядку Радою безпеки та оборони України [27; 60];

– використання інструментів, що дозволяють різним категоріям користувачів створювати звіти на основі сукупності даних, що є в АІС, з урахуванням розмежування прав доступу;

– використання інструментів формування й експорту побудованих звітів, у тому числі за формами, передбаченими законодавством України;

– реалізація та публікація прикладних програмних інтерфейсів доступу до відкритих даних АІС для забезпечення можливості створення сторонніми розробниками програмного забезпечення ресурсів і прикладних програм візуалізації відкритих даних;

– підтримка вбудовування на рівні АІС програмного забезпечення сторонніх розробників, що реалізує функціональність інформаційних панелей, що забезпечує аналіз даних і прогнозування. Створення на основі такого верифікованого програмного забезпечення каталогу, що містить різноманітність візуальних уявлень даних, що зберігаються в АІС, та функціональність їх обробки [там само].

Розвиток різних аналітичних інструментів АІС сприятиме зрештою створенню єдиного інформаційного ресурсу, що забезпечує різним категоріям користувачів можливість вибору й індивідуального налаштування необхідних аналітичних інструментів та їх функціональних можливостей для більш комплексної оцінки ризиків національної безпеки.

З метою формування єдиного інформаційного простору та розвитку інформаційно-аналітичних можливостей в АІС передбачається реалізація різних інформаційних сервісів:

– сервіс надання (експорту) даних інформаційних систем органів державної влади та органів місцевого самоврядування;

– сервіс підписки на зміни єдиного реєстру баз даних (індикаторів та показників);

– сервіс передплати на періодичне оновлення даних з інформаційних систем органів державної влади та органів місцевого самоврядування за обраними показниками окремих груп індикаторів і показників з подальшим їх відображенням на профільних робочих столах керівників органів державної влади та можливістю експорту даних з АІС;

– сервіс деталізації даних, що зберігаються в АІС, за аналітичними показниками з інформаційних систем постачальників, що надаються в інтерактивному режимі в АІС;

– доступ до електронних сервісів, що надаються інформаційними системами органів державної влади та органів місцевого самоврядування;

– сервіс оперативного надання реєстрів, довідників та класифікаторів з репозиторію та модулів управління державних інформаційних систем інших органів державної влади та органів місцевого самоврядування;

– сервіс зберігання даних інформаційних систем органів державної влади й органів місцевого самоврядування в єдиній моделі даних, передбаченої в АІС, із забезпеченням інтерактивного доступу до даних через спеціальні інтерфейси, використовуючи апаратні та програмні ресурси АІС – можливість надання даного сервісу доцільно розглянути на етапах розвитку системи АІС [39; 49; 50].

Зазначені інформаційні модулі можуть бути, зокрема, затребувані місцевими органами виконавчої влади, які підвідомчі профільним міністерствам, агенціям, службам тощо. В умовах різнорідності джерел даних, що підключаються до АІС, необхідно планувати використання сучасних інструментів, що дозволяють:

– проводити аналіз даних, що надходять (індикаторів та показників), вилучати їх з баз даних інформаційних систем постачальників та перетворювати їх у єдині формати, які використовуються в АІС з метою усунення дублюючих один одного показників;

– здійснювати перетворення отриманих даних перед їх завантаженням в АІС, включаючи вибір необхідних записів та полів, усунення некоректних

та неповних значень, сортування, агрегацію, дезагрегацію, валідацію значень та інші способи очищення даних;

– здійснювати завантаження даних в АІС з урахуванням забезпечення вимог до версійності та історичності їх зберігання, підтримки цілісності посилань при зберіганні даних в АІС.

Окрема увага має бути приділена захисту інформації, яка має забезпечуватися на всіх етапах проєктування, розробки, впровадження та експлуатації АІС. Захист інформації повинен забезпечуватися на всіх технологічних етапах обробки інформації та у всіх режимах функціонування, у тому числі під час проведення ремонтних та регламентних робіт. Розширення кола користувачів АІС передбачає реалізацію механізму розмежування прав доступу, технології єдиного входу (єдиної процедури реєстрації) й організацію обліку звернень користувачів до даних. Відкрита (публічна) частина АІС надає користувачам мереж загального користування вільний доступ до основної функціональності та заздалегідь визначеним і налаштованим інформаційним панелям, які містять тематичні набори аналітичних показників для роботи експертів [39; 50].

Доступ користувачів до закритої частини АІС здійснюється через мережу загального користування з використанням систем криптозахисту інформації, що встановлюються на автоматизованому робочому місці користувача, та відповідних засобів аутентифікації. Збір й обробка первинних даних і розширення складу користувачів та споживачів інформації в АІС вимагатиме вдосконалення використовуваних у ній технологій забезпечення інформаційної безпеки, включаючи:

– ведення переліку інформаційних ресурсів, які є постачальниками даних для АІС та відомостей про рівень конфіденційності даних, що зберігаються в них;

– ведення єдиного каталогу користувачів АІС, їх ролей і категорій;

– шифрування інформації, що передається в АІС, та її антивірусний і криптографічний захист, контроль захищеності при її обробці;

– підтримку обміну юридично вагомих електронних документів між АІС та джерелами даних із використанням засобів електронного підпису;

– знеособлення даних фізичних та юридичних осіб, які надходять до АІС із відомчих джерел.

Зазначені інструменти необхідно використовувати також і при розвантаженні даних з АІС до інших державних інформаційних систем органів державної влади й органів місцевого самоврядування. Розробка та впровадження спеціалізованої АІС для оцінки ризиків національної безпеки в умовах впливу цифрових технологій дозволить вирішити проблему подвійного значення:

1) консолідувати відомчі бази даних з наявними індикаторами та показниками для цілей збору й обробки даних на користь національної безпеки;

2) усунути дублюючі один одного індикатори та показники для подальшої комплексної оцінки на їх основі ризиків національної безпеки.

При цьому АІС може бути визнана як самостійна система з елементами передиктивної аналітики для подальшого стратегічного планування, так і частиною наявних систем, підтримуючи діяльність експертних та наукових рад відповідних міністерств та відомств інших органів.

ВИСНОВКИ

Одержані під час дослідження результати передбачають визначення науково-теоретичних засад формування механізмів публічного управління у сфері національної безпеки в умовах впливу цифрових технологій і розробленні практичних рекомендацій щодо вдосконалення таких механізмів в Україні.

На підставі результатів, визначено такі висновки та пропозиції:

1. Узагальнення теоретичних засад щодо генези сфери національної безпеки в умовах впливу цифрових технологій дозволило виявити, що розвиток цієї сфери відзначається еволюційністю та парадигмальністю, зокрема, у зміщенні акцентів функціонування системи управління такою безпекою в бік публічності. З'ясовано, що цей принцип актуалізує механізми забезпечення насамперед безпеки людини. Дана тенденція притаманна й Україні, свідченням чого є прийнята Стратегія національної безпеки «Безпека людини – безпека країни» (2020 р.). У той же час, наполягається на Україна відстає в удосконаленні публічно-управлінських процесів у сфері національної безпеки з урахуванням тенденцій щодо розвитку цифровізації, на які, у свою чергу, більш успішно зважають економічно розвинені держави світу. Виявлено, що вони прагнуть вчасного врахування особливостей впливу цифрових технологій на найважливіші сфери суспільної життєдіяльності, у тому числі на прийнятий Європарламентом закон про штучний інтелект (2024 р.).

2. Визначено, що головною небезпекою, пов'язаною з використанням технологій цифровізації, є відсутність чітко ідентифікованих (видимих одразу) ознак руйнівного впливу цифрових технологій. Доведено, що цей вплив відзначається латентністю та може трансформуватися за тих чи інших умов: він передбачає насамперед потенційну можливість цільового зовнішнього та/або внутрішнього впливу із використанням цифрових технологій для поширення певної інформації, що пронизує все інституційне

середовище, представлене суб'єктами публічного управління та його об'єктом (національною безпекою), із метою зміни векторів їхнього прогнозованого функціонування із заданим рівнем інтенсивності. У цьому контексті представлено систематизацію типів технологій цифровізації: великі дані; штучний інтелект; Інтернет речей; автоматизація та робототехніка; 3D друк; віртуальна валюта та блокчейн; хмарні обчислення; технологія зв'язку нового покоління. Ця типологізація цифрових технологій засвідчила складність і специфічність їхнього розвитку, що проявляється на таких основних рівнях функціонування суспільно-політичної та соціальної системи: інфраструктурна конвергенція; конвергенція пристрою; конвергенція в послугах; ринкова конвергенція тощо.

3. Із урахуванням положень фундаментальної науки досліджено особливості формування механізмів публічного управління у сфері національної безпеки, підставою для групування яких визнано методи державного управління як одні з найбільш адаптивних елементів системи публічного управління. На цій підставі рекомендовано виокремлювати правові, організаційні, інформаційні та ресурсні механізми публічного управління у сфері національної безпеки в умовах впливу цифрових технологій. Наполягається на взаємному впливові цих механізмів публічного управління під час їхнього формування та функціонування. Окрім методів публічного управління, у складі механізмів публічного управління у сфері національної безпеки в умовах розвитку цифровізації виокремлено також мету, завдання, принципи, функції, форми й інструменти державного впливу. При цьому визначено, що цифровізація позиціонується як синергетична сила, яка чинить стабілізуючий або дестабілізуючий вплив на державний і приватний сектори. Уважаємо, що врахування синергетичного та комплексного підходів дозволить унеможливити значною мірою появу деструктивного впливу цифровізації та її технологій на зазначені сектори.

4. Проаналізовано загрози та перспективи впровадження моделі публічного управління у сфері національної безпеки в умовах впливу

цифрових технологій в Україні та за кордоном, серед яких найбільш складно прогнозованими є технології штучного інтелекту через їх недостатню дослідженість. Базис аналізу можуть становити вимірювані індикатори та параметри, розгляд яких передбачає врахування балансу між повнотою та доступністю даних (деякі бази даних мають обмежений або повний доступ). Тому запропоновано визначати показник узгодженості (консистентності) національної безпеки (security consistency) у межах моделі публічного управління у сфері нацбезпеки, що формується за допомогою різниці між показниками загроз (threats) та можливостями технологій штучного інтелекту (AI capability) реагувати на такі загрози. У межах дослідження за основу брався методичний підхід вимірів «Analyzing Affiliation Networks» (J. Scott), «Global capability index» і «Composite Index of National Capability». Цей підхід дозволив окреслити декілька варіантів упровадження моделі публічного управління у сфері національної безпеки в умовах впливу цифрових технологій, зокрема, штучного інтелекту: 1. Модель стійка до загроз і показників індикатора «можливостей штучного інтелекту» (економічна сфера); сприйняття загроз (threat perception) з індикатора «оцінки загроз». 2. Модель чутлива до загроз і таких показників: технологічної та соціальної сфери. 3. Модель демонструє стійкість до більшості загроз і показників економічної, соціальної та технологічної сфер. 4. Модель, що передбачає подальше оцінювання загроз і показників, які підлягають тестуванню, зокрема у сфері управління (state companies, legal authorization) з індикатора «можливостей штучного інтелекту»; тип/характер загроз, об’єкти/активи, що захищаються. Метод мережевого аналізу дозволив умовно проранжувати країни за показниками досягнень у сфері цифровізації та розвитку її технологій.

5. Оцінено стан функціонування механізмів публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні, який (стан) охарактеризовано як незадовільний, зокрема, у частині впровадження правового, організаційного й інформаційного

механізмів публічного управління. При цьому виявлено недоліки змістовного визначення функцій організаційного механізму публічного управління у сфері нацбезпеки в умовах впливу цифрових технологій (наявні розпорошеність і дублювання повноважень органів державної влади центрального рівня у зазначеній сфері). Крім того, обґрунтовано застосування комплексного підходу до вдосконалення чинної правової бази у сфері забезпечення національної безпеки в умовах впливу цифрових технологій. Із застосуванням запропонованого підходу доведено необхідність оновлення Стратегії національної безпеки України (на період до 2030 року) й уточнено складники механізму реалізації цієї стратегії. Акцентовано на важливості узгодження положень оновленої Стратегії національної безпеки України із нормами, по-перше, Закону України «Про національну безпеку України» у частині національних інтересів і загроз національній безпеці. А по-друге, Закону України «Про стимулювання розвитку цифрової економіки в Україні», постанови Уряду України «Про схвалення Національної економічної стратегії на період до 2030 року» тощо в частині визначення особливостей впливу цифрових технологій на національну безпеку. На відміну від вищевказаних механізмів публічного управління у сфері нацбезпеки в умовах впливу цифрових технологій, виявлено, що ресурсний механізм публічного управління в цій сфері відзначається необхідним правовим підґрунтям, зокрема, у частині визначення фінансового забезпечення. Однак ускладненим видається оцінювання кадрового складника ресурсного механізму публічного управління через обмеженість інформації в зазначеній сфері в умовах запровадженого воєнного стану на території України.

6. Обґрунтовано визначення комплексного й інституційного підходів до вдосконалення системи публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні. Застосування цих підходів може дозволити на системній основі модернізувати наявне

інституційне середовище публічного управління у сфері національної безпеки в умовах впливу цифрових технологій у напрямку, по-перше, усунення дублювання функцій органів публічної влади в цій сфері з позиції закріплення за ними повноважень щодо рівноважного використання цифрових технологій і комплексного визначення соціально-політичних ефектів розвитку цифрових технологій за допомогою індикативного підходу. Серед цих ефектів особливе місце відведено ефектам технології великих даних (big data) у публічній політиці через їх вплив на сферу забезпечення національної безпеки. А по-друге, оцінювання цифрових бар'єрів, рівня цифрової довіри та перспектив трансформації балансу між забезпеченням конфіденційності та розвитком системи національної безпеки. Крім того, акцентовано на синергії геопросторових даних для адміністрування тергромад і забезпечення системи безпеки, а також на розвитку публічно-приватного партнерства в цій сфері.

7. Запропоновано шляхи розвитку механізмів публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні. Наполягається на розвитку, по-перше, правового механізму публічного управління в цій сфері шляхом удосконалення чинного законодавства у сфері національної безпеки в напрямку доповнення його положеннями щодо ролі та місця зазначених технологій у системі публічного управління. По-друге, організаційного механізму публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні за рахунок виваженого впровадження технологій штучного інтелекту та діджиталізації діяльності сектору безпеки й оборони, на підставі чого уточнено індикатор можливостей штучного інтелекту й індикатор оцінки загроз у цій сфері, що передбачає активне застосування нейроаналітики. Крім того, ресурсний механізм публічного управління у сфері нацбезпеки вимагає актуалізації хмарних рішень і послуг у сфері публічного управління в цій сфері, розвиток

конвергентних систем на заміну традиційних сховищ даних у цій сфері, а також використання моделі Zero Trust у системах безпеки за необхідності. По-третє, інформаційний механізм публічного управління у сфері національної безпеки в умовах впливу цифрових технологій в Україні передбачає забезпечення розвитку цифрового суспільства, яке повсюдно застосовує мобільні додатки й інтерактивні платформи для отримання об’єктивної інформації та високоякісних послуг з метою формування системи безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ажажа М.А., Куртєв А.В. Компетентісний підхід та особливості його реалізації в системі підготовки кадрів державного управління та надання публічних послуг // Вісник Національного університету цивільного захисту України. 2024. Вип. 1 (20). С. 256–263.

2. Антонова Н.Б., Захарова Л.М., Вечір Л.С. Теорія та методологія державного управління: курс лекцій. 2005. 231 с.

3. Антонюк В.В. Механізми державного реагування на сучасні виклики та загрози інформаційній безпеці // Державне управління: удосконалення та розвиток. Вип. 8(10). 2014. С. 1–5.

4. Баштанник В.В. Інституціоналізація правозахисної функції влади як напрям гуманізації публічного управління: досвід Європейського Союзу та Україна // Збірник ДРІДУНАДУ. 2011. С. 87–97.

5. Баштанник О.В. Історичний інституціоналізм в політичній науці: конкретизація аналітичного поля застосування // Грані. 2012. С. 113–118.

6. Баштанник О.В. Інституціональна/інституційна спроможність інститутів політичної системи як аналітична категорія та функціональний аспект публічного управління // Держава та регіони. Серія: Публічне управління та адміністрування. 2023. № 3. С. 83-88

7. Бабков Ю.П., Бєлай С.В., Бондаренко О.Г. Підходи до запровадження елементів національної системи стійкості у діяльність органів державного і військового управління // Честь і закон. 2023. № 3 (86). С. 12–20.

8. Бєлай С.В. Державні механізми протидії кризовим явищам соціально-економічного характеру: теорія, методологія, практика : монографія. Харків: Національна акад. НГУ, 2015. 349 с.

9. Великанова М.М. Ризик у правові доктрині: підходи до визначення сутності // Проблеми цивільного права та процесу. 2017. С. 159-

162. URL: https://univd.edu.ua/general/publishing/konf/19-20_05_2017/pdf/47.pdf.

10. Великий тлумачний словник сучасної української мови / уклад. і голов. ред. В. Т. Бусел. Київ ;Ірпінь: ВТФ «Перун», 2001. 1440 с.

11. Вєдєнєєв Д. В., Семенюк О. Г. Розвиток концептуальних і науково-практичних поглядів на сутність еконвенційної (гібридної) конфліктності :монографія. Київ : ТОВ «Вид. дім «АртЕк» 2021. 228 с.

12. Воропаєва Т.С. Національна безпека України: етнопсихологічні аспекти // Проблеми безпеки української нації на порозі XXI ст. 1998. С. 156–158.

13. Галушко С.П. Модель функціонування механізмів публічного управління у сфері національної безпеки в умовах цифровізації та впливу її технологій // Вісник Національного університету цивільного захисту України. Вип. 2 (21). 2024.

14. Галушко С.П. Теоретичні засади публічного управління у сфері національної безпеки в умовах цифровізації // Вісник Національного університету цивільного захисту України. Серія: Державне управління. Вип. 1 (20). 2024. С. 80–87.

15. Галушко С.П. Typology of digital technologies and their socio-political and state-legal effects on the sphere of national security // Public administration and state security aspects. 2024. Vol. 1. Pp. 15–32.

16. Галушко С.П. Аналіз стану функціонування та перспектив розвитку системи публічного управління у сфері національної безпеки в умовах цифровізації та впливу інформаційних загроз // Держава і суспільство: сучасні виклики та пошук рішень : матеріали III Всеукраїнської науково-теоретичної конференції (16.05.2024, м. Київ). Київ: КТЕУ. С. 294–298.

17. Галушко С.П. Концептуальні засади розвитку публічного управління у сфері національної безпеки в умовах впливу технологій цифровізації // Публічне управління та адміністрування в Україні: євроінтеграційний поступ : матеріали I Всеукраїнської науково-практичної

конференції за міжнародною участю (31.05.2024 р., м. Івано-Франківськ). Івано-Франківськ: І.-Ф.НТУНіГ. С. 330–332.

18. Галушко С.П. Підходи до вдосконалення системи публічного управління у сфері національної безпеки України в умовах цифровізації // Державне управління: удосконалення та розвиток. 2024. № 11. URL: https://www.nayka.com.ua/index.php/dy/article/view/5048.

19. Горбулін В. Як перемогти росію у війни майбутнього. К.: Вид-во Брайт Букс. 2020. 256 с.

20. Двуліт З.П., ЗавербнийА.С., Романюк А.О. Диджиталізація – дієвий інструмент антикризового розвитку бізнесу в умовах пандемії. Ефективна економіка, 2021. № 1. URL: http://www.economy.nayka.com.ua/?op=1&z=85571-8.

21. Дергачова В.В., Голюк В.Я. Цифрова термінологія у стратегіях. Сутність, місце та роль діджитал менеджменту. Економічний вісник НТУУ «Київський політехнічний інституту», 2022. № 22. С. 114−117.

22. Дідківська Л.І., Головко Л.С. Державне регулювання економіки : навч. посіб. К. : Знання-Прес, 2000. 209 с.

23. Дія Центри. URL: https://center.diia.gov.ua/cnap-analytics.

24. Довгань О.Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки // Інформаційна безпека людини, суспільства, держави. 2015. Вип. 3 (19). С. 6-17.

25. Домбровська С.М., Помаза-Пономаренко А.Л., Лукиша Р.Т. Інституціональна державна політика соціально-економічного розвитку регіонів України в умовах ризиків: монографія. Харків: НУЦЗ України, 2018. 216 с.

26. Домбровська С., Помаза-Пономаренко А., Нікіпєлова Є. Уніфікація правового механізму України та Республіки Польща щодо зміцнення національної безпеки : монографія. Харків: НУЦЗУ. 2019. 256 с.

27. Домбровська С.М., Помаза-Пономаренко А.Л., Крюков О.І.,

Порока С.Г. Інформаційні загрози та комунікативна інфраструктура в державному секторі: монографія. Харків: НУЦЗУ, 2024. 244 с.

28. Древаль Ю.Д., Помаза-Понмаоренко А.Л. Проблематика державно-правового регулювання соціальної безпеки // Матеріали Міжнародної науково-практичної конференції «Державне управління у сфері цивільного захисту: наука, освіта, практика». Харків: НУЦЗ України, 2019. С. 209–210.

29. Дрешпак В.М. Дрешпак В.М., Бондаренко Є.М. Комунікативна культура державного службовця у світлі циклічної парадигми // Вчені записки Таврійського національного університету ім. В. І. Вернадського. Серія: Державне управління. 2019. Т. 30 (69). № 6. С. 1–6.

30. Еволюція воєнного мистецтва: навчальний посібник. У 2 ч. Ч. 1. Київ. 2017. URL: https://shron3.chtyvo.org.ua/Viedienieiev_Dmytro/Evoliutsiia_voiennoho_mystetstva_U_2_ch_Ch_1.pdf?PHPSESSID=p68bmuj1tqjeh40je4buj69nh6.

31. Енциклопедичний словник з державного управління / [укл. Ю.П. Сурмін, В.Д. Бакуменко, А.М. Михненко та ін.] за ред. Ю.В. Ковбасюка, Ю.П. Сурміна. К.: НАДУ, 2010. 820 с.

32. Жаровська І., Ортинська Н. Інформаційна війна як сучасне глобалізаційне явище // Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки. 2020. Вип. 2 (26). С. 56–61. https://doi.org/10.23939/law2020.26.056.

33. Жилін С.В. Перспективи розвитку державного регулювання щодо забезпеченя безпеки банківських установ у контексті формування інформаційного суспільства // Вісник Національного університету цивільного захисту України. Вип. 1 (20). 2024. С. 215–228.

34. Іщук С.М. Інтернет-комунікації: інформаційний зміст та ігровий характер // Вісник Національного авіаційного університету. 2008. № 2. С. 87–91.

35. КотелевецьД. О. Тенденції розвитку цифрової економіки в Україні // Проблеми сучасних трансформацій. Серія: «Економіка та управління», 2022. № 5. DOI: https://doi.org/10.54929/2786-5738-2022-5-03-01.

36. Котух Є.В. Кібербезпека у публічному секторі : монографія. Харків: Колегіум. 2021. 272 с.

37. Краус К.М., Краус Н.М., Манжура, О.В. Електронна комерція та Інтернет-торгівля: навчально-метод. посібник. Київ : Аграр Медіа Груп, 2021. 454 с.

38. Крук С.І. Поняття та сутність механізмів державного управління у сфері забезпечення національної безпеки України// Держава та регіони, 2018. № 4. С. 87–90.

39. Крюков О.І. Інформаційне забезпечення публічної влади як чинник національної безпеки держави в умовах глобалізації. Вісник Національного університету цивільного захисту України. Серія: Державне управління. Вип. 1(4). 2016. С. 142–149.

40. Крюков О.І. Комунікація влади і суспільства як чинник реалізації політики інформаційної безпеки. Вісник Національного університету цивільного захисту України. Вип. 1(6). 2017. С. 201–207.

41. Крюков О.І., Помаза-Пономаренко А.Л. Теорія та історія державного управління : конспект лекцій. Харків: НУЦЗ України, 2016. 40 с.

42. Крюков О.І., Помаза-Пономаренко А.Л., Лопатченко І.М. Публічне управління у сфері цивільної безпеки : навчальний посібник. 2024. 172 с. URL: http://repositsc.nuczu.edu.ua/handle/123456789/19932.

43. Крюков О.І., Шкурат І.В. Методологія дослідження та механізми формування еліти в умовах глобалізації // Публічне управління: теорія та практика. 2013. Вип. 2. С. 71-77.

44. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі: навч. посіб. Київ: ВІКНУ, 2016. 286 с. URL: http://www.mil.univ. kiev.ua/files/222_1044284240.pdf.

45. Курбан О.В. Сучасні інформаційні війни в соціальних онлайн-мережах // Інформаційне суспільство. 2016. Вип. 23. С. 85–90.

46. Лапін А., Грінчук І., Оленюк Д. Діджиталізація економіки в Україні: сучасний стан та перспективи // Електронний журнал «Ефективна економіка». 2022. № 7. DOI: https://doi.org/10.32702/2307-2105.2022.7.22.

47. Лободенко К.В. Удосконалення механізмів правозахисної політики держави. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2019/3_2019/22.pdf.

48. Лопатченко І.М., Помаза-Пономаренко А.Л., Батир Ю.Г. Державне регулювання у сфері інформаційної безпеки України в умовах воєнного стану // Вісник Національного університету цивільного захисту України. 2024. № 1 (20). С. 14–24.

49. Любохинець Л.С., Шпуляр Є.М. Цифрова трансформація національної економіки: сучасний стан та тренди майбутнього // Вісник Хмельницького національного університету. Економічні науки, 2019. № 4. С. 213–128.

50. Мазуренко Л.І. Інформаційна безпека в умовах російсько-української війни: виклики та загрози. Вісник Харківського національного університету імені В.Н. Каразіна, серія «Питання політології». 2022. № 42. С. 50–57.

51. Мельник, Л.Г., Карінцева, О.І., Кубатко, О.В., Сотник, І.М., Завдовєва, Ю.М. Цифровізація економічних систем та людський капітал: підприємство, регіон, народне господарство // Механізм регулювання економіки, 2020. № 2. С. 9–28.

52. Мельтюхова Н.М., Набока Л.В. Реалізація державно-управлінських відносин на регіональному рівні: монографія. Х.: Вид-во ХарРІ НАДУ «Магістр», 2014. 180 с.

53. Новіков В.О. Аналіз сучасної концепції інформаційно-гібридної війни // Державне управління: удосконалення та розвиток:

електронний журнал. 2023. № 9. URL: https://www.nayka.com.ua/index.php/dy/article/view/2133.

54. Новіков В.О. Дисфукнціоналізація інституційної системи та механізмів публічного управління в умовах інформаційно-гібридних війн // Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2020. Вип. 2 (13). С. 345–354. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/18688/1/vdu13.pdf.

55. Новіков В.О. Ризик-орієнтований підхід до формування інституційних механізмів публічного управління в умовах інформаційно-гібридних війн: досвід Франції, Казахстану й України // Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2020. Вип. 1 (12). С. 300–308.

56. Новіков В.О. Information and hybrid wars in the current environment: public-administrative aspect // Public administration and state security aspects. 2023. Vol. 2. P. 43–51.

57. Новіков В.О. Theoretical and institutional features of the modern definition of the concept of hybrid war // Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2023. Вип. 2 (19). С. 207–212.

58. Олещук П.М. Новітні політичні технології інформаційного впливу : монографія. Київ : Видавець Вадим Карпенко, 2018. 288 с.

59. Олійник О.В. Структура суб’єктів забезпечення інформаційної безпеки в Україні // Актуальні проблеми держави і права. Вип. 68. 2016. С. 485-491.

60. Офіційний веб-сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2469-19.

61. Офіційний веб-сайт Державної служби статистики України. URL: https://www.ukrstat.gov.ua/.

62. Пархоменко-Куцевіл О.І. Формування та реалізація

державної молодіжної політики: європейський досвід та позитивні практики для україни. URL: http://perspectives.pp.ua/index.php/sn/article/view/9142.

63. Помаза-Пономаренко А.Л. Роль інституту президентської влади у сфері забезпечення національної безпеки // «Теорія та практика державного управління і місцевого самоврядування». 2019. № 1. URL: http://el-zbirn-du.at.ua/index/zmist_2019_1/0-39.

64. Помаза-Пономаренко А.Л., Батир Ю.Г., Лопатченко І.М. Вплив BANI-світу на державне регулювання ринку праці та державну молодіжну політику // Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2024. Вип. 1 (20). С. 296–306.

65. Помаза-Пономаренко А.Л., Батир Ю.Г., Лопатченко І.М. План відновлення сталого розвитку та системи безпеки України : монографія. Харків: НУЦЗУ, 2023. 240 с.

66. Помаза-Пономаренко А.Л., Вербицький О.В. Виклики соціальної (гуманітарної, міграційної, інформаційної та ін.) безпеки України в ситуаціях ковідного / надзвичайного характеру як фактори позасистемності й трансформації // Вісник Національного університету цивільного захисту України. 2021. Вип. 1 (14). С. 298–304.

67. Помаза-Пономаренко А.Л., Микитюк Ю.М. Цифровізація державної політики vs. державна політика цифровізації у сфері правового регу-лювання : монографія. Х.: НУЦЗУ. 2021. 200 с.

68. Помаза-Пономаренко А.Л., Сємілєтов О.С., Медведєва Д.О., Крюков О.І. Ефективність дії механізмів публічного управління в екологічній сфері в Україні: контент-аналіз правової, інституційної й інноваційної складових // Публічне управління та митне адміністрування. 2021. № 2 (29). С. 44-48.

69. Помаза-Пономаренко А.Л., Новіков В.О. Шляхи трансформації інституційних механізмів публічного управління в Україні: від інформаційних загроз до гібридних війн // Державне будівництво. 2023. № 2.

URL: https://periodicals.karazin.ua/db/issue/archive.

70. Помаза-Пономаренко А.Л., Тарадуда Д.В. Драйвери сталого розвитку та системи громадської безпеки України в контексті реалізації її євроінтеграційних прагнень // Державне управління: удосконалення та розвиток. 2024. № 2. URL: https://www.nayka.com.ua/index.php/dy/article/view/2989.

71. Помаза-Пономаренко А.Л., Тарадуда Д.В. Розвиток публічно-приватного партнерства у сфері критичної інфраструктури: світовий і вітчизняний досвід // Дніпровський науковий часопис публічного управління, психології, права. 2024. Вип. 3.

72. Помаза-Пономаренко А.Л., Тарадуда Д.В. Службово-бойова діяльність сил охорони правопорядку та міжнародне гуманітарне право // Державне управління: удосконалення та розвиток. 2024. № 3. URL: https://www.nayka.com.ua/index.php/dy/article/view/3229.

73. Порока С.Г. Правове забезпечення державної політики у сфері національної та цивільної безпеки України. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/16867/1/Poroka.pdf.

74. Почепцов Г.Г. Смислові та інформаційні війни // Інформаційне суспільство. 2013. Вип. 18. С. 21–27.

75. Прав Р.Ю. Діяльність суб’єктів формування і реалізації політики державної безпеки в інформаційній сфері України. URL: http://www.dy.nayka.com.ua/pdf/9_2018/103.pdf.

76. Правосуд О.В. Фактори формування довіри населення як механізму публічного управління в контексті забезпечення системи безпеки. URL:
http://repositsc.nuczu.edu.ua/bitstream/123456789/15861/1/Pravosud818.pdf.

77. Примуш Р.Б. Роль цифровізації в системі публічного управління у сфері національної та цивільної безпеки в Україні. URL: http://vdu-nuczu.net/ua/11-ukr/storinkaavtora/268-primush-r-b-rol-tsifrovizatsiji-v-

sistemi-publichnogo-upravlin-nya-u-sferi-natsionalnoji-ta-tsivilnoji-bezpeki-v-ukrajini.

78. Про адміністративні послуги : Закон України від 06.09.2012 р. № 5203-VI. URL: https://zakon.rada.gov.ua/laws/show/5203-17#Text.

79. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.

80. Про стимулювання розвитку цифрової економіки в Україні, Закон України // Відомості Верховної Ради України. 2023, № 6-7, ст. 18.

81. Про Стратегію національної безпеки України : указ Президента України від 12.02.2007 р. № 105. URL: https://zakon.rada.gov.ua/laws/show/105/2007#Text.

82. Про нову редакцію Стратегії національної безпеки України : указ Президента України від 08.06.2012 р. № 105. URL: https://www.president.gov.ua/documents/3892012-14402.

83. Про Стратегію національної безпеки України : указ Президента України від 26.05.2015 р. № 287/2015. URL: https://www.president.gov.ua/documents/2872015-19070.

84. Про Стратегію національної безпеки України : указ Президента України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text.

85. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації. Розпорядження Кабінету Міністрів України від 24.12.2018 № 67-р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80.

86. Саприкін О. В. Інтернет-ресурси як інструмент інформаційної війни й інформаційна безпека України // Бібліотекознавство. Документознавство. Інформологія. 2015. № 2. С. 72–77.

87. Світова гібридна війна: український фронт : монографія / за заг. ред. В.П. Горбуліна. Київ : НІСД, 2017. 496 с.

88. Світовий рейтинг цифрової конкурентоспроможності – IMD. URL: https://www.imd.org/centers/worldcompetitiveness-center/rankings/world-digital.

89. Семен Н.Ф. Засоби протидії інформаційній агресії в українському інтернет-просторі // Перспективні напрямки дослідження українського медійного контенту: фундаментальні та прикладні аспекти : матеріали Всеукр. наук.-практ.конф. (м. Київ, 7 квіт. 2016 р.). Київ:Інститут журналістики. 2016. С. 231–234.

90. Ситник Г.П. Державне управління у сфері національної безпеки (концептуальні та організаційно-правові засади) : підручник. Київ: НАДУ, 2012. 544 с.

91. Степанов В.Ю. Цифровізація та ризики цифрової безпеки // Вісник Національного університету цивільного захисту України (Серія «Державне управління»). 2024. № 1 (20).

92. Стратегія інформаційної безпеки : рішення Ради національної безпеки і оборони України від 15.10.2021 р. URL: https://zakon.rada.gov.ua/laws/show/685/2021?find=1&text=%D0%B3%D1%96%D0%B1%D1%80%D0%B8%D0%B4%D0%BD#w1_1.

93. Топ збройних та політичних конфліктів у 2023 році: що про них відомо // Слово і діло. URL: https://www.slovoidilo.ua/2023/04/03/infografika/svit/top-zbrojnyx-ta-politychnyx-konfliktiv-2023-roczi-pro-nyx-vidomo.

94. Требін М.П. Феномен інформаційної війни у світі, що глобалізується. Вісник Національного університету “Юридична академія України імені Ярослава Мудрого”. Серія: Філософія, філософія права, політологія, соціологія // Право. 2013. № 2 (16). С. 188–198.

95. Україна 2030Е – країна з розвинутою цифровою економікою. Український інститут майбутнього, 2018. URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html.

96. Центральність // Вільна Енциклопедія Вікіпедія. URL: https://uk.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BD%D1%82%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D1%96%D1%81%D1%82%D1%8C.

97. Цимбал Б.М. Безпека особистості в системі національної безпеки держави. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/17307/1/ZBNMKS2023%20%281%29.pdf.

98. Хмиров І.М. Державне управління розвитком дистанційної освіти України. URL: https://nuczu.edu.ua/images/topmenu/science/spetsializovani-vcheni-rady/disKhmyrov.pdf.

99. Шевченко С.О., Гаєвська Л.А. Інноваційні підходи до модернізації публічного управління у сфері забезпечення якості освіти в мережевому середовищі. URL: https://www.nayka.com.ua/index.php/dy/issue/archive.

100. Шеломенцев В. П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення // Вип. 2 (28). 2012. С. 299–309.

101. Шпига П., Рудник Р. Основні технології та закономірності інформаційної війни. Проблеми міжнародних відносин. 2014. № 8. С. 326–339.

102. Щепанський Е.В. Державне управління соціально-економічними ризиками: парадигма сутнісно-організаційних аспектів в умовах діджиталізації // Експерт: парадигми юридичних наук і державного управління. 2021. URL: https://journals.maup.com.ua/index.php/expert/article/view/1927.

103. Щепанський Е.В. Public Management of Socio-Economic Risks: A Paradigm of Essential Organizational Aspects in the Conditions of Digitalization. URL: http://ena.lp.edu.ua:8080/bitstream/ntb/28224/1/011-044-047.pdf.

104. Яровий Т.С. Концептуальні засади лобіювання як інструмент реалізації цілей державної безпеки // Інвестиції: практика та досвід. 2020. № 2. С. 99–103.

105. 3D Printing Trends 2019. Hubs. URL: https://www.3dhubs.com/get/trends.

106. 5g Readiness Index Report. URL: https://www.incites.eu/incites-map/Europe_5G_Readiness_Index_Report.pdf.

107. Ahmed W., Ameen K. Defining big data and measuring its associated trends in the field of information and library management // Library Hi Tech News. 2017. Vol. 34, issue 9. P. 21–24.

108. Akerman A., Gaarder I., Mogstad M. The Skill Complementarity of Broadband Internet // The Quarterly Journal of Economics. 2015. Vol. 130. № 4. P. 1781–1824.

109. Alter S., Sherer S. A general, but readily adaptable model of information system risk // Communications of the association for information systems. 2004. Vol. 14, no. 1. P. 1–28.

110. Analyzing Affiliation Networks / J. Scott [et al.] // Handbook of Social Network Analysis. SAGE, 2015. P. 640.

111. Ang R., Goh D. H. Predicting juvenile offending: A comparison of data mining methods // International journal of offender therapy and comparative criminology. 2013. Vol. 57, no. 2. P. 191–207.

112. Aradau C., Munster R. van. Governing Terrorism through Risk: Taking Precautions, (Un)knowing the Future // European Journal of International Relations. 2007. Vol. 13, no. 1. P. 89–115.

113. Arterton F. C. Political Participation and «Teledemocracy» // PS: Political Science Politics. 1988. Vol. 21, №. 3. P. 620–627.

114. Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy / Y.K. Dwivedi [et al.] // International Journal of Information Management. 2019. Vol. 57. P. 101994.

115. Artificial Intelligence and National security, august 2020. p.3-4 // Congressional Research Service. Mode of access:

https://fas.org/sgp/crs/natsec/R45178.pdf.

116. Artificial Intelligence and UK National Security: Policy Considerations, from RUSI, 2020 // RUSI. URL: https://rusi.org/publication/occasional-papers/artificial-intelligence-and-uk-national- security-policy-considerations.

117. Artificial Intelligence for the American People //White House USA - 2019- Mode of access: https://trumpwhitehouse.archives.gov/ai/.

118. Artificial Intelligence Index 2018 Annual Report // Stanford – 2018 - Mode of access: https://hai.stanford.edu/ai-index-2018.

119. Artificial intelligence in Swedish business and society Analysis of development and potential URL: https://www.vinnova.se/contentassets/ 29cd313d690e4be3a8d861ad05a4ee48/vr_18_09.pdf.

120. Artificial intelligence (AI) in Sweden 2019. URL: https://www.scb.se/en/finding-statistics/statistics-by-subject-area/education-and-research/research/research-and-development-in-sweden/pong/statistical-news/artificial-intelligence-ai-in- sweden-2019/.

121. Artificiell intelligens i Sverige URL: https://www.scb.se/contentassets/4d9059ef459e407ba1aa71683fcbd807/uf0301_2019a01_br_xftbr2001.pdf.

122. AI Using Standards of Mitigate Risk» Public-private analytic exchange program 2018. US Department of Homeland Security and Office of the Director of National Intelligence United States of America. Official website of the Department of Homeland Security. URL: https://www.dhs.gov/sites/ default/files/publications/2018_AEP_Artificial_Intelligence.pdf.

123. AI Sweden. URL: https://www.ai.se/en/about-aisweden/our-story.

124. Analyzing Affiliation Networks / J. Scott [et al.] // Handbook of Social Network Analysis. SAGE, 2015. P. 640.

125. Annual report for state-owned enterprises 2019. Report from Ministry of Enterprise and Innovation URL: https://www.government.se/

reports/2020/09/annual-report-for-state-owned-enterprises-2019/.

126. Anshari M., Alas Y. Smartphones habits, necessities, and big data challenges // Journal of High Technology Management Research. 2015. Vol. 26, issue 2. P. 177–185.

127. Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It, from Harvard Kennedy School. Belfer Center for Science and International Affairs, 2019 // Belfer Center, Harvard Kennedy School URL: https://www.belfercenter.org/sites/default/files/2019-08/AttackingAI/AttackingAI.pdf.

128. Ayoub K., Payne K. Strategy in the age of artificial intelligence // Journal of strategic studies. 2016. Vol. 39. P. 793–819.

129. Baldwin D. Security studies and the end of the Cold War // World politics. 1995. Vol. 45. P. 117–141.

130. Baldwin D. The concept of security // Review of international studies. 1997.Vol. 23. P. 5–26.

131. Balzacq T. Securitization theory. London: Routledge, 2011. 272 p.

132. BBVA Research analyzes 99 countries by digitalization index (https://www.bbva.com/en/which-countries-are-the-most-digitally-advanced/); Bloomberg's primary research service (BNEF) analyzes the industrial digitalization of 40 countries (https://about.bnef.com/blog/bloombergnefs-country-ranking-reveals-models-industrial-digitalization/); as part of the Digital Economy project, almost all UN member countries are analyzed.

133. Benkler Y. The wealth of networks: How social production transforms markets and freedom. Yale University Press, 2006. 528 p.

134. Beniger J. The Control Revolution. Harvard University Press, 1986. 508 p.

135. Berger S., Denner M. S., Roglinger M. The Nature of Digital Technologies - Development of a Multi-layer Taxonomy // Proceedings of the 26th European Conference on Information Systems (ECIS). 2018. P. 1–18.

136. Betz D J., Stevens T. Analogical reasoning and cyber security // Security Dialogue. 2013. Vol. 44(2). P.147-164.

137. Bonacich P. Power and Centrality: A Family of Measures // American Journal of Sociology. 1987. Vol. 92, no. 5.

138. Building an AI World: Report on National and Regional AI Strategies // Cifar. – 2018. Mode of access: https://www.cifar.ca/cifarnews/2018/12/06/building-an-ai-world-report-on-national-and-regional-ai-strategies.

139. Bimber B., Flanagin A., Stohl C. Collective Action in Organizations: Inter- action and Engagement in an Era of Technological Change. Cambridge University Press, 2012. 240 p.

140. Black D., Bissessar Ch., Boolaky M. Online Education as an Opportunity Equalizer: The Changing Canvas of Online Education // Interchange. 2019. Vol. 50. № 3. P. 423–443.

141. Blockchain&Cryptocurrencies Regulation Index URL: https://doingcrypto.org.

142. Breyer-Maylander T. Management 4.0 – Den digitalen Wandel erfolgreich meistern. Carl Hanser Verlag GmbH Co. 2017. 408p.

143. Brown D. Electronic government and public administration // International Review of Administrative Sciences. 2005. Vol. 71, Is. 2. P. 241–254.

144. Brose C. The new revolution in military affairs: War's sci-fi future // Foreign affairs. 2019. Vol. 98, no. 4.

145. Brozek B., Janik B. Can artificial intelligences be moral agents? // New ideas in psychology. 2019. Vol. 54. P. 101–106.

146. BSA Global Cloud Computing Scorecard 2018. URL https://cloudscorecard.bsa.org/2018/pdf/BSA_2018_Global_Cloud_Scorecard.pdf.

147. Bulgurcu B., Cavusoglu H., Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness // MIS Quarterly. 2010. Vol. 34. P. 523–548.

148. Buzan B. People, states and fear. An agenda for international

security studies in the Post-Cold War Era. ECPR Press, 1991. 318 p.

149. Buzan B., Waever O., Wilde J. Security: a new framework for analysis. London: Lynne Rienner, 1998. 239 p.

150. Casarosa F. (2022). Cybersecurity certification of Artificial Intelligence: a missed opportunity to coordinate between the Artificial Intelligence Act and the Cybersecurity Act. International Cybersecurity Law Review. 3 (1). Pp. 115–130.

151. Castells. The new public sphere: Global civil society, communication net- works, and global governance // The Annals of the American Academy of Political and Social Science. 2008. Vol. 616, Issue. 1. P. 78–93.

152. Carrizales T. Critical Factors in an Electronic Democracy: a Study of Municipal Managers // Electronic Journal of E-Government. 2008. Vol. 6, Is. 1. P. 23–30.

153. Cyber Threat // Impreva. URL: https://www.imperva.com/cyber-threat-index/.

154. Cybern Risk // Trend Micro. URL: https://www.trendmicro.com/ en_hk/security-intelligence/breaking- news/cyber-risk-index.html.

155. Cybersecurity: Let’s get tactical. // TechRepublic. URL: https://www.techrepublic.com/resource-library/whitepapers/cybersecurity-let-s-get-tactical-free- pdf/?ftag=CMG-01-10aaa1b.

156. Competition and transmission evolution of global food trade: A case study of wheat / C. Dong [et al.] // Physica A: Statistical Mechanics and Its Applications. 2018. Vol. 509. P. 998–1008.

157. Composite Index of National Capability // The Correlates of War Project. URL: https://correlatesofwar.org.

158. Collier J. Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision // Politics and Governance, 2018. Vol. 6(2). pp.13-21.

159. Cortez N. Patients Without Borders: The Emerging Global

Market for Patients and the Evolution of Modern Health Care // Indian Law Journal. 2008. Vol. 83. P. 71–113.

160. Cronin A. How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns. Princeton University Press, 2009. 336 p.

161. Chen P. Australian Politics in a Digital Age. Australia, New Zealand School of Government: ANU Press, 2013. 268 p.

162. Chen D.L., Eagel J. Can machine learning help predict the outcome of asylum adjudications? // Proceedings of the ACM Conference on AI and the Law. 2017. P. 237–240.

163. Clark, David; Regan, Patrick, 2016, "Mass Mobilization Protest Data", Harvard Dataverse, V5. URL: https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/HTTWYL.

164. Coglianese C., Lehr D. Regulating by robot: Administrative decision making in the Machine-learning era // Georgetown law journal. 2017. P. 1734.

165. Criminal Compliant // The United States Department of Justice. URL: https://www.justice.gov/ sites/default/files/opa/press-releases/ attachments/2015/03/30/criminal_complaint_force. pdf.

166. Cocelli M., Arkin E. A threat evaluation model for small-scale naval platforms with limited capability // EEE Symposium Series on Computational Intelligence. 2017. P. 1–8.

167. Composite Index of National Capability // The Correlates of War Project. – Mode of access: URL: https://correlatesofwar.org.

168. Cloud computing services Data from Knoema Database. URL: https://knoema.com/isoc_cicce_use-20171214/cloud-computing-services.

169. Crunchbase database. Наприклад дані по компанії Century Analytics. URL: https://www.crunchbase.com/organization/century-analytics.

170. Dataset for this research with raw data located on an open repository GitHub URL: https://github.com/AlTurobov/Data_Network-

Analysis_Digital-Competition.

171. Deshmuhk A.A Framework for Online Internal Controls // AMCIS August. 2004. P. 4471–4479.

172. Decision support system for optimum decision making process in threat evaluation and weapon assignment: Current status, challenges and future directions / A. Naseem [et al.] // Annual Reviews in Control. 2017. Vol. 43. P. 169–187.

173. Disinformationindex. URL: https://disinformationindex.org.

174. Devereux S., Vincent K. Using technology to deliver social protection: exploring opportunities and risks // Development in practice. 2010. Vol. 20, no. 3. P. 367–379.

175. Digital Economy and Society Index 2019. European Commission URL: https://digital-agenda-data.eu/datasets/desi/visualizations.

176. Dreshpak V.M., Kovalov V.G., Babachenko N.V., Pavlenko E.M. (2020) Communicative policy of public authorities in european countries: comparative analysis, International Journal of Management, Vol. 11, Iss. 06, pp. 529-543.

177. DRMKC – INFORM. Europian commission. URL: https://drmkc.jrc.ec.europa.eu/inform-index/INFORM-Risk/Results-and-data/moduleId/1782/id/419/controller/Admin/action/Results.

178. Feld S. L. The Focused Organization of Social Ties // American Journal of Sociology. 1981. Vol. 86, no. 5.

179. Fioramonti L., Kononykhina O. Measuring the Enabling Environment of Civil Society: A Global Capability Index // Voluntas. 2015. Vol. 26. P. 466–487.

180. Floyd R., Matthew R. A. Environmental security: approaches and issues // Environmental security: approaches and issues. Routledge, 2013. P. 320.

181. Flew T. New Media: An Introduction. Oxford University Press, 2005. 280 p.

182. Framework for the identification and demand-orientated classification of digital technologies / A. Lipsmeier [et al.] // IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD). 2018. P. 186–194.

183. Future scenarios and challenges for security and privacy / M. Williams [et al.] // IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a Better Tomorrow. 2016. P. 1–6.

184. Galanos V. Artificial intelligence does not exist: Lessons from shared cog- nition and the opposition to the nature/nurture divide // IFIP Advances in Information and Communication Technology. 2018. Vol. 537. P. 15–25.

185. Garcia-Alonso M.D.C., Levine P. Chapter 29 Arms Trade and Arms Races: A Strategic Analysis // Handbook of Defense Economics. Elsevier, 2007. P. 941–971.

186. Gheciu A., Wohlforth W. The Oxford Handbook of International Security. Oxford, UK : Oxford University Press, 2018. 784 p.

187. Gelman A., Hill J., Vehtari A. Regression and Other Stories (Analytical Methods for Social Research). Cambridge University Press, 2020. 552 p. chapter 5.

188. Gibb S., Strimmer K. Differential protein expression and peak selection in mass spectrometry data by binary discriminant analysis // Bioinformatics. 2015. Vol. 31, no. 19. P. 3156–3162.

189. Globalization and environmental challenges: reconceptualizing security in the 21st century / H. G. Brauch [et al.]. Berlin: Springer Science, 2008. 1141 p.

190. Global Cybersecurity Index v.4 // The Telecommunication Development Sector (ITU-D). URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

191. Goddard S. E. Uncommon ground: Indivisible territory and the politics of legitimacy // International Organization. 2006. Vol. 60, no. 1. P. 35–68.

192. Going Digital in Sweden. OECD Reviews of Digital Transformation. URL: https://www.oecd.org/sweden/going-digital-in-sweden.pdf.

193. Global Connectivity Index 2019. Countries Profiles. Huawei URL: https://www.huawei.com/minisite/gci/en/country-profile.html.

194. Global statistic GSMA Intelligence. URL: https://www.gsmaintelligence.com.

195. Global Terrorism Database. URL: https://www.start.umd.edu/gtd/.

196. Gould R. V. Power and social structure in community elites // Social Forces. 1989. Vol. 68, no. 2. P. 531–552.

197. Goos M., Manning A., Salomons A. Explaining Job Polarization: Routine Biased Technological Change and Offshoring // American Economic Review. 2014. Vol. 104. № 8. P. 2509–2526.

198. Grant R., Verona G. What's holding back empirical research into organizational capabilities? Remedies for common problems // Strategic organization. 2015. Vol. 13, issue 1. P. 61–74.

199. Hanlon R., Christie K. In Freedom from Fear, Freedom from Want: An Introduction to Human Security. Toronto: University of Toronto Press, Higher Education Division, 2016. 288 p.

200. Hao X., An H., Sun X. amd Zhong W. The import competition relationship and intensity in the international iron ore trade: From network perspective // Resources Policy. 2018. Vol. 57. P. 45–54.

201. Hafner-Burton E. M., Kahler M., Montgomery A. H. Network Analysis for International Relations // International Organization. 2009. Vol. 63, no. 3. P. 559–592.

202. Highly Violent Conflict Probability. URL: https://drmkc.jrc.ec.europa.eu/inform-index/INFORM-Risk/Results-and-data/moduleId/1782/id/419/controller/Admin/action/Results.

203. Hoffman B. Inside Terrorism. Columbia University Press, 2006.

288 p.

204. Hoffman F. Conflict in the 21th Century: the Rise of Hybrid Wars. URL: http://www.projectwhitehorse.com/pdfs/ HybridWar_0108.pdf.

205. Hollis D.B. Why States need an International Law for Information Operations // Lewis and Clark Law Review. 2007. Vol. 11. № 4. P. 1023–1061.

206. Horowitz M. C. Artificial Intelligence, International Competition, and the Balance of Power // Texas National Security Review. 2018. Vol. 1. P. 37–57.

207. Edwards P. The closed world: computers and the politics of discourse in Cold War America. MIT Press, 1997. 468 p.

208. Enders W., Sandler T. The Political Economy of Terrorism. 1-nd. Cambridge University Press, 2006. 390 p.

209. Engin Z., Treleaven P. Algorithmic Government: Automating Public Services and Supporting Civil Servants in using Data Science Technologies // The Computer Journal. 2019. Vol. 62, Issue 3. P. 448–460.

210. ENISA (European Union Agency for Network and Information Security), National Cyber Security Strategies in the World. www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

211. European Commission. Thematic Paper “Creating Digital Strategies”. August 2018 For instance, The German Federal Government has issued a set of national strategies that outlines a roadmap for digital transformation. https://germandigitaltechnologies.de/national-strategies/.

212. European Parliament Research Service. Ten technologies which could change our lives: Political impacts and policy implementations. 2015. URL: https://www.europarl.europa.eu/EPRS/EPRS_IDAN_527417_ten_trends_to_change_your_life.pdf.

213. Everett M. G., Borgatti S. P. Extending Centrality // Models and Methods in Social Network Analysis (Structural Analysis in the Social Sciences).

Cambridge University Pressp, 2005. P. 57–76.

214. IMD World Digital Competitiveness Ranking 2019. Technological Framework Sub-factor. URL: https://www.imd.org/wcc/world-competitiveness-center-rankings/world-digital-competitiveness-rankings- 2019/.

215. In each test subject, there is theoretically no minimum or maximum score in PISA; rather, the results are scaled to fit approximately normal distributions, with means for OECD countries around 500 score points and standard deviations around 100 score points. About two-thirds of students across OECD countries score between 400 and 600 points. Less than 2percent of students, on average across OECD countries, reach scores above 700 points, and at most a handful of students in the PISA sample for any country reach scores above 800 points.URL: http://www.oecd.org/pisa/pisafaq/.

216. Indicator - Balanced International Trade in Services EBOPS 2010. URL: https://unstats.un.org/unsd/classifications/Family/Detail/101.

217. Industrial Robots – Statistics&Facts. Statista. URL: https://www.statista.com/topics/1476/industrial-robots/.

218. Information Economy Report: Digitalization, Trade and Development, (United Conference on Trade and Development, 2017), https://unctad.org/en/PublicationsLibrary/ier2017_en.pdf.

219. Interim Report, November 2019 // NSCAI. Mode of access: https://drive.google.com/file/d/153OrxnuGEjsUvlxWsFYauslwNeCEkvUb/view.

220. International Federation of Robotics. URL: https://ifr.org/worldrobotics.

221. International Telecommunication Union Statistic database. Individuals using the Internet 2005-2019. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

222. iSi. URL: http://www.pircenter.org/media/content/files/9/13462438640.pdf.

223. Janowski T. Digital government evolution: From transformation

to contextualization // Government Information Quarterly. 2015. Vol. 32, Issue. 3. P. 221–236.

224. Jarrahi M. Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making // Business horizons. 2018. Vol. 61, no. 4. P. 577–586.

225. Jarvis L., Lister M. Critical Perspectives on Counter-Terrorism. Routledge, 2015. 234 p.

226. Jho W., Song K. J. Institutional and technological determinants of civil e-Participation: Solo or duet? // Government Information Quarterly. 2015. Vol. 32, Issue. 4. P. 488–495.

227. Jensen K. B. Definitive and Sensitizing Conceptualizations of Mediatizaion // Communication Theory. 2013. Vol. 23, Issue 3. P. 203– 222.

228. Johnson E., Kolko B. E-government and Transparency in Authoritarian Regimes: Comparison of National-and City-Level E-government Web Sites in Central Asia // Studies in Russian, Eurasian and Central European New Media. 2010. No. 3. P. 15–48.

229. Johansson F., Falkman G. Comparison between two approaches to threat evaluation in an air defense scenario // Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics). 2008. Vol. 5285. P. 110–121.

230. IBM X-Force Threat Intelligence // IBM. URL: https://www.ibm.com/security/data- breach/threat-intelligence.

231. IMD World Digital Competitiveness Ranking 2019. Rank: Use of Big Data and analytics. URL: https://worldcompetitiveness.imd.org.

232. Kaplan A., Haenlein M. Siri, Siri, in my hand: Who’s the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence // Business Horizons. 2019. Vol. 62, no. 1. P. 15–25.

233. Karpf D. The MoveOn effect: The unexpected transformation of American political advocacy. Oxford University Press, 2012. 256 p.

234. Katz M.D., Bommarito M.J., Blackman J. A general approach for predicting the behavior of the Supreme Court of the United States // PLoS ONE. 2017. Vol. 12, no. 4. P. 1–18.

235. Kennedy D. The move to institutions // Cardoso law review. 1987. Vol. 8, no. 5. P. 841–988.

236. Keskinbora K. H. Medical ethics considerations on artificial intelligence // Journal of Clinical Neuroscience. 2019. Vol. 64. P. 277–282.

237. Kissell R., Malamut R. Algorithmic Decision-Making Framework // The Journal of Trading. 2005. Vol. 1. P. 12–21.

238. Klaver M.H.A., Luiijf H.A.M., Nieuwenhuijs A.H., Cavenne F., Ulisse A., Bridegeman G. European risk assessment methodology for critical infrastructures // 2008 First International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future, IEEE, Piscataway, New Jersey, USA, 10-12 November 2008, pp. 1–5.

239. Kumar S., Tripathi B. Modelling of Threat Evaluation for Dynamic Targets Using Bayesian Network Approach // Procedia Technology. 2016. Vol. 24. P. 1268–1275.

240. Lazega E., Wasserman S., Faust K. Social Network Analysis: Methods and Applications // Revue Fran ç aise de Sociologie. 1995. Vol. 36, vol. 4. P. 781–783.

241. Lee J., Long A., McRae M., Handler S. Bitcoin Basics: a Primer on Virtual Currencies // Business Law International. 2015. Vol. 16. № 1. P. 21.

242. Library of Congress. URL: https://www.loc.gov/search/?q=%22Artificial+intelligence%22&fa=original-format%3Alegislation&sb=date.

243. Liu Z., Chen H. A predictive performance comparison of machine learning models for judicial cases // IEEE Symposium Series on Computational Intelligence. 2018. P. 1–6.

244. Loebbeke C. Digitalisierung – Technologien und

Unternehmensstrategien. Handbuch Medienmanagement. Springer Verlag, 2006. 360 p.

245. Longino H. Individuals or populations? // Philosophy of social science: an introduction. Oxford university press, 2014. P. 102–120.

246. Loverace Test. URL: https://www.envisioning.io/vocab/lovelace-test.

247. Lum K., Isaac W. To predict and serve? // Significance. 2016. Vol. 13, no. 5. P. 14–19.

248. Mabee B. Security Studies and the Security State': Security Provision in Historical Context // International Relations. 2003. 17(2). pp.135-151.

249. Manoharan A., Carrizales T. J. Technological equity: An international perspective of e-government and societal divides // Electronic Government. 2011. Vol. 50, Issue 1. P. 56–66.

250. Marquardt K.L. How and how much does expert error matter? Implications for quantitative peace research // Journal of Peace Research. 2020. Vol. 57, no. 6. P. 692–700.

251. Martin K. Ethical Implications and Accountability of Algorithms// Journal of Business Ethics. 2018. Vol. 160. P. 835–850.

252. McClendon L., Meghanathan N. Using Machine Learning Algorithms to Analyze Crime Data // Machine Learning and Applications: An International Journal. 2015. Vol. 2, no. 1. P. 1–12.

253. Mead Earle E. Makers of Modern Strategy: Military Thought from Machiavelli to Hitler. Princeton: Princeton university press, 1944. 951 p.

254. Mergel, Edelmann, Haug. Defining digital transformation: 36, Issue 4. P. 101385.

255. Mikhaylov S.J., Esteve M., Campion A. Artificial intelligence for the public sector: Opportunities and challenges of cross-sector collaboration // Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences. 2018. Vol. 376, no. 2128. P. 1–21.

256. Ministry of Economic Affairs and Employment of Finland Report. URL: https://www.businessfinland.fi/496a6f/globalassets/julkaisut/digital-finland-framework.pdf.

257. Monitoring Progress in National Initiatives on Digitising Industry. Country Report Finland. July 2019. URL: https://ec.europa.eu/information_society/newsroom/image/document/2019-32/country_report_-_finland_-_final_2019_0D3030C8-E1C1-39A6-5D48192F99EE4DD4_61204.pdf.

258. Moustaka V., Theodosiou Z., Vakali A., Kounoudes A., Anthopoulos L. G. Enhancing social networking in smart cities: Privacy and security borderlines // Technological Forecasting and Social Change. 2019. Vol. 142. P. 285-300.

259. Naeem H., Masood A. An optimal dynamic threat evaluation and weapon scheduling technique // Knowledge- Based Systems. 2010. Vol. 23, Vol. 1. P. 337–342.

260. Nakaya T., Yano K. Visualising crime clusters in a space-time cube: An exploratory data-analysis approach using space-time kernel density estimation and scan statistics // Transactions in GIS. 2010. Vol. 14. P. 223–239.

261. Nance W. D., Straub D. W. An Investigation into the Use and Usefulness of Security software in Detecting Computer Abuse // ICIS 1988 Proceedings. 1998. Vol. 36. P. 283–294.

262. National approach to artificial intelligence. URL: https://www.government.se/4a7451/contentassets/fe2ba005fb49433587574c513a837fac/national- approach-to-artificial-intelligence.pdf.

263. National Cyber Strategy of the United States of America // The White House, September 2018. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

264. National Security Commission on Artificial Intelligence, Interim Report, 2019 // The National Security Comission on Artificial Intelligence

(NSCAI)– Mode of access: URL: https://www.

265. National Strategy: Digital Switzerland. URL: https://strategy.digitaldialog.swiss/en/.

266. Neack L. National, International, and Human Security: A Comparative Introduction. Lanham: Rowman Littlefield, 2017. 236 p.

267. Network feature and influence factors of global nature graphite trade competition / X. Wang [et al.] // Resources Policy. 2019. Vol. 60. P. 153–161.

268. Norris P. Virtual democracy // Harvard International Journal of Press/Politics. 1998. Vol. 3, no. 2. P. 1–4.

269. Nordic Foreign and Security Policy. Report from Ministry for Foreign Affairs. URL: https://www.government.se/reports/2020/07/nordic-foreign-and-security-policy-2020/.

270. Novikov V. Approaches to improvement of the institutional system and mechanisms of public administration in the conditions of information-hybrid wars // Eurasian Academic Research Journal. 2020. Vol. 37. Pp. 75-80.

271. Novikov V. Pomaza-Ponomarenko A., Taraduda D. Assessment of risks of ukraine's digital security as a component of information security in modern conditions // 5th international scientific conference „Euroatlantic security and policy of the russian federation" (05-06.06.2024, Poland).

272. O'Connell M.E. Cyber Security without Cyber War // Journal of Conflict Security Law. 2012. Vol. 17. № 2. P. 187–209.

273. Official site Government of the Netherlands. Dutch Digitalisation Strategy. URL: https://www.government.nl/documents/reports/2018/06/01/dutch-digitalisation-strategy.

274. Padgett J. F., Ansell C. K. Robust Action and the Rise of the Medici // American Journal of Sociology. 1993. Vol. 98, no. 6. P. 1400–1434.

275. Payne K. Artificial intelligence: A revolution in strategic affairs? // Survival. 2018. Vol. 60. P. 7–32.

276. Paret P., Craig G. A., Gilbert F. Makers of modern strategy from

Machiavelli to the Nuclear Age - Princeton University Press, 1986. 951p.

277. Parker G. The Military Revolution: Military Innovation and the Rise of the West. 2-nd. Cambridge: Cambridge University Press, 1996. 292 p.

278. Pape R. Dying to Win: The Strategic Logic of Suicide Terrorism. Random House Trade Paperbacks, 2006. 368 p.

279. Pencheva I., Esteve M., Mikhaylov S. J. Big Data and AI – A transformational shift for government: So, what next for research? // Public Policy and Administration. 2020. Vol. 35, vol. 1. P. 24–44.

280. Perspective on Issues in AI Governance report from Google // Google. Mode of access: https://ai.google/static/documents/perspectives-on-issues-in-ai-governance.pdf.

281. Piper A. “Risk-informed innovation. Harnessing risk management in the service of innovation”. 2014. URL: www.economistinsights.com/ technologyinnovation/analysis/risk-informed-innovation.

282. Pomaza-Ponomarenko A., Hren M., Durman O., Bondarchuk N., Vorobets V. Management mechanisms in the context of digitalization of all spheres of society // Revista San Gregorio. SPECIAL EDITION-2020. Núm. 42. URL: http://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/issue/view/ RSAN42/showToc.

283. Pomaza-Ponomarenko A., Kryvova S., Hordieiev A., Hanzyuk A., Halunko O. Innovative Risk Management: Identification, Assessment and Management of Risks in the Context of Innovative Project Management // Economic Affairs (New Delhi). 2023, 68(4), pp. 2263–2275. DOI: 10.46852/0424-2513.4.2023.34. URL: https://ndpublisher.in/admin/issues/EAv68n5z8.pdf.

284. Pomaza-Ponomarenko A., Taraduda D., Leonenko N., Poroka S., Sukhachov M. Ensuring the safety of citizens in times of war: aspects of the organization of civil defense // AD ALTA: Journal of Interdisciplinary Research. 2024. Volume 14. Issue 1. Pp. 216–220.

285. Pool I. S. Technologies of Freedom. Harvard University Press,

1984. 299 p.

286. Powering European public sector innovation Towards a new architecture: report of the expert group on public sector innovation». URL: https://op.europa.eu/en/publication-detail/-/publication/6e9860e0-6b28-463b-8ecf-e86ec826e308.

287. Predicting judicial decisions of the European court of human rights: A natural language processing perspective / N. Aletras [et al.] // PeerJ computer science. 2016. Vol. 2. P. 93.

288. PWC. Dutch Innovation Survey. Digital Transformation. Netherlands 2018. URL: https://www.pwc.nl/en/insights-and-publications/themes/ digitalization/dutch-innovation-survey/digital- transformation.html.

289. Radchenko O., Kriukov Kovach V. ext of “Civilizations Clash” as the Main Object of Infovation War in Ukraine. In: Radchenko O., Kovach V., Semenets-Orlova, I., Zaporozhets, A. (eds) National Security Drivers of Ukraine. (2023) Contributions to Political Science. Springer, Cham. https://doi.org/10.1007/978-3-031-33724-6_18. pp. 301-316.

290. Race to 5g Report. CITA. URL: https://www.ctia.org/news/race-to-5g-report.

291. Reis J., Santo P. E., Melao N. Artificial Intelligence in Government Services: A Systematic Literature Review // Advances in Intelligent Systems and Computing. 2019. Vol. 930. P. 577–586.

292. Rinaldi S.M., Peerenboom J.P., Kelly T.K. Identifying, understanding, and analyzing critical infrastructure interdependecies // IEEE Control Systems Magazine. 2001. Vol. 21. Iss. 6. P. 11–25.

293. Regulation (EC) № 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) № 526/2013 (Cybersecurity Act) // Official Journal of the European Union L 151 of 7 June 2019.

294. Review of Controls for Certain Emerging Technologies A Proposed Rule by the Industry and Security Bureau on 11/19/2018 // Federal register. – Mode of access: https://www.federalregister.gov/documents/ 2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies.

295. Report «Building an AI World: Report on National and Regional AI Strategies» // Cifar – 2018. Mode of access: https://www.cifar.ca/cifarnews/2018/12/06/building-an-ai-world-report-on-national-and-regional-ai-strategies.

296. Rodan S. A. Choosing the Beta Parameter When Using the Bonacich Power Measure // Journal of Social Structure. 2011. Vol. 12, Vol. 1. P. 1–23.

297. Ronca M., Ross B., Dodd E. Digital justice: online learning beyond COVID-19 // UTS Centre for Social Justice & Inclusion Newsroom. URL: https:// www.uts.edu.au/partners-and-community/initiatives/ social-justice-uts/news/digital-justice-online-learningbeyond-covid-19.

298. Rose J., Flak L. S., Saebo O. Stakeholder theory for the E-government context: Framing a value-oriented normative core // Government Information Quarterly. 2018. Vol. 35, Issue 3. P. 362–374.

299. Russell S., Norvig P. Artificial Intelligence A Modern Approach. Pearson Education Inc., 2010. 1132 p.

300. Sageman M. Leaderless Jihad: Terror Networks in the Twenty-First Century. University of Pennsylvania Press, 2008. 208 p.

301. Sassen S. Globalization and its discontents: Essays on the new mobility of people and money. New Press, 1998. 288 p.

302. Schlag G., Junk J., Daase C. Transformations of security studies: dialogues, diversity and discipline. Routledge. 2015. P.250:2

303. Schinagl S., Shahim A. What do we know about information security governance? “From the basement to the boardroom”: towards digital security governance // Information & Computer Security. 2020. 28(2). pp. 261-292.

304. Schuh G., Klappert G. Technologiemanagement – Handbuch Produktion und Managemen. Springer Verlag, 2011. P. 17-34.

305. Sharre P. Killer apps: The real dangers of an AI arms race // Foreign Affairs. 2019. 236 p.

306. Shabtai S. Israel's national security concept: new basic terms in the military-security sphere // Strategic Assessment. 2010. 13(2). pp. 8-10.

307. Shih H. Y., Chang T. L. S. International diffusion of embodied and disembodied technology: A network analysis approach // Technological Forecasting and Social Change. 2009. Vol. 76, no. 6. P. 821–834.

308. Siponen M. T., Oinas-Kukkonen H. A review of information security issues and respective research contributions // ACM SIGMIS Database: the DATABASE for Advances in Information Systems. 2007. Vol. 38(1). P.60-80.

309. SIPRI Military Expenditure Database.URL: https://www.sipri.org/databases/milex.

310. SIPRI Arms Transfers Database. Supplier. URL: https://www.sipri.org/databases/armstransfers.

311. Statistical modeling, causal inference and social science\newline. URL: https://statmodeling.stat.columbia.edu/2011/08/13/checking_your_m/.

312. Storsul T. adn Fagerjord A. Digitization and Media Convergence // International Encyclopedia of Communication. 2008. P. 1319–1323.

313. Sveriges Riksdag. URL: https://www.riksdagen.se/sv/global/sok/?q=&doktyp=sfs.

314. Synchronous Big Data analytics for personalized and remote physical therapy / P. Calyam [et al.] // Pervasive and Mobile Computing. 2016. Vol. 28. P. 3–20.

315. Syvak T., Vorona P., Nesteriak Y., Paliukh V., Dakal A. Current State of Strategic Communications in Ukraine and Their Functional Influence on Efficiency of State Management System // Contributions to Political Science.

2023. art F1367, pp. 167–182.

316. Schnaufer TadA. II. Redefining Hybrid Warfare: Russia's Non-linear War against the West. Journal of Strategic Security, Vol. 10, No. 1 (Spring 2017), pp. 17–31. URL: https://www.jstor.org/stable/26466892.

317. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd edition / ed. by M.N. Schmitt. CUP. 2017. Pp. 11–16.

318. Tene O., Polonetsky J. Taming The Golem: Challenges of Ethical Algorithmic Decision-Making // North Carolina Journal of Law and Technology. 2016. Vol. 19. P. 125–173.

319. The 2019 AI Index report. Human-Centered Artificial Intelligence. Stanford University URL: https://hai.stanford.edu/ai-index/2019.

320. The structure and knowledge flow of building information modeling based on patent citation network analysis / Y. N. Park [et al.] // Automation in Construction. 2018. Vol. 87. P. 215–224.

321. The ethics of algorithms: Mapping the debate / B.D. Mittelstadt [et al.] // Big Data and Society. 2016. Vol. 3, no. 2. P. 1–21.

322. The Ultimaker 3D Printing Sentiment Index. URL: https://3d.ultimaker.com/Ultimaker-3D-Printing-Sentiment-Index.

323. The EU Counter-Terrorism Policy Responses to the Attacks in Paris: Towards an EU Security and Liberty Agenda / D. Bigo [et al.] // CEPS Liberty and Security in Europe. 2015. Vol. 81. P. 1–28.

324. The Militarization of Artificial Intelligence August 2019 // United Nations, New York, NY. Mode of access: https://www.un.org/disarmament/the-militarization-of-artificial-intelligence/ .

325. The National Security Commission on Artificial Intelligence. p. 7 // The National Security Commission on Artificial Intelligence (NSCAI) – Mode of access: https://www.nscai.gov/home.

326. To study the technological network by structural equivalence / C. S. Weng [et al.] // Journal of High Technology Management Research. 2010.

Vol. 21, no. 1. P. 52–63.

327. Trade-off Across Privacy, Security and Surveillance in the Case of Metro Travel in Europe / S. Patil [et al.] // Transportation Research Procedia. 2014. Vol. 1, no. 1. P. 121–132.

328. Transforming Singapore Through Technology. Nation strategy Smart Nation. Official site URL: https://www.smartnation.sg.

329. Trombley S. Managing your information risk // Computer Fraud and Security. 2015. Vol. 2015, vol. 7. P. 5–9.

330. United Nations. Department of Economic and Social Affairs. UN E-Government Surveys (2001-2018). URL: https://publicadministration.un.org/en/Research/UN-e-Government-Surveys.

331. United Nations. Digital Economy Report 2019. URL: https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=2466.

332. US Department of Defense (2010) Quadrennial Defense Review Report. Washington, DC: US Department of Defense.

333. U.S. LEADERSHIP IN AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools: Prepared in response to Executive Order 13859 Submitted on August 9, 2019 // National Institute of Standarts and Technology (NIST) – 2019 -Mode of access: https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.

334. UN E-Government Survey 2018. URL: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018.

335. United Nations. Digital Economy Report 2019. URL: https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=2466.

336. Universes. URL: https://univrses.com/about-us/.

337. Vacca W., Davidson M. The Regularity of Irregular Warfare. Parameters, 2011, vol. 41, issue 1, pp. 18-34.

338. Vallverdu J. The emotional nature of post-cognitive

singularities // The Technological Singularity, The Frontiers Collection. Springer-Verlag, 2017. P. 193–208.

339. Varieties of Democracy (V-Dem). База даних «Country-Year: V-Dem Full+Others». Regimes of the world – the RoW measure (D) (v2x_regime). URL: https://www.v-dem.net/en/data/data/v-dem-dataset-v111/.

340. Van Dijk J. The Network Society: Social Aspects of New Media. SAGE Publications Ltd, 2005. 272 p.

341. Veale M., Borgesius, F.Z. (2021). Demystifying the Draft EU Artificial Intelligence Act – Analysing the good, the bad, and the unclear elements of the proposed approach. Computer Law Review International. 22 (4). Pp. 97–112.

342. Vydra S., Klievink B. Techno-optimism and policy-pessimism in the public sector big data debate // Government Information Quarterly. 2019. Vol. 36, no. 4. P. 101383.

343. Wachal R. Humanities and Computers // The North American Review (New). 1971. P. 30–32.

344. Wang W., Li Z., Cheng X. Evolution of the global coal trade network: A complex network analysis // Resources Policy. 2019. Vol. 62. P. 496–506.

345. Watson R.T., Mundy B.A strategic perspective of electronic democracy // Communications of the ACM. 2001. Vol. 44, Issue 1. P. 27–30.

346. Whitman M. E., Mattord H. J. Principles of Information Security. 4-nd. Cengage Learning, 2011. 656 p.

347. WIPO IP Portal. Global Brand Database. URL: https://branddb.wipo.int/branddb/en/

348. WIPO IP Statistics Data Center. WIPO Statistic database. Patents grants by Technology. Total count by applicant's origin. 2018 Digital Technology. Last updates: October 2019. URL: https://www3.wipo.int/ipstats/index.htm?tab=patent.

349. WTO. URL: https://data.wto.org.

350. Wither James K. Making Sense of Hybrid Warfare. Connections. 2016. Vol. 15. No. 2. P. 73–87. URL:https://www.jstor.org/stable/26326441.

351. World Bank Group Report Cryptocurrencies and Blockchain 2018. URL: http://documents.worldbank.org/curated/en/293821525702130886/ pdf/Cryptocurrencies-and- blockchain.pdf.

352. Wolfers A. «National Security» as an Ambiguous Symbol // Political Science Quarterly. 1952. Vol. 67, no. 4. P. 481–502.

353. Zhang H. Y., Ji Q., Fan Y. Competition, transmission and pattern evolution: A network analysis of global oil trade // Energy Policy. 2014. Vol. 73. P. 312–322.

354. Zarsky T. The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making // Science Technology and Human Values. 2016. Vol. 41, P. 118–132.

355. Zegart A., Morell M. Spies, lies, and algorithms: Why U.S. Intelligence agencies must adapt or fail // Foreign Affairs. 2019. Vol. 3.

Додаток 1

Концептуальне обґрунтування теоретичних засад pre-research

Основою дослідження є розгляд цифрових технологій як ресурсів, і відповідно розгляд конкуренції країн у сфері цифровізації за допомогою мережного аналізу. Мережевий підхід визначає структури як інтеграційні властивості (emergent properties) постійних патернів у відносинах між агентами (акторами), які можуть визначати, включати й обмежувати цих агентів (акторів) [201]. З погляду мережевого аналізу, переконання та дії окремих агентів не є незалежними.

Комбінація величини та частоти взаємодії між двома вузлами мережі (вузлами можуть бути представлені: актори, організації, інститути, країни тощо) показує потенціал взаємозв'язку. Розподіл зв'язків у мережі передбачає дві важливі структурні характеристики: центральність (важливість) вузлів у мережі та розподіл мережі на підгрупи. Варіанти центральності в мережі включають класичний ступінь (Degree centrality), близькість (Closeness centrality) і проміжки (Betweenness centrality) [213], а також численні варіації центральності й унікальні підходи для конкретних завдань.

Ступінь центральності (Degree centrality) вузла – це сума значень зв'язків між цим вузлом та кожним іншим вузлом у мережі. Цей показник вказує яку доступність має певний вузол по відношенню до інших вузлів. Центральність близькості (Closeness centrality) обчислюється з використанням довжини шляху між вузлом та кожним іншим вузлом. Цей захід відображає час, необхідний для поширення інформації або ресурсів для даного вузла в мережі. Центральність проміжності (Betweenness centrality) відповідає кількості найкоротших шляхів у мережі, які проходять через попередньо визначений вузол, і, отже, вимірює залежність мережі від конкретного вузла підтримки можливості зв'язків.

Центральність власного вектора (Eigenvector centrality), часто у наукових дослідженнях пов’язують із визначенням становища влади, і включає як кількість зв’язків вузла, так і силу цих зв’язків, але й центральність цих інших вузлів [137].

Структура мережі може визначати ефективність у розподілі інформаційних чи матеріальних ресурсів, і навіть здатність протистояти загрозам порушення. У контексті міжнародних відносин учені Е. Хафнер-Бертон та А. Монтгомері [201] вказують, що більш високий ступінь централізації в міжнародній системі дозволяє аналізувати конфлікти, та позицію влади конкретних країн щодо забезпечення розвитку цифрових технологій. Привілейовані позиції (або «центральні» у мережевому аналізі) у світовій політиці можуть визначати порядок денний, формулювати дебати та проводити політику, яка приносить їм користь. Понад те, визначення позиції суб’єктів (країн, організацій) дозволяють аналізувати можливості впливу суб’єктів у структурі мережі. Мережеві структури та зв’язки також створюють поведінкові очікування: очікується, що держави відіграватимуть певну роль у певних позиціях. Вузол, який відіграє опосередковану функцію, може отримати вплив завдяки своїй центральності (що визначається як betweeneess centrality), оскільки він може забезпечити єдині зв'язки з більшою мережею. Власне кажучи, вплив є продуктом зв’язку з іншими центральними вузлами [191; 196; 274].

Таким чином, мережевий аналіз дозволяє розглянути структуру міжнародних відносин між країнами щодо інформації, ресурсів, торговельних відносин тощо. Тоді виникають запитання. Чи можемо ми простежити взаємозв’язок країн щодо поширення (і конкуренції) цифрових технологій, чи можемо ми отримати нові знання про цифрові технології в контексті мережевої взаємодії країн.

Сучасні дослідження показують, що цифровізація системи публічного управління еволюціонувала та створила складну структуру, що позначається на системі національної безпеки. Аналіз такого еволюційного процесу

можливий завдяки вивченню: 1) доступності цифрових технологій; 2) впровадження цифрових технологій; 3) інституціоналізації методів цифрового управління; 4) визначення ключових технологій, їх ролі та значущості, а також урахування технологічної взаємодії в єдиній концепції [223]. Мережевий аналіз дозволяє здійснити аналіз не лише системи організацій, політичних та соціальних суб'єктів (акторів), але й створити мережі ресурсів та інформації, чи технологій [307].

В аналізі соціальних мереж термін «афіліація» (affiliations) зазвичай відноситься до даних про членство або участь. У деяких випадках метою збору даних про афілійованість є не розуміння структури зв'язків між двома наборами, а розуміння структури зв'язків усередині одного з наборів [124]. Власне кажучи, деякі обставини вимагають аналізу відносин «всередині» певного набору даних. Іноді неможливо отримати дані про стан функціонування тієї чи іншої сфери суспільної життєдіяльності. У таких ситуаціях можливе формування набору даних. Таким чином, можна побудувати зв'язки між членами набору вузлів шляхом визначення спільної приналежності як зв'язку (наприклад, участь у тому заході, членство у тому самому корпоративному правлінні) [178].

Застосовуючи логіку аналізу мереж аффіліацій (affiliate networks) цього дослідження, можемо розглядати країни як учасників (вузли), які мають спільні зв'язки (ties), виражені з погляду їх використання цифрових технологій. Іншими словами, використання у країні певної технології демонструє її «участь» у певній групі країн, що розвивають та (або) застосовують конкретну цифрову технологію.

Теоретичне вивчення технології з використанням мережного аналізу дозволяє також визначити роль і місце конкретних типів технологій у єдиній структурі. Згідно з теорії поля, а також концепцією технологічної парадигми та технологічних траєкторій, запропонованої у 1982 р., технології центральних позицій мають більше можливостей стати домінуючим зразком і відігравати провідну роль у процесі розвитку технологій. Технології на

периферії мережного взаємозв'язку грають роль послідовників, і навіть схильність до розробки допоміжних технологій за основним напрямом розвитку [326].

Мережевий характер дослідження заснований на двох аспектах [124]: 1) ко-афіліація створює умови для розвитку різного роду зв'язків; 2) загальні афіліації можуть бути наслідком зв'язку.

Таким чином, коафіліація може розглядатися як прояв відносин, який, можливо, безпосередньо не спостерігається. У цьому дослідженні аналіз відносин між державами-членами ООН ґрунтується на впровадженні на їх території різних цифрових технологій. Наявність конкретної цифрової технології дозволяє допустити, що країна так чи інакше взаємодіє з іншою країною зі схожими технологіями в галузі досліджень, торгівлі, розвитку тощо. Це підтверджується дослідженнями з поширення технологий [307], і навіть сучасними феноменами науково-технічної взаємодії між державами (від академічної мобільності до санкцій).

Дані були зібрані для всіх 193 країн-членів ООН. Розвиток цифрових технологій неможливий без телекомунікаційної інфраструктури, технологічної бази (technological framework) та використання Інтернету. З цієї причини в основі даного дослідження знаходяться дані індексів країн ООН, що включають чотири основні показники: TII – індекс телекомунікаційної інфраструктури (telecommunication infrastructure index388), UI – використання Інтернету (use of the Internet), IDT – інтеграція цифрових технологій (Integration of Digital Technology), TF – технологічні основи (Technological Framework). Таблиця нижче демонструє підхід до збору даних на прикладі трьох країн за прикладом матриці даних:

Країна	TII	UI	IDT	DCT(p)	CT(p)	TF	BD	AI	IoT	AR	3Dp	VCB	CC	5g
Велика Британія	0.8	94.9	0.52	797	1407	18	5.35	31.7	57		114.7	7.31	24.9	66.8
Танзанія	0.14							18	21					
США	0.75	87.3		24444	38232	11	6.19	50.41	69	200	113.5	6.04	18	87

Матриця даних містить показники по конкретній країні за рядками, та показники для конкретного типу технології у стовпцях. У першому стовпці показані країни (наприклад, Сполучене Королівство Великобританії та Північної Ірландії, Об’єднана Республіка Танзанія та Сполучені Штати Америки), у другому стовпці – показник індексу телекомунікаційної інфраструктури ООН, у третьому – використання Інтернету, у четвертому – інтеграція цифрових технологій тощо. Дані використання Інтернету (UI) були структуровані з бази даних International Telecommunication Union [221]. Дані технологічної основи як для бізнесу, так і для уряду відображені в індикаторі Технологічної основи (TF) з IMD World Digital Competitiveness Ranking 2020 [231]. ІКТ – як загальна тенденція для країн – ілюструє зміни в галузі цифровізації та трансформації бізнесу та готовності уряду до використання технологій оцінюється за допомогою стандартної концепції інтеграції цифрових технологій. Індикатор інтеграції цифрових технологій (IDT) було взято зі звіту Європейської комісії (Індекс цифрової економіки та суспільства 2020» [175]).

Дотримуючись логіки побудови комплексної мережевої взаємодії, необхідно враховувати показники патентної активності країн. Для цього в базі даних Всесвітньої організації інтелектуальної власності було відібрано два основні патенти, що належать до цифрових технологій: патенти на технології цифрового зв'язку (Digital Communication Technology Patents [175; 348]) та патенти на комп’ютерні технології (Computer Technology Patents [348]). Звичайно, аналіз патентів та цитування патентів має численні обмеження: наявність патенту не свідчить про фактичне впровадження технології у країні. Проте два типи патентів були додані для конкретної мети повного охоплення поширення цифрових технологій.

Наступне заповнення набору даних здійснювалося із формуванням індикаторів для конкретних цифрових технологій. Це дозволить виділити список «трендових» технологій для країн, спираючись на два документи: звіт Європейської парламентської дослідницької служби «Ten technologies which

could change our lives: Political impacts and policy implementations» [212] та «Digital Economy Report» [335].

Аналіз даних [170] для мережевого аналізу складається з чотирьох загальних показників, двох індикаторів патентів: DCT.p – патенти на цифрові комунікаційні технології, CT.p – патенти на комп'ютерні технології та вісім індикаторів для кожного типу цифрових технологій: BD – великі дані, AI – штучний інтелект, IoT – інтернет речей, AR – автоматизація та робототехніка, 3Dp – 3D-друк, VCB – віртуальна валюта та блокчейн, CC – Хмарні обчислення та 5g.

Створена матриця даних показує, які типи цифрових технологій використовують чи застосовуються країнами, зокрема, у напрямку забезпечення національної безпеки. Рядки відповідають країнам, а стовпці – типу використовуваної технології. Логіка дослідження, представлена вище, має на увазі, що володіння (використання) технології в одній країні формує зв'язок з іншою країною, що також використовує технологію того ж типу.

Підготовка даних для мережного аналізу включає такі етапи:

1) приведення даних до структури мережного аналізу;

2) транспонування матриці для отримання мережі технологій;

3) округлення показників;

4) матрична дихотомізація за допомогою підходу до оптимізації з використанням оптимальних порогів [188]. Суть цього підходу полягає у максимізації взаємної інформації між відповідями для кожної змінної. Після дихотомізації вносимо матрицю до структури графів, тоді дані будуть готові до аналізу мережі.

Зазначені етапи спрямовані на підготовку даних для мережевого аналізу, які слід конвертувати в коафіліаційну матрицю (країни – типи технологій). Таким чином, можна отримати мережу країн, де матриця коафіліації (спільної приналежності за країнами) демонструє кількість технологій, які країни використовують спільно. «Вузол» (node) - це

конкретна країна; зв’язки (ties) надають інформацію щодо показника кількості найпоширеніших видів технологій. Так само можна створити мережу технологій, в якій матриця коафіліації (матриця: технологія на технологію) демонструє кількість країн, які використовують конкретну технологію. У цьому випадку вузол (node) є типом цифрової технології, а кількість зв’язків (ties) – це число країн, які використовують цю технологію.

Спочатку побудуємо мережі цифрових технологій з ілюстрацією чотирьох найпопулярніших типах центральностей: Degree, Closeness, Eigenvector [320] і Betweenness [240]: прямі та непрямі зв’язки. Eigenvector centrality – це головний власний вектор матриці суміжності, що визначає мережу. Ключова ідея цього заходу центральності у тому, що значимість вузла розуміється пропорційно сукупної значимості сусідніх вузлів. Betweenness centrality дозволяє виміряти ступінь, в якому конкретний вузол розташований між різними двома несуміжними вузлами. Центральність між об’єктами — це відповідний індикатор, який вимірює ступінь, у якому вузли забезпечують непрямі зв’язки між рештою вузлів у мережі. Побудова мережі країн має особливості, пов`язані з наявністю даних. Неможливість побудови мережі для 193 країн була виявлена через велику кількість даних. Наприклад, для африканського регіону дані про цифрові технології практично повністю відсутні. Тому було вирішено проаналізувати лише ті країни, щодо яких є практично повний набір даних [137].

Попередній аналіз набору даних аналогічних мереж технологій. Єдиними відмінностями є зміна індикатора заокруглення (для мережі країн – це округлення до третього знака) та множення транспонованої матриці. Для мережі країн спочатку необхідно транспонувати основну матрицю, а потім основну матрицю множити на транспоновану. Аналогічно мережі технологій, слід будувати графіки з чотирма популярними типами центральності: Degree centrality, Closeness centrality, Eigenvector centrality та Betweenness centrality. Degree centrality є мірою мінливості індивідуальних показників центральності. У наших даних Degree centrality визначається як число

цифрових технологій, що широко використовуються. Closeness centrality вимірює наскільки близько вузол знаходиться до решти вузлів. Центральність близькості відноситься до суми геодезичних відстаней від вузла і до всіх n-1 інших у мережі.

У мережах цифрових технологій Degree centrality, Closeness centrality та Eigenvector centrality формують технології 1 рівня: використання інтернету (UI), автоматизація та робототехніка (AR), інтернет речей (IoT), технологія 5g та два типи патентів (патенти на технології цифрового зв'язку та патенти на комп'ютерні технології. Технології 2 рівня: Штучний інтелект (AI) та 3D-друк (X3Dp) для всіх трьох типів центральності, а також технологічна основа (TF) у Betweenness centrality.

Щодо мереж країн, які відповідають Degree centrality, Closeness centrality та Eigenvector centrality, то вони формують країни 1 рівня: Сінгапур, Китай, Німеччина, Бельгія, Канада, Великобританія, Нідерланди, Фінляндія, Франція, Японія, Республіка Корея, Італія, Швейцарія, США, Ірландія. Країни 2 рівня: Індія, Іспанія та Австралія.

Обґрунтовуючи результати мережного аналізу, слід зазначити одну методологічну особливість. Обидві таблиці центральності (для двох мереж) вказують на значні відмінності у показниках Eigenvector та Bonacich Power centralities. Ці відмінності вимагають додаткової перевірки [137; 296] показника Bonacich centrality. Бета-параметр (у розрахунках Bonacich centrality) впливає показники «потужності», які є мірою Bonacich centrality. Відмінності можна пояснити за рахунок: 1) неточностей у обчисленнях центральності; 2) тим що, що значні відмінності є унікальною особливістю побудованих мереж. Дотримуючись рекомендацій С. Родана [там само], може бути проведено додаткову перевірку, після якої відмінності між центральностями Bonacich та Eigenvector centralities залишаються значними. Додаткова перевірка дає вагомі підстави для відхилення першого пояснення, але не повною мірою гарантує відсутність систематичних похибок у розрахунках. Щоб перевірити загальні результати й отримати окрему

перевірку бета-показника Bonacich centrality, необхідно порівняти мережі у предметному полі конкуренції у сфері цифрової трансформації. Безперечно, інтерпретація результатів враховуватиме специфіку індикатора Bonacich centrality. Результати центральностей мережевого аналізу цифрових технологій представлені табл. 1.

Таблиця 1

Інформація щодо центральностей мережевого аналізу цифрових технологій

Тип цифрової технології	**Центральність за ступенем (Degree Centrality)**	**Центральність за близькістю (Closeness Centrality)**	**Центральность за посередністю (Betweenness Centrality)**	**Центральность власного вектору (Eigenvector Centrality)**	**Центральность Боначичі (Bonachin Power Centrality)**
Індекс телекомунікаційної інфраструктури	*7*	0.0055	0	0.428	0
Використання Інтернету	*20*	*0.0769*	**7.0714**	**0.9863**	0.102
Інтеграція цифрових технологій	*7*	0.0055	0	0.4234	0
Патенти на цифрові технології	*20*	*0.0769*	1.5714	1	0.102
Патенти на комп'ютерні технології	*20*	*0.0769*	1.5714	1	0.102
Технологічна основа	*10*	*0.0435*	0.1429	0.5704	0.1429
Великі дані	*7*	*0.0055*	0	0.4079	0
Штучний інтелект	*16*	*0.0588*	3.5	0.8934	0.2245
Інтернет речей	*20*	*0.0769*	1.5714	1	0.102
Автоматизація	*20*	*0.0769*	1.5714	1	0.102
3D друк	*15*	*0.0556*	0.4286	0.8182	0.0204
Віртуальна валюта та блокчейн	*7*	*0.0055*	0	0.4234	0
Хмарні обчислення	*7*	*0.0055*	0	0.4234	0
Технологія зв'язку 5g	*20*	*0.0769*	1.5714	1	0.102

Значення Інтернету (використання Інтернету – UI в мережі), безумовно, не можна недооцінювати. На всіх рівнях суспільно-політичного життя Інтернет посідає ключове місце. Будь-які спроби цифрової трансформації будуть безрезультатними без Інтернету. Крім того, Інтернет є джерелом реального взаємозв'язку всіх типів цифрових технологій. Подібна логіка може бути використана до технології 5g. Розглядаючи її як еволюційний етап розвитку Інтернету, можна визначити фактичне становище цієї технології в системі безпеки та сталого розвитку.

У свою чергу, два типи патентів представляють собою не що інше, як політичний і науково-технічний напрямок держав. Запатентовані технологічні розробки демонструють прагнення країн незалежного розвитку. Власне кажучи, патенти відіграють вирішальну роль суверенної реалізації цифрової трансформації. В іншому випадку державам доведеться імпортувати технічні рішення з інших країн та/або технологічних компаній, втрачаючи контроль над даними та інформацією.

Більш несподіваний результат може бути отриманий відповідно до позиції Інтернету речей (IoT) та автоматизації (AR). З одного боку, ці два напрями взаємопов'язані. Будь-яке досягнення у побудові Smart Cities (Дія Сіті) так чи інакше пов'язане з автоматизацією виробничих процесів та забезпеченням міської інфраструктури роботизованими пристроями. З іншого боку, напрямок Інтернету речей, незважаючи на велику увагу громадськості, не демонструє стрімких результатів у реальності. Так, концепції розумних будинків, розумного уряду, розумного бюджету тощо поступово впроваджуються. Центральне становище Інтернету речей обумовлено революційними практичними результатами. Швидше за все, цей результат слід інтерпретувати як потенційні можливості у майбутньому. Автоматизація та робототехніка, у свою чергу, демонструють значні результати в економічній сфері (виробництво та виготовлення), а також у сфері нацбезпеки. В останні роки з'являється все більше прикладів використання безпілотників (дронів) як у військових місіях, так і всередині

країни для патрулювання громадської та цивільної безпеки. Значні практичні результати, а також фінансові стимули та політичне врегулювання цього напряму визначають позицію у мережі цифрових технологій [301].

Зрозуміло, технологічна інфраструктура є основою для концепцій цифровізації разом із доступом до Інтернету. Тому технологічна основа (інфраструктура та готовність реалізації цифровізації) TF не повинна входити до лідируючої групи. Швидше за все, це пов’язано зі зниженням уваги, у різних міжнародних звітах, до оцінки, індексації й аналізу. Більше того, оцінка кожної країни щодо технологічної готовності та доступності технічної інфраструктури методологічно надзвичайно складна. Інакше кажучи, ця позиція обумовлена нестачею даних.

Позиція в мережі 3D-друку аналогічна до розробки змісту концепції Інтернету речей. Дана технологія має значні результати та потенціал для революційних змін у багатьох областях – від 3D-друку будинків, машин та обладнання до 3D-друку внутрішніх органів. Сьогодні все це знаходиться на рівні експериментів і локального застосування. З огляду на це результати мережного аналізу можна інтерпретувати як значні потенційні можливості найближчим часом.

Позиція Big Data зумовлює появу дискусій як із боку наукової спільноти, так і практиків. За всіма показниками центральності великі дані розташовані на периферії мережі. Це виглядає не зовсім зрозуміло, ураховуючи значний дослідницький інтерес та практичні результати технології. Технології аналізу великих даних надають перетворюючий вплив на уряди в усьому світі [279], використовуються в процесі прийняття політичних рішень [258], аналізуються з погляду ризиків для конфіденційності громадян і в питаннях забезпечення безпеки громадян [342] тощо. Звичайно, технології Big Data створюють не тільки переваги, але й значні ризики системи безпеки на рівні збору, аналізу й обробки даних (загрози конфіденційності), а також ризики на етапах інтерпретації результатів аналізу та прийняття табл. аняючи рішень на основі даних.

Таким чином, результати мережевого аналізу щодо великих даних залишаються суперечливими. Якщо розглядати великі дані виключно як нові високотехнологічні та складні методи аналізу великої кількості даних, то результати цілком логічні. Власне кажучи, у великих даних немає нічого революційного, крім еволюційного розвитку аналітичних методів. В іншому випадку, ураховуючи виміри великих даних такі, як швидкість, обсяг, достовірність та цінність [126; 314; 329], великі дані представляють собою цілу теорію збору, структурування, аналізу та роботи з конкретними даними. Іншими словами, великі дані – це надійні дані різних форматів, створені й отримані з різних геопросторових положень. Обсяг даних досить великий, щоб його не можна було обробити певним програмним забезпеченням, електронною таблицею або комп'ютером і який може створити цінність для організацій [107]. Видається, що в даному мережевому дослідженні становище великих даних явно недооцінюється, що залишає місце для подальших наукових розробок.

Інші типи цифрових технологій опиняються на мережі мережі, крім AI – штучного інтелекту. Центральності Betweenness, Eigenvector та Bonacich power вказують, що штучний Інтелект є ключовою цифровою технологією. У взаємозв'язку цифрових технологій штучний інтелект є найбільш «впливовим» типом цифрових технологій, зумовлючи появу значної кількості сталих зв'язків. Уряди різних країн використовують неоднакові підходи для просування штучного інтелекту та його технологій. Проте він стає одним із ключових факторів розвитку держави, посилюючи / знижуючи міжнародну конкуренцію та глобальну безпеку.

Отримані результати з позицією розвитку штучного інтелекту можуть бути піддані критиці, тому що він включає багато невідомих. Технологія штучного інтелекту, з усією її неоднозначністю, є однією з найбільш затребуваних, яка концентрує навколо себе концепцію цифрової трансформації. Результати центральностей мережевого аналізу країн представлені в табл. 2.

Таблиця 2

Інформація щодо центральностей мережевого аналізу країн

Назва країни	**Централь-ністьза ступенем (Degree Centrality)**	**Центральність за близькістю (Closeness Centrality)**	**Центральність за посередністю (Betweenness Centrality)**	**Централь-ність власного вектору (Eigenvector Centrality)**	**Централь-ність Боначича (Bonachin Power Centrality)**
Австралія	41	0.019	3.902	0.825	*0.406*
Австрія	19	0.001	0	0.41	0
Бельгія	*56*	*0.027*	**7.827**	0.994	0.039
Болгарія	19	0.001	0	0.39	0
Канада	52	0.024	2.247	0.966	0.089
Китай	*56*	*0.027*	3.157	*1*	0.039
Хорватія	19	0.001	0	0.39	0
Чехія	21	0.001	0.111	0.413	0.075
Данія	33	0.017	2.009	0.6	0.344
Естонія	19	0.001	0	0.393	0
Фінляндія	56	0.027	3.157	1	0.039
Франція	56	0.027	3.157	1	0.039
Німеччина	56	0.027	3.157	1	0.039
Греція	19	0.001	0	0.401	0
Угорщина	19	0.001	0	0.403	0
Індія	45	0.021	0.902	0.906	0.076
Ірландія	52	0.024	2.463	0.961	-0.183
Італія	55	0.026	7.36	0.987	0.051
Японія	56	0.027	3.157	1	0.039
Литва	19	0.001	0	0.389	0
Люксембург	26	0.015	0.923	0.494	-0.136
Нідерланди	56	0.027	3.157	1	0.039
Норвегія	29	0.001	1.264	0.508	-0.249
Польща	19	0.001	0	0.41	0
Португалія	19	0.001	0	0.403	0
Південна Корея	56	0.027	3.157	1	0.039
Румунія	19	0.001	0	0.401	0
Сингапур	54	0.026	7.369	0.978	0.064
Словакія	21	0.001	1	0.4	0.075
Словенія	20	0.001	0	0.392	0.05
Іспанія	44	0.02	4.81	0.857	-0.066
Швеція	56	0.027	32.197	0.993	0.039
Швейцарія	56	0.027	3.157	1	0.039
Турція	19	0.001	0	0.417	0
Україна	19	0.001	0	0.418	0
Англія	54	0.026	2.686	0.983	0.001
США	56	0.027	3.157	1	0.039

Щодо отриманих результатів із мережі країн, можна встановити, що США та Китай є двома провідними конкуруючими лідерами щодо впровадження та розвитку цифрових технологій. Більше того, «технологічна» конкуренція перетворилася на «торгову війну» між цими країнами у 2019 році. Наукове, технічне, інноваційне й економічне лідерство цих двох країн дало старт дискусіям щодо повернення біполярності. Усе це лише підтверджує позиції США та Китаю у цьому дослідженні. Однак варто зазначити, що щодо Китаю необхідно виявляти обережність під час аналізу та дослідження соціо-політичного порядку денного. Важко відокремити реальні досягнення та результати від інформаційного шуму довкола [107].

Японія та Південна Корея є не лише ключовими гравцями в технічному та інноваційному розвитку азіатського регіону, а й у всьому світі. Незважаючи на деякі культурні особливості, ці країни успішно інтегрують найкращі практики та досягнення в галузі цифрових технологій на глобальному рівні. Франція та Німеччина входять до лідерів цифрового порядку денного ЄС. У принципі ці країни займають ключові позиції в ЄС з багатьох суспільно-політичних питань. Тому лідерство в цифровому порядку є продовженням обраного курсу розвитку країн.

На перший погляд, потрапляння до списку лідерів Фінляндії, Нідерландів та Швейцарії може здатися дивним. У Фінляндії існує одна з кращих стратегій цифрової трансформації, що реалізуються на загальнодержавному рівні [256]. При цьому Фінляндія була визнана однією з провідних країн цифрової трансформації. Крім цифровізації політики та державного управління, Фінляндія окремо стимулює цифрову трансформацію в бізнесі [там само]. Більше того, згідно з звітом ЄС щодо країн [257], Фінляндія не тільки створює політичні, соціальні та економічні можливості для цифровізації, але й неухильно досягає практичних результатів, як на національному, так і на локальному рівні (у формі експериментів щодо впровадження різних типів цифрових технологій).

Нідерланди, у свою чергу, також ухвалили стратегію цифровізації [273]

на законодавчому рівні. За результатами реалізації стратегії країна демонструє високі показники. Наприклад, у 2018 році PWC провела масштабне дослідження [288], у результаті якого було напрацьовано численні позитивні практики по всій країні. Крім того, цифровий порядок денний Нідерландів спрямовано на досягнення соціально значущих результатов [273]. З огляду на це населення демонструє високий рівень цифрової довіри. Крім того, практична реалізація приносить покращення безпосередньої якості життя (наприклад, у питаннях інклюзивності).

У Швейцарії існує багатопланова інноваційна екосистема, що дозволяє підприємствам розвивати та практично реалізовувати цифрову трансформацію у масштабі всієї країни. Національна стратегія «Digital Switzerland» [265] установлює чотири основні цілі:

– забезпечення рівної участі для всіх та зміцнення солідарності;

– забезпечення системи безпеки, довіри та прозорості публічної влади;

– подальше покращення цифрових можливостей;

– забезпечення зростання (якості життя) та рівня добробуту населення.

На додаток до політичного, соціального й економічного розвитку цифрового порядку денного Швейцарії суттєве значення приділяється технологічному розвитку. Швейцарія стимулює самостійні науково-технічні розробки й активно залучає міжнародні компанії.

Результати мережевого дослідження дозволили виявити 9 країн лідерів цифрової трансформації, а саме: Китай, Фінляндія, Франція, Німеччина, Японія, Нідерланди, Республіка Корея, Швейцарія та США (див. табл.. 2). Усі ці країни мають не лише доктринальні стратегії цифрової трансформації, а й практичні результати.

Одним із найнесподіваніших результатів є місце Швеції серед переліку проаналізованих країн. Варто зазначити, що така позиція Швеції може бути визначена лише з використанням методології мережевого аналізу, жодний інший метод не розкриває латентний потенціал країни у цифровому порядку.

За Degree and Closeness centralities Швеція впевнено входить до групи лідерів, що не дивно. Доповідь ОЕСР «Going Digital in Sweden» демонструє значний позитивний прогрес Швеції як у сфері державного регулювання та запровадження економічних стимулів, так і суспільної довіри. Іншими словами, багаторівнева стратегія Швеції передбачає таке:

– науково обґрунтоване державне регулювання;

– систематичну фінансову підтримку;

– розвиток державно-приватного партнерства за підтримки малого бізнесу;

– підвищення цифрової грамотності та цифрової довіри населення.

Більше того, уряд Швеції регулярно табл. аняюч стан ефективності впровадження цифровізації та надає необхідні інструменти для громадського (цивільного) контролю. Такий комплексний підхід дозволяє Швеції бути справді ключовим гравцем у цифровій трансформації на глобальному рівні.

Швеція є абсолютним лідером, з погляду Betweenness centrality, її стратегія та практичні результати уряду Швеції є кращими, ніж у США, Китаю, Японії та інших країн-технологічних лідерів. Результат вказує на те, що Швеція є своєрідним «центром», через який проходить більшість технологічних та інформаційних потоків у світі. Стимулювання та стрімкий розвиток технологічних гігантів таких, як IKEA, Spotify, Skype, Ericsson, H and M, Electrolux та Volvo, нарівні з розвитком стартапів, що дозволяють Швеції акумулювати максимально можливу кількість розробників цифрових технологій з їх подальшим упровадженням.

Крім того, політична й економічна стабільність, висока якість життя, а також привабливий інвестиційний клімат зробили Швецію однією з ключових країн для іноземних технологічних компаній та інвесторів. Таким чином, Швецію справді можна вважати центральним вузлом, куди «стікаються» більшість інноваційних, технологічних та ІКТ-напрямків, що дозволяє цій країни підвищити рівень власної системи безпеки.

Згідно з мережним аналізом, Сінгапур дещо «відстає» від лідерських позицій у мережі. Однак національна стратегія Smart Nation [328], а також супутні політичні, соціальні й економічні перетворення в країні вказують на значний еволюційний прогрес у галузі цифрових перетворень. Окремо, варто відзначити Індію та Велику Британію. Індія, як країна, що швидко зростає і розвивається, не виділяється за результатами мережевого аналізу. Проте за ретельному аналізі показників центральності його відставання незначне. Це вказує на можливість зміни позиції країни на міжнародній арені найближчим часом. Щодо Великобританії, то її «незначні» успіхи в цьому дослідженні, пов’язані зі зміною політичної та соціальної уваги. Перебуваючи в затяжному піку Brexit, Великобританія не приділяла належної уваги цифровій трансформації. Більше того, додатковий аналіз періоду останніх 5-10 років може продемонструвати значні зміни у політичному й економічному напрямку розвитку Великої Британії.

Таким чином, результати мережевого аналізу країн дають уявлення про поточний стан міжнародної конкуренції у сфері цифровізації. Зрозуміло, геополітична та міжнародна взаємодія провідних країн (а також країн, «табл. аняючи» лідерів) має бути ґрунтовно досліджено окремо.

Додаток 2

Індикатор можливостей штучного інтелекту (AI – capability)

Питання вимірів й оцінювання можливостей (capability) є дуже актуальним напрямом у фундаментальній науці політико-правового й соціального блоку (починаючи від складання індексів державної спроможності (state capacity), ураховуючи теорії політичної комунікації та закінчуючи дослідженнями організаційних можливостей (organizational capabilities)). Сутнісно, усі виміри «capability» у науковій літературі представлені або різними регресійними моделями для виявлення зв'язків індикаторів та їх впливу на можливості (capabilities), або експертними інтерв'ю (докладніше див. роботу Р. Гранта та Г. Верона [198], де проводиться аналіз основних емпіричних досліджень та їх проблемних зон у сфері організаційні capabilities). Окремим напрямом досліджень є створення складових індексів capabilities на національному та міжнародному рівнях (наприклад: Global capability index, Composite Index of National Capability).

У межах цього дослідження за основу береться методологічний підхід вимірів «Global capability index» [179] та «Composite Index of National Capability» [157], який ураховує витрати та фінансування військової й оборонної сфер. Зазначений підхід представляє собою формування єдиного індикатора по країні, який є сумою показників конкретних сфер (полів), поділену на кількість даних сфер. Наприклад, «Global capability index» формується на основі вимірювань трьох сфер (полів) (dimensions):

– соціально-економічне середовище: освіта, рівність та гендерна рівність, цифрова участь, інфраструктура комунікаційних технологій;

– соціально-культурне середовище: довіра, соціальна толерантність, участь у колективних діях тощо;

– середовище управління (Governance environment): індивідуальні та колективні можливості соціальної та політичної активності, верховенство

закону, політичний діалог, нормативно-правова база цивільних об’єднань та організацій тощо.

Ураховуючи значний масив параметрів у кожній області/полі, кінцевий розрахунок індикатора «capability» є сумою показників по областях, з урахуванням коефіцієнтів щодо кількості кожного індикатора, поділеного на три області.

Такий підхід визначений у межах «Composite Index of National Capability» ураховує теоретичні положення фундаментальної науки. У випадку врахування теорії поля може вираховуватися шість параметрів (а не три, як з Global Capability Index), вони сумуються і поділяються на кількість параметрів.

Виходячи з концептуальної рамки розуміння штучного інтелекту та цілей створення показника можливостей штучного інтелекту (AI capability) можна виділили чотири області/сфери:

1. Технологічна (Technological): ураховує технологічні аспекти штучного інтелекту, а саме застосування технології в державному управлінні та сфері забезпечення безпеки, а саме можуть ураховуватися показники точності алгоритмів і результати проходження тестів (Turing Test, Loverace Test тощо). Проте в межах цього дослідження можна відмовилися від двох індикаторів, оскільки щодо них можуть бути відсутні дані по країнах, що є відображенням технологічних можливостей технології.

2. Економічна (Economic environment): ураховує фінансування технології штучного інтелекту в контексті загального військового (оборонного) бюджету. Слід розуміти, що сфера безпеки може мати різні джерела фінансування, включаючи засекречені видатки бюджету, фінансування за рахунок інших статей та розділів тощо, тому можна враховувати публічні дані про фінансову підтримку технологій штучного інтелекту безпосередньо у військовому (оборонному) бюджеті. Без фінансування й економічного стимулювання розвиток технології й особливо

її застосування у сфері забезпечення безпеки є малоймовірним.

3. Управління (Governance environment): ураховує кількість державних підприємств, пов’язаних із технологіями штучного інтелекту й існування правової санкції на використання штучного інтелекту у військовій сфері. Цей блок відображає готовність держави розвивати технології штучного інтелекту та застосовувати можливості цих технологій.

4. Соціальна (Social environment): ураховує зайнятість населення у сферах і галузях розробки та застосування технології штучного інтелекту та кількість стартапів, що фокусуються на розвитку технологій штучного інтелекту. Відображає залучення громадськості, а також можливість держави мобілізувати високопрофесійні кадри.

Зазначені області/сфери з показниками та їх короткою характеристикою розрахунку наведені в табл.. 3.

Таблиця 3

Оцінювання можливостей штучного інтелекту

Сфера/область (dimension)	**Показник**	**Стисла характеристика**
Технологічна (0.25)	UT (use of technology)	Застосування штучного інтелектуу державному управлінні та військовій (оборонній) сфері (так/ні)
Економічна (0.25)	MF (military funding)	Військові витрати на розвиток і впровадження штучного інтелекту / Загальні військові витрати
Управління (0.3)	SC (state companies)	Державні підприємства, що впроваджують технології штучного інтелекту (так/ні)
	LA (legal authorization)	Правові санкії на використання штучного інтелекту у військовій (оборонній) сфері (так/ні)
Соціальна (0.2)	JO (job openings)	Зайнятість населення (наявні вакансії (job openings) / кількість працездатного населення
	RS	Стартапи, пов'язані з впровадженням та/або розвитком штучного інтелекту

Агрегування зазначених областей/сфер є заключним етапом формування індикатора можливостей технології штучного інтелекту (AI capability), у межах якого визначаються ці області/сфери:

1) технологічна та економічна сфери отримують вагу «0.25» з 1;

2) область управління – вагу «0.3» у зв'язку з соціально-політичною значимістю цієї галузі у питаннях безпеки.

За аналогічним принципом, соціальна сфера має вагу «0.2», незважаючи на значущість громадянського суспільства та суспільної реакції, у сфері забезпечення безпеки населення «знає лише те, що держава вважає за можливе знати». Іншими словами, роль суспільства у питаннях можливості технології у сфері безпеки буде найменш значуща поряд з іншими областями вимірюваннями.

Формула (1) обчислення індикатора можливостей штучного інтелекту (AI capability) має такий вигляд:

$$\text{AIcapability} = \frac{(0.25 \cdot UT + 0.25 \cdot MF + 0.3 \cdot (SC + LA) + 0.2 \cdot (JO + RS))}{4} \quad (1)$$

У формулі обчислення індикатора можливостей штучного інтелекту (AI capability) представлений показник UT (як показник застосування/використання штучного інтелекту в державному управлінні та військовій сфері), що відноситься до технологічної сфери. Показник MF (фінансування штучного інтелекту у військовій сфері), що відноситься до економічної сфери. SC (показник державних компаній у сфері штучного інтелекту) та LA (показник наявності правової санкції на застосування технології штучного інтелекту у військових цілях) відносяться до області Управління. Крім того, два показники відносяться до соціальної сфери: JO (показник зайнятості у сфері штучного інтелекту) та RS (показник стартапів у сфері штучного інтелекту).

Для кращого розуміння структури даних та підвищення валідності

аналізу нижче представлені описові статистики показників можливостей штучного інтелекту, а також кореляційний аналіз кожної країни. Зважаючи на інтеграційні прагнення України, можна представити аналітичні дані щодо індикатора можливостей штучного інтелекту (описові статистики) у США, Швеції, Франції та Німеччині (таблиці 4–7). Вибір даних країн зумовлений тим, що Франція та Німеччина визнані як регіональні безпекові лідери у Центральній Європі, а Швеція є лідером у забезпечені впровадження та розвитку цифрових технологій. Щодо США, то ця країна є членом НАТО і відіграє важливу роль у забезпеченні безпеки у Північній Америці зокрема і глобальної безпеки загалом.

Таблиця 4

Індикатор можливостей штучного інтелекту (описові статистики) у США

Показник	**Min**	**Max**	**Середнє значення**	**Медіана**	**1 квар-тал**	**3 квартал**	**Стандарт. відхилення**	**Дисперсія**
UT	0	1	0.625	1	0	1	0.5175492	0.2678571
MF	0	0.4591507	0.206761	0.2276017	0	0.3471062	0.1936002	0.03748102
SC	0	1	0.5	0.5	0	1	0.5345225	0.2857143
LA	0	1	0.625	1	0	1	0.5175492	0.2678571
JO	0	0.1247333	0.03701667	0.0112	0	0.06675	0.04881349	0.00238275
RS	0	1	0.5	0.5	0	1	0.5345225	0.2857143

Таблиця 5

Індикатор можливостей штучного інтелекту (описові статистики) у Швеції

Показник	**Min**	**Max**	**Середнє значення**	**Медіана**	**1 квар-тал**	**3 квартал**	**Стандарт. відхилення**	**Дисперсія**
UT	0	1	0.6	1	0	1	0.5477226	0.3
MF	0	0.002937	0.0005875	0	0	0	0.001313668	1.72572306
SC	0	1	0.8	1	1	1	0.4472136	0.2
LA	0	1	0.4	0	0	1	0.5477226	0.3
JO	0	0	0	0	0	0	0	0
RS	0	1	0.8	1	1	1	0.4472136	0.2

Таблиця 6

Індикатор можливостей штучного інтелекту (описові статистики) у Франції

Показник	Min	Max	Середнє значення	Медіана	1 квартал	3 квартал	Стандарт. відхилення	Дисперсія
UT	0	1	0.5	0.5	0	1	0.5345225	0.2857143
MF	0	1.7717860	2.21473207	0	0	0	6.26420807	3.92403113
SC	0	1	0.75	1	0.75	1	0.46291	0.2142857
LA	0	1	0.125	0	0	0	0.3535534	0.125
JO	0	0	0	0	0	0	0	0
RS	0	1	0.75	1	0.75	1	0.46291	0.2142857

Таблиця 7

Індикатор можливостей штучного інтелекту (описові статистики) у ФРН

Показник	Min	Max	Середнє значення	Медіана	1 квартал	3 квартал	Стандарт. відхилення	Дисперсія
UT	0	1	0.2857143	0	0	0.5	0.48795	0.2380952
MF	0	0	0	0	0	0	0	0
SC	1	1	1	1	1	1	0	0
LA	0	1	0.2857143	0	0	0.5	0.48795	0.2380952
JO	0	0.00381	0.0010184	0	0	0	0.001745	3.04515506
RS	0	1	0.4285714	0	0	1	0.5345225	0.2857143

Додаток З

Індикатор оцінки загроз (Threat evaluation)

Оцінці загроз (threat evaluation) присвячено чимало наукових розробок, що здебільшого об'єднані єдиним напрямом – оцінка загроз і розподіл зброї (Threat Evaluation and Weapon Assignment – TEWA, наприклад [166; 172; 229; 239; 259]). TEWA вважається основним компонентом системи ADS час найпоширенішими є моделі на основі байєсівських мереж (Bayesian networks) [там само], нечіткої логіки (fuzzy logic/fuzzy inference rules) [229; 259] та систем підтримки прийняття рішень (decision support system) [172].

TEWA-моделі, засновані на мережах «bayesian networks», дозволяють долати невизначеності (неповнота інформації про об'єкти; відсутність інформації про стан інфраструктури; ймовірність та/або випадковість в управлінні конкретним озброєнням тощо) при моделюванні. У підході «bayesian networks» змінні TEWA-моделі містять межі ймовірностей або розподіл ймовірностей, що дозволяє оцінювати загрози навіть у разі неповноти даних.

У свою чергу, моделі, засновані на правилах концепції нечітких множин будуються за принципом функцій належності (функцій членства - membership function). У теорії чітких множин члени *x* універсальної множини *X* є або членами, або не членами множини A ⊆ X.

Таким чином, значення, присвоєні *x*, потрапляють у діапазон, вказуючи ступінь членства елемента (нечіткому) наборі, про які йдеться. Великі значення вказують на більш високий ступінь членства, тоді як нижчі значення вказують на нижчий ступінь членства (degree of membership). Власне кажучи, для конкретного контексту може бути важко визначити чіткі межі (показники/параметри) змінної, тому використовується функція членства, яка дозволяє розраховувати схожі за ступенем членства показники змінної. У цьому контексті можна висловити два важливі зауваження:

1) оцінка членства (membership grades) у правилах нечітких множин не відноситься до оцінки ймовірності [229];

2) щодо самих правил нечіткої логіки відсутня єдність у науковому академічному середовищі – частина дослідників не визнають такий підхід, вважаючи його надто абстрактним.

Застосування систем прийняття рішень у TEWA-моделях дозволяє враховувати показники геоінформаційних систем (ГІС картрування вразливих активів), доповнювати модель методами прогнозування, розподіляти та оцінювати «економічно ефективне призначення зброї» [172]. Відтак, система прийняття рішень дозволяє розширити перелік параметрів моделі, а також оцінювати додаткові фактори (наприклад, економічну доцільність) при оцінці загроз. Самі TEWA-моделі із системою прийняття рішень можуть будуватися на основі машинного навчання (найпопулярніші моделі з древом рішень (цілей); більш просунуті моделі ґрунтуються на глибокому навчанні, наприклад Tactical Air Combat Decision Support System), теорії ігор, теорії поля та динамічних мереж («bayesian networks»).

Зазначимо, що моделі TEWA передбачають створення повноцінної системи реагування та протидії загрозам, що виходить за рамки даного дослідження. Таким чином, на основі наявних досліджень з оцінки загроз, у тому числі з урахуванням масштабного мета-аналізу (156 публікацій досліджень TEWA з 1975 по 2016 р.) проведеного вченими Насімом, Шахом, Ханом та ін., розроблено емпіричну модель розрахунку загроз.

Оцінка загроз найчастіше представлена двома [259] або трьома [172] етапами. Двоетапна модель передбачає таке: 1) оцінку та ранжування загроз; 2) призначення зброї (weapon assignment). Триетапна модель складається з такого: 1) оцінки сприйняття загрози (threat perception); 2) розрахунку індексу загроз (-и) (threat index calculation); 3) оцінка впровадження цифрових технологій у військовій сфері. Кожна модель оцінки загроз має право на існування, але повинна обов’язково враховувати відповідність загроз об’єкту/активу, що захищається (defended asset).

Кожен етап включає розрахунок конкретних характеристик [172]. Так, на етапі сприйняття загрози розраховуються критичні параметри конкретного типу озброєння, що передбачає використання цифрових технологій (наприклад, крилатої ракети): швидкість, висота, поперечний перетин радіолокації / ефективна поверхня розсіювання радіолокаційних хвиль (Radar cross-section), маневреність (maneuver capability), кут пікірування (dive angle), атакуючий підхід (attack approach) та ін. Етап призначення зброї безпосередньо враховуючи характеристики наявного оборонного озброєння і містить параметри: а) загроза призначається зброї на основі індексу загрози; б) загроза з найвищим індексом загрози (TI).

Узагальнено модель TEWA представляє собою оцінку та ранжування загроз у сфері безпеки за перерахованими вище характеристиками та розрахунок відповідності оціненої загрози об’єктам/активам, що захищаються, з подальшим визначенням озброєння для забезпечення безпеки об’єктів та нейтралізації загроз. Безпосередньо оцінку загроз (без розподілу озброєння) можна представити у вигляді блок схеми, де розраховується загальна кількість загроз (при оцінці та ранжируванні) і виводиться показник відповідності загрози об'єкту/активу, що захищається (рис. 1) [259].

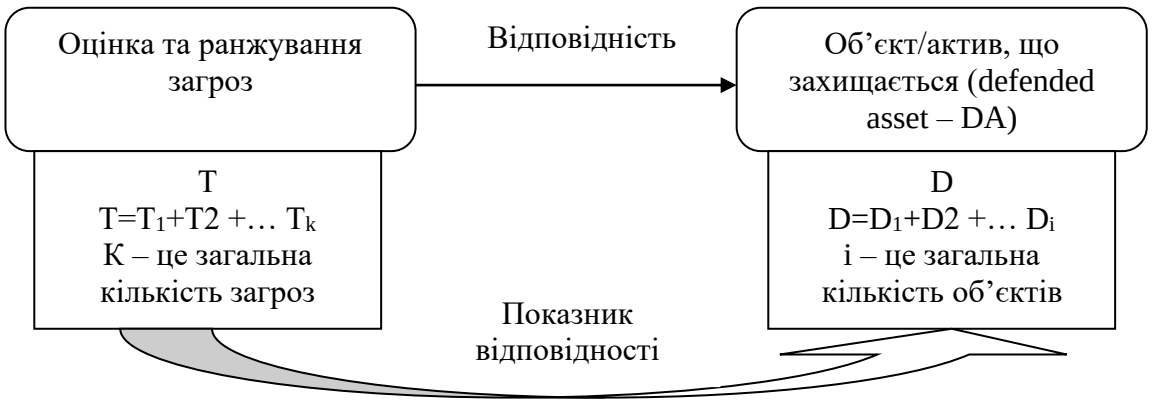

Рис. 1. Блок-схема узагальненої моделі TEWA (оцінка та ранжування загроз у сфері безпеки об’єктів/активів)

Для цілей цього дослідження показники сприйняття загроз (ТР) та характеристика/тип загроз (ТТ) концептуалізовані в такий спосіб сприйняття загрози (на підставі аналізу стратегій та інших нормативно-правових актів):

1. Показник освіти (education – Ed) – без навчання та перепідготовки населення, щоб відповідати темпам технологічних змін і різним типам загроз [122]. Збільшення освіченого, інформаційного та цифрового населення також буде сприяти протистоянню впливу інформаційних загроз. Таким чином, будь-яка держава, яка вказує на загрози, пов'язані зі штучним інтелектом, на рівні політики, адаптує освітню систему для підвищення освіченості, усвідомленості про технологію штучного інтелекту. У цьому дослідженні показник освіти розраховуватиметься з показників результатів країни за рейтингом PISA виключно за напрямом математики й теорії поля, оскільки вони є фундаментальними для розробок та застосування технології штучного інтелекту. Розрахунок є співвідношенням рейтингу країни в конкретний рік до максимально можливого показника рейтингу [215].

2. Показник нормативно-правового регулювання (regulation, Reg) – сприйняття загроз із боку держави відбивається у сфері нормативно-правового регулювання. Питома вага нормативно-правових актів, що закріплюють (у тій чи іншій мірі) загрози з боку технології штучного інтелекту, розраховуватиметься таким чином: кількість нормативно-правових актів (далі – НПА) зі згадуванням технологій штучного інтелекту на загальну кількість НПА на рік.

3. Показник внутрішніх патентів (domestic patents – DP) – визначення сприйняття загроз з боку держави неможливе без науково-технічних досліджень та розробок. Для розрахунку цього показника можуть враховуватися лише внутрішньодержавні патенти на тематику «штучний інтелект». Показник буде питомою вагою кількості внутрішніх патентів за тематикою у співвідношенні із загальною кількістю патентів у цей рік.

Характер/тип загроз, пов'язаних із розвитком цифрових технологій і штучного інтелекту (на підставі досліджень, індексів та показників звітів,

експертних оцінок). Цей показник може бути використаний для конкретного обчислюваного показника характеру/типу загроз. На жаль, на даний момент відсутні стійкі статистичні показники безпосередньо релевантних технологій штучного інтелекту [153]. Практично всі звіти та дослідження мають «доктринальний» характер, а саме: вказують, що є якийсь тип загроз, пов'язаних з розвитком цифрових технологій і штучним інтелектом, має певну характеристику загроз, проте жодного статистичного чи математичного вираження немає. З огляду на це доцільно приймати рішення про побудову чисельного бінарного показника:

0 – тип/характер загрози відсутній у країні у звітному році;

1 – тип/характер загроз був присутній (зафіксований/ задокументований) у країні у звітному році згідно з наступним переліком типів/характеру загроз, пов'язаних з розвитком цифрових технологій і штучного інтелекту [264]:

а) загрози критичній інфраструктурі;

б) кіберзагрози / кібератаки за допомогою штучного інтелекту (штучний інтелект розширює вектори загроз, вразливих для кібератак, виявляючи та експлуатуючи слабкі місця системи);

в) підприємства з дезінформації (зокрема Deepfakes);

г) порушення прав людини (мається на увазі, bias алгоритмів, порушення персональних даних, загрози біометричним даним тощо).

Відповідно до зазначеного переліку за кожен конкретний рік формуватиметься показник від «0» до «4». Якщо у досліджуваному році було зафіксовано якийсь тип загроз – виставляється «1», якщо не було – «0».

Розрахунок показника сприйняття загроз (TP) – це сума показників проксі даних у сфери освіти (Ed), проксі регулювання (Reg) та проксі внутрішніх патентів (DP), що визначається за формулою (2) таким чином:

$$TP = (Ed + Reg + DP) \quad (2)$$

Формула розрахунку сприйняття загроз вмісту: Ed – показник освіти, Reg – показник нормативно-правового регулювання, DP – показник внутрішніх патентів.

Показник типу/характеру загроз (TT) прийматиме значення від 0.1 до 4 і може бути виражений такою формулою (3).

$$TT \in [0.1 \dots 4] \quad (3)$$

Зазначений підхід до оцінки загроз буде заснований на оцінці сприйняття загроз (TP) та оцінці типу загроз (TT) у співвідношенні із кількістю захищених об’єктів (DA). Сприйняття загроз (TP) щодо технології штучного інтелекту ґрунтується на аналізі національних стратегій із забезпечення нацбезпеки країн та їх нормативно-правових актів у сфері безпеки. Тип загроз (-и) (TT), у свою чергу, може бути типологізований із релевантного теоретичного огляду, експертних оцінок, показників та індексів з міжнародних та національних звітів.

Об’єкти, що захищаються/активи (DA) – те, на що, власне, спрямовані загрози технологій штучного інтелекту. Ураховуючи специфіку спрямованості даного дослідження, з практичної точки зору, неможна вирахувати загальну кількість активів/об’єктів, що захищаються. Тому враховуватися (чисельний бінарний показник) будуть усі області, що згадуються в НПА країни, як такі, що захищаються. Умовний перелік [264] вказано в табл. 8.

Окремим елементом розрахунку є показник значущості/цінності активів/об’єктів, що мають захищатися (наприклад, об’єкти критичної інфраструктури). Учені С. Кумар і Б. Тріпаті вказують на високу роль визначення (у межах моделі) показника «значення захисту активів (protection value), що призначається особою, яка приймає рішення» та «знаходиться між 0 і 1» [239].

Таблиця 8

Перелік об’єктів/активів, що захищаються

Сфера, що визначається НПА	**Чисельний показник (визначення у НПА)**
Розвіддані	0 – відсутній; 1 – наявний.
Дані державних компаній	0 – відсутній; 1 – наявний.
Персональні дані громадян	0 – відсутній; 1 – наявний.
Автомобілі з автономним керуванням (self-drivingcars)	0 – відсутній; 1 – наявний.
Автономне озброєння (autonomous weapons)	0 – відсутній; 1 – наявний.

Такий показник є необхідним для врахування розподілу пріоритету загроз з боку політичних акторів та осіб, які приймають рішення у сфері забезпечення нацбезпеки. Пропонована модель також матиме показник значущості (PV) і прийматиме значення від «0» до «1», але з розподілом показника ваги. Характеристика оцінювання наведено у таблиці 9.

Таблиця 9

Показники вагомості

Характеристика показника вагомості	**Шкала**	**Вага**	**Обгрунтування**
1	2	3	4
Технологія штучного інтелекту в Стратегії національної безпеки країни	0 – відсутня; 1 – наявна.	0.3	Закріплення цифрових технологій (у тому числі штучного інтелекту) у національній безпековій стратегії є найвищим «визнанням» з боку держави значущості як самих цифрових технологій, так і потенціалу загроз, пов’язаних із цими технологіями.
1	2	3	4

Технологія штучного інтелекту в Стратегії національної безпеки країни	0 – відсутня; 1 - наявна;	0.3	Якщо в рамках системи державних органів у структурі забезпечення нацбезпеки створено спеціальний орган, присвячений забезпеченю розвитку цифровізації та технологій штучного інтелекту, то можна стверджувати, що держава визначає високий пріоритет даних цифрових технології.
Національна стратегія у сфері штучного інтелекту (цифровізації)	0 – відсутня; 1 – наявна.	0.2	Національна стратегія, що має безпосереднє відношення до сфери забезпечення системи безпеки, проте в силу специфіки самої технології штучного інтелекту, певною мірою регламентуватиме і питання нацбезпеки.
Сформульоване визначення штучного інтелекту в національній стратегії з цифрової трансформації	0 – відсутнє; 1 – наявне.	0.1	Відсутність окремого державно-правового регулювання (або хоча б доктринального закріплення наміру у вигляді національної стратегії) з фокусуванням уваги на особливостях упровадження та розвитку штучного інтелекту.
Державні (або афілійовані з державою) підприємства з розробки технологій штучного інтелекту у військовій сфері та/або у сфері нацбезпеки	0 – відсутні; 1 – наявні.	0.1	Облік технологічних підприємств є відображенням наявності власних (не іноземних) технічних можливостей (обчислювальних потужностей, програмного забезпечення тощо) у держави виявляти загрози розвитку цифрових технологій загалом і технологій штучного інтелекту зокрема.
Максимальний показник			**1**

Найбільш важливим і одним із ключових моментів розрахунку загроз є моніторинг й оцінювання зовнішніх і внутрішніх факторів. Наприклад, ПІР-

центр при створенні «Індексу міжнародної безпеки» [222] засвідчує пріоритет військових факторів перед будь-якими іншими (політичними факторами, тероризмом, техногенними та природними факторами, економічними факторами). Загальну політичну чи економічну кризу можна якимось чином подолати та наслідки глобальної екологічної катастрофи, у тому числі викликаної діями терористів. Щодо глобальної ядерної війни, то це явище можна вважати цілком незворотним та «летальним» для всього людства. Більше того, передбачається ранжування всередині кожної з груп за показниками глобального, регіонального та локального факторів безпеки. У запропонованому підході зазначені фактори також враховані. Виходячи із загальної теоретичної рамки дослідження – секторальний підхід аналізу сфери забезпечення нацбезпеки, запропонований Копенгагенською школою, запроваджується показник – фактор загрози (TF). Фактор загрози в межах моделі публічного управління у сфері нацбезпеки в умовах впливу цифровізації представлений як процес оцінювання кожної країни відносно до загальної оцінки п’яти секторів безпеки (табл. 10), запропонованих дослідником Б. Бузаною [148–149].

Таблиця 10

Показники загроз

Сфера/сектор безпеки	**Характеристика**	**Шкала оцінювання**
1	2	3
Політична	Загрози суверенності, посягання на легітимність та владний авторитет	0 - відсутність; 1 - локальна; 2- регіональна; 3 – міжнародна
Військова	Усі військові питання визначаються як загрози системі безпеки (окрім миротворчих цілей та ліквідації наслідків стихійних лих)	0 - відсутність; 1 - локальна; 2 - регіональна; 3 – міжнародна

1	2	3
Економічна	Загрози економічної стабільності держави та окремим елементам економічної системи (наприклад, банківський і фінансовий сектори)	0 - відсутність; 1 - локальна; 2- регіональна; 3 - міжнародна
Екологічна	Усі питання навколишнього середовища на території держави, а також глобальні міжнародні кліматичні виклики, що стосуються держави (глобальне потепління, забруднення, озоновий шар тощо)	0 - відсутність; 1 - локальна; 2- регіональна; 3 - міжнародна
Соціальна	Питання колективної ідентичності (мовної, культурної, релігійної тощо) та балансу (співвідношення) різних культур і мультикультуральність	0 - відсутність; 1 - локальна; 2- регіональна; 3 - міжнародна

Отже, фактори загроз (TF) ураховуються як питома вага відношення суми шкали оцінювання на максимальну кількість оцінки сфер (як під напрямків) національної безпеки (див. підрозділ 2.2, рис. 2.2).

Додаток 4

Прогнозування перспектив упровадження моделі пубіочного управління у сері національної безпеки в умовах впливу цифрових технологій

Показник	**Дані показника**	**Стандартне відхилення моделі**	**Прогнозний результат упровадження моделі**	**Тип моделі**
MF (Military funding) Економічна сфера, Можливості штучного інтелекту	Min: 0 Max: 0.9255269	0.7071068	Min: 0.6218285 Max: 0.8532102 (в пределах 1sd)	**Модель стійка до загроз**
UT (use of technology) + Test + AA (algorithm accuracy) Технологічна сфера, Можливості штучного інтелекту	Min: 0 Max: 5.450846	0.7071068	Min: 0.02811615 Max: 1.390828	**Модель чутлива до загроз і показників (у бік max значень)**
Сфера Управління (SC (state companies) + LA (legal authorization)) не підлягає тестуванню, оскільки мінімальний показник (0) і максимальний показник (2) присутні в моделі за різні роки				
JO (job openings) + RS (стартапи) Соціальна сфера, Можливості штучного інтелекту	Min: 0 Max: 2.712146	0.7071068	Min: 0.5116695 Max: 1.054099	**Модель чутлива до загроз і показників (у бік max значень)**
Сприйняття загроз (TP) Оцінювання загроз	Min: 0 Max: 1.976549	0.7071068	Min: 0.8982343 Max: 0.5276314	**Модель стабільна за більшістю показників**
Показник типу/характеру загроз, пов’язаних із розвитком цифрових технологій (ТТ) підлягає тестуванню, оскільки мінімальний показник (0) і максимальний показник (4) присутні в моделі за різні роки				

Додаток 5

З метою надання пояснювального потенціалу результатів мережного аналізу було здійснено додатковий регресійний аналіз. Він дозволив пояснити складову показника центральності (обрана центральність за посередництвом другого мережевого аналізу) – як елемента технологічного потенціалу й індикатора дифузії інновацій у сфері цифровізації. Перевірка спрямована на виявлення зв'язку показника центральності за посередництвом з факторами, що характеризують різні загрози для держав та їх інституційні можливості.

Регресійний аналіз спрямовано на виявлення чинників, які можуть пояснити становище країни у торговельній мережі цифрових технологій і послуг. При цьому привертають увагу фактори, пов'язані з питаннями нацбезпеки чи їх купіруванням, можливістю запобігання загрозам у цій сфері. Власне, слід прагнути продемонструвати можливості дослідження ролі цифрових технологій і дифузії інновацій у сфері національної безпеки. Держави й уряди можуть розвивати цифрові технології (особливо технології подвійного призначення) як реакцію на внутрішні та зовнішні загрози. Отже, виявлення зв'язку чинників загроз із показниками, умовно, технологічної центральності, може продемонструвати значний пояснювальний механізм державного управління урядів. Вказане виходить за межі дослідження, зважаючи на це пропонується пілотна версія для демонстрації потенціалу впливу цифрових технологій на сферу безпеки.

Для перевірки використовувався регресійний аналіз, а саме: лінійна регресія. Як залежна змінна, вона виступає показником центральності за посередництвом із іншим мережевим аналізом (торгівля технологіями, цифровими технологіями та послугами). Незалежними змінними виступають:

– 2 змінні з торгівлі зброєю: торгівля зброєю дані щодо країни постачальника [310] та торгівля зброєю дані щодо країни одержувача [309].

Зазначені змінні мють теоретичне обґрунтування як у межах досліджень нацбезпеки, так і логічний зв'язок із торгівлею цифровими та новітніми технологіями;

– 2 змінні, пов'язані з протестами [163]: безпосередньо протестна мобілізація та насильність протесту. Ці змінні розглядаються як внутрішні загрози національній безпеці (людського характеру);

– тероризм [195] як внутрішня та зовнішня загроза національній безпеці (людського характеру);

– імовірність насильницького конфлікту [202] як внутрішня, так і зовнішня загроза національній безпеці (людського характеру);

– природні катаклізми [177] – внутрішні та зовнішні загрози (природного характеру);

– політичний режим [339] на підставі даних V-dem, де 1 – закрита автократія, 2 – виборча автократія, 3 – виборча демократія, 4 – ліберальна демократія;

– ефективність уряду – змінна, яка є прикладом інституційних можливостей щодо реагування на загрози, пов'язані із розвитком цифрових технологій.

Варто зазначити, що первинно тестувалося чотири змінні інституційних можливостей, але через їхню значльну кореляцію один з одним було прийнято рішення в моделі публічного управління у сфері нацбезпеки в умовах впливу цифрових технологій використовувати тільки критерій «ефективність уряду».

Ураховуючи, що мережевий аналіз стосувався двох часових періодів, було ухвалено рішення зібрати дані та побудувати модель за такі періоди: 2015 р. та 2020 рр.

У табл. 11 представлені результати проведеного регресійного аналізу з оцінкою моделі публічного управління у сфері нацбезпеки за звітний період у 2015 р. і 2020 році. За підсумками проведеного аналізу для моделі 2015 р.

було виявлено, що істотними є торгівля зброєю, як країною-постачальником, так і країною-одержувачем, а також тероризм. Щодо торгівлі зброєю, то результати можуть свідчити про особливості розвитку цифрових технологій подвійного призначення. Власне кажучи, очікується, що такі технології подвійного призначення можуть виступати й елементами торгівлі зброєю. Альтернативним поясненням можуть бути особливості торгових шляхів, тому що торгівля цифровими технологіями процесуально схожа з торгівлею зброєю (як у рівні торговельних відносин, так і за логікою міжнародних політичних процесів). Щодо тероризму, то держави, які постраждали або побоюються терористичних загроз, розвивають на власних теренах технологічну складову (торгівля технологіями пов’язана з певним рівнем розвитку НДДКР та застосуванням новітніх технологій у сферу науки й освіти), розглядаючи цифрові технології як елемент протидії терористичним загрозам.

Модель публічного управління у сфері національної безпеки в умовах впливу цифрових технологій 2020 року має відмінні результати, від моделі 2015 р. Аналіз інформації щодо торгівлі зброєю в межах звітного періоду демонструє зв’язок лише з країною-постачальником. Зазначене можна пояснити специфікою торгових відносин (зміна/закриття контрактів, зміна торгових шляхів/каналів збуту та ін.). Крім того, варто брати до уваги вплив санкційної політики (яка активно застосовується до рф після 2014 р.), що суттєво змінює торгові маршрути, особливо у питаннях озброєння. Значимість (хоч і не настільки сильну) представляють масові протести та режим країни – виборча демократія.

Щодо акцій протестів і непокори, то результати можуть пояснюватися збільшенням масової протестної мобілізації, у зв'язку з чим результати 2020 р. є відмінними від моделі 2015 р. Причинами цього є виникнення та поширення пандемії COVID-19, що обмежили пересування людей у громадських місцях по всьому світові.

Таблиця 11

Результати регресійного аналізу

		2015	2020
Показник центральність (за посередництвом)		**Betw Centr**	
Торгівля зброєю. Країна-постачальник	ArmsTransS	0.003***	0.004**
		(0.001)	(0.002)
Торгівля зброєю. Країна-отримувач	ArmsTransR	-0.022***	-0.009
		(0.006)	(0.009)
Масова протестна мобілізація	MassProtest	-0.046	0.648*
		(0.217)	(0.337)
Насильницький протест	ProtesterViolence	0.097	-8.874
		(3.317)	(8.110)
Тероризм	GlobalTerror	0.231***	-0.422
		(0.078)	(0.258)
Імовірність насильницького конфлікту	HViolentConflP	0.723	0.300
		(1.614)	(0.970)
Природні катастрофи	NaturalDisast	0.0001	0.006
		(0.001)	(0.004)
Режим (виборча автократія)	Regime2	-1.771	30.505**
		(10.488)	(14.385)
Режим (виборча демократія)	Regime3	2.924	31.421*
		(7.815)	(16.119)
Режим (ліберальна демократія)	Regime4	6.276	29.698**
		(7.505)	(13.777)

Крім того, альтернативним поясненням може бути підвищена увага держав безпосередньо до акцій протестів. Власне кажучи, уряди почали розглядати протести як загрози, які потенційно можна усунути або контролювати за допомогою цифрових технологій, у межах яких усе більшу цікавість викликають технології штучного інтелекту. Зазначене може бути викликане ще й доступністю, поширеністю та результативністю впровадженя цифрових технологій. Так, якщо на початку 2010-х років технологічні рішення були на стадіях розробки й тестування, то після 2020 р. уряди та приватні інституції, отримавши значні результати у цій сфері й оцінивши можливості та перспективи впровадження цифрових технологій, стали

розглядати їх як певні інструменти для прийняття ґрунтовних і науково виважених управлінських рішень для розв’язання проблем у сфері безпеки. Режими виборчої демократії й електоральної автократії також засвідчують значимість зв’язку в моделі публічного управління у сфері нацбезпеки в умовах впливу цифрових технологій у 2020 р. Це складно однозначно інтерпретувати з огляду на те, що характеристики політичного режиму визначаються великою кількістю факторів. Однак, можемо стверджувати, що результати вказують перспективи подальших досліджень щодо впливу режимних характеристик на торговельні відносини та роль держав у торгових зв’язках цифрових технологій, що впливають на систему безпеки.

Підкреслимо, що наведені результати регресійного аналізу є наслідком обґрунтування визначеної вище в роботі гіпотези, а, відтак, її пілотною версією. Її метою є визначення: 1) потенційних можливостей пошуку пояснювальних механізмів результатів мережевого аналізу; 2) можливих напрямів подальших досліджень для посилення аргументації значущості та ролі показників цифрової центральності. Власне, показники центральностей щодо розвитку цифрових технологій і країн стосовно цих процесів змістовно відбивають як дифузію інновацій та цифровізації, так і можуть бути визнані як індекс технологічної центральності. Пошук механізмів, що пояснюють позиції країн у мережевій структурі та їх роль щодо загроз (якщо розглядати цифрові технології як елементи можливостей держави запобігати таким загрозам) значно розширює існуючі дискусії як у предметному полі досліджень національної безпеки, так і в логіці політики цифровізації.

Розвиток такого аналізу може бути спрямований на розширення змінних (як у процесі визначення загроз національній безпеці, так і можливостей їх усунення, а також моніторинг безпекового середовища, що є важливим для вдосконалення моделі публічного управління у сфері нацбезпеки в умовах впливу цифрових технологій (з урахуванням ефектів, результатів, факторів, загроз тощо).