e-ISSN **3041-2498**

Public Management and Policy

https://www.eu-scientists.com/index.php/pmap

Behavioral Models of Regulating Information and Cybersecurity in Public Authorities in Digital Transformation Conditions

Ivan Petroie [1] *

[1] *State Higher Educational Institution "University of Educational Management" (Ukraine). Third-Year Postgraduate Student at the Department of Public Administration and Project Management.*

* ***Corresponding Author,*** e-mail: ipetroe@gmail.com

ARTICLE INFO

Research Article

DOI: 10.70651/3041-2498/2026.3.21

Received:
16 February 2026
Accepted:
20 March 2026
Published online:
24 March 2026

ABSTRACT

The subject of the study is behavioral models of regulating information and cybersecurity in public authorities in digital transformation conditions. The article aims to conduct a comparative analysis of leading behavioral models of information and cybersecurity and to develop recommendations for public authorities to improve behavioral information security based on them. The methodological foundation of the study includes the systemic and interdisciplinary approaches, structural and comparative analysis, synthesis, and modelling. The source base consists of scientific publications on the topic of the study indexed in Scopus, selected and verified using Scopus AI tools. The conceptual basis of the study is the taxonomy of unintentional, intentional, and malicious behavior in the system of information and cybersecurity, which allows one to consider the information and cyber space of public authorities as a complex systemic phenomenon encompassing the interaction of people, software, and networks. As a result of the study, three groups of behavioral models of information and cybersecurity are systematized: 1) traditional cognitive models; 2) multidimensional operational models; 3) risk management models. It is established that the quality of regulatory documents and policies of public authorities is a particularly important tool for ensuring compliance with information security requirements. The advisability of applying a comprehensive value-oriented and multidimensional process-oriented model of managing behavioral information security in public authorities in digital transformation conditions is substantiated.

KEYWORDS

public authorities; information security; behavioral models; information security awareness; measurement; regulation.

e-ISSN **3041-2498**

Публічне управління і політика

https://www.eu-scientists.com/index.php/pmap

Поведінкові моделі регулювання інформаційної та кібербезпеки в органах публічної влади в умовах цифрових трансформацій

Іван К. Петроє [1]*

[1] *Державний заклад вищої освіти «Університет менеджменту освіти» (Україна). Аспірант третього року навчання кафедри публічного врядування і проєктного менеджменту.*

*** *Автор-кореспондент,*** e-mail: ipetroe@gmail.com

СТАТТЯ

Дослідницька

DOI: 10.70651/3041-2498/2026.3.21

Отримана:
16.02.2026 р.
Прийнята:
20.03.2026 р.
Опублікована:
24.03.2026 р.

АНОТАЦІЯ

Предметом дослідження є поведінкові моделі регулювання інформаційної та кібербезпеки в органах публічної влади в умовах цифрових трансформацій. Метою статті є порівняльний аналіз провідних поведінкових моделей інформаційної та кібербезпеки і розроблення на їх основі рекомендацій з удосконалення поведінкової інформаційної безпеки в органах публічної влади. Методологічну основу дослідження становлять системний і міждисциплінарний підходи, а також методи структурного й порівняльного аналізу, синтезу та моделювання. Джерельною базою слугують наукові публікації за темою дослідження, індексовані в базі Scopus, відібрані та верифіковані з використанням інструментів Scopus AI. Концептуальною основою дослідження є таксономія ненавмисної, навмисної та зловмисної поведінки в системі інформаційної та кібербезпеки, що дозволяє розглядати інформаційний і кіберпростір органів публічної влади як складне системне явище, яке охоплює взаємодію людей, програмного забезпечення та мереж. За результатами дослідження систематизовано три групи поведінкових моделей інформаційної та кібербезпеки: 1) традиційні когнітивні моделі; 2) багатовимірні операційні моделі; 3) моделі управління ризиками. Встановлено, що якість регуляторних документів та політик органів публічної влади є особливо важливим інструментом забезпечення дотримання вимог інформаційної безпеки. Обґрунтовано доцільність застосування комплексної ціннісно-орієнтованої та багатовимірних процесних моделей управління поведінковою інформаційною безпекою в органах публічної влади в умовах цифрових трансформацій.

КЛЮЧОВІ СЛОВА

органи публічної влади; інформаційна безпека; поведінкові моделі; обізнаність про інформаційну безпеку; вимірювання; регулювання.

1. Introduction

Цифрова трансформація являє собою процес загальноорганізаційних змін в управлінні та інформаційних технологіях (IT) у відповідь на виклики у зовнішньому середовищі [1]. Впровадження цифрових трансформацій в органах публічної влади докорінно змінює не лише технологічне середовище управлінської діяльності, а й систему інформаційної та кібербезпеки, вимоги до поведінки персоналу у цифровому просторі. Технологічна модернізація внутрішніх адміністративних процесів (масове впровадження електронних послуг, переведення критичної державної інфраструктури у цифровий формат, цифровізація реєстрів, баз даних і комунікаційних каналів) спричиняє також системні зміни у способах взаємодії органів публічної влади з громадянами, суб'єктами господарювання та міжнародними партнерами. Ці процеси принципово розширюють сферу кібератак, збільшують вразливості та ускладнюють управління інформаційними потоками організаційного, галузевого, регіонального й державного рівнів.

Як доводять результати останніх досліджень зарубіжних вчених, жодна з вразливостей систем інформаційної безпеки не є суто технологічною. Однією з ключових проблем у сфері інформаційної безпеки є низький рівень дотримання (compliance) вимог політик працівниками. У цьому контексті формування та реалізація дієвої політики інформаційної безпеки в органах публічної влади є одним серед пріоритетних напрямів публічного управління, що безпосередньо пов'язаний із забезпеченням суверенітету, захистом прав громадян і підтриманням довіри суспільства до публічних інституцій.

Периметр вразливостей поведінкових інформаційних та кіберсистем органів публічної влади в Україні значно розширився з початку повномасштабного вторгнення рф. Водночас, наукова і практична значущість проблеми зумовлена як зростанням кількості кіберінцидентів у публічному секторі України в умовах воєнного стану, так і тим, що ефективність будь-яких технічних і нормативних заходів безпеки в органах публічної влади значною мірою визначається рівнем забезпечення поведінкової інформаційної та кібербезпеки персоналу. Загрози від поведінкової інформаційної безпеки зростають в умовах запровадження дистанційної форми зайнятості, переходом на дистанційні та гнучкі гібридні форми роботи, розширення хмарних рішень, зростання взаємозалежності відомчих інформаційних систем та інше. O. Ogbanufe, R. E.Crossler, D.Biros [2] показали, що перехід на дистанційну роботу змінює баланс між механізмами мотивації захисту та відповідальної поведінки: в умовах роботи поза офісом необхідно посилювати інформаційні, освітні пояснювальні заходи щодо дотримання політики інформаційної безпеки.

2. Literature Review

Тема цифрової трансформації є актуальною та важливою для обговорення серед дослідників та практиків публічного управління, які відзначають сприятливий зв'язок між цифровою трансформацією та покращенням організаційної ефективності. R. A. Maalem Lahcen et al. [3] розглядають кіберпростір як складне середовище взаємодії людей, програмного забезпечення та мереж і пропонують системний погляд на ненавмисну-навмисну-зловмисну (Unintentional-Intentional-Malicious, UIM) поведінку в системі кібербезпеки. Людська помилка трактується авторами як аномалія взаємодії, яку слід розглядати на найвищому рівні таксономії загроз. Автори наголошують на необхідності міждисциплінарного підходу, що поєднує IT-безпеку, кримінологію, психологію та управління людськими ресурсами.

Результати досліджень Cram, W. A., D'Arcy, J., Proudfoot, J. [4] доводять, що позитивне ставлення та особисті переконання працівників щодо політик та дотримання вимог є найбільш прогнозованими сферами в системі управління інформаційною безпекою. Важливе значення для нашого дослідження мають результати, представлені в наукових публікаціях N. B. Balagopal, S. K. Mathew [5]. Вчені здійснили системний аналіз наукових джерел та виявили фактори, які впливають на наміри співробітників:

1) дотримуватися вимог інтернет-провайдера;
2) порушувати їх;
3) спільні фактори, які одночасно сприяють як порушенню, так і дотриманню співробітниками вимог інтернет-провайдера.

На окрему увагу заслуговують також дослідження, в яких показано, що причиною недотримання правил безпеки є не лише суб'єктивні фактори поведінки персоналу, а й дизайн самої політики, який часто ускладнює її сприйняття та виконання. Зокрема, зарубіжні вчені E. Rostami, F. Karlsson [6] виявили, що якість формулювань самого документа політики інформаційної безпеки є визначальним чинником: нечіткість інструкцій генерує об'єктивні підстави для їхнього невиконання, незалежно від мотивації службовця. Цю позицію підтверджують результати дослідження M. Niemimaa [7]. Вчений доводить, що дотримання і недотримання правил безпеки є нормативно амбівалентними категоріями: «правильність» відповідності залежить від адекватності самих процедур конкретному контексту.

У цілому ж, розглянуті дослідження актуалізують необхідність вивчення поведінкових моделей інформаційної безпеки для формування та реалізації якісних політик інформаційної безпеки органів публічної влади.

3. Problem Statement

Вчені B. K. Gebremeskel, G. M. Jonathan, S. D. Yalew фіксують перелік специфічних проблем інформаційної безпеки, що виникають у процесі цифрових трансформацій організацій, ключовими серед яких є: фінансові обмеження, ризик порушень безпеки, обмежений контроль над даними та потреба в динамічному управлінні безпекою [1]. При цьому, функціонуючі системи захисту інформаційної та кібербезпеки органів публічної влади здебільшого орієнтовані на технічні контрзаходи. В той час, як представлені у працях R. A. Maalem Lahcen, B. Caulkins, R. Mohapatra, M. Kumar [3], O. Ogbanufe, R. Crossler E., D. Biros [2] докази засвідчують, що на практиці 95% порушень інформаційної безпеки спричинені людськими помилками.

За результатами досліджень A. Sharma, A. Koohang, S. P. Sungh, вчені, практики та політики одностайні в тому, що розуміння причин, які впливають на дотримання або порушення вимог, може допомогти у розробці та впровадженні надійних програм і політик інформаційної безпеки, розвитку культури обізнаності з інформаційною безпекою та запобіганню порушенням безпеки [8].

З огляду на викладене, формування науково обґрунтованої політики інформаційної та кібербезпеки потребує обов'язкового врахування багатовимірного характеру людської поведінки та забезпечення належного регулювання поведінкової інформаційної безпеки в органах публічної влади.

Метою дослідження є порівняльний аналіз провідних поведінкових моделей інформаційної та кібербезпеки і розроблення на їх основі рекомендацій з удосконалення поведінкової інформаційної безпеки органів публічної влади в умовах цифрових трансформацій.

На досягнення мети визначено та виконано такі завдання:

1) здійснено огляд, порівняльний аналіз та систематизацію провідних поведінкових моделей інформаційної та кібербезпеки;

2) запропоновано та обґрунтовано рекомендації з удосконалення поведінкової, інформаційної та кібербезпеки органів публічної влади в умовах цифрових трансформацій.

4. Methods and Materials

Методологічне підґрунтя даного дослідження становлять системний та міждисциплінарний підходи, методи структурного та порівняльного аналізу, синтезу та моделювання. Базовою для даного дослідження є концепція поведінкової кібербезпеки R.A. Maalem Lahcen, B. Caulkins, R. Mohapatra, M. Kumar [3], що дозволяє розглядати інформаційний та кіберпростір органів публічної влади як складне системне явище, що охоплює взаємодію людей, програмного забезпечення та мережі, необхідні для реалізації владних повноважень та публічних функцій в умовах цифрових трансформацій.

Поєднання системного та структурованого підходів дозволяє розглядати поведінкову безпеку, з одного боку, як цілісне системне явище з лише їй притаманними структурними компонентами, а з іншого боку, як підсистему в системі інформаційної та кібербезпеки органів публічної влади.

Застосування полідисциплінарного підходу зумовлено тим, що дослідження поведінкової інформаційної безпеки як складного явища потребує міждисциплінарних знань (передусім

психології, кримінології, організаційної поведінки та ін.) для пояснення причин дотримання чи недотримання співробітниками політики інформаційної безпеки.

Оскільки різні галузі пропонують різні пояснення причин, які впливають на поведінку людини, застосування порівняльного аналізу, синтезу та інтеграції теорій з різних галузей покликано забезпечити комплексний підхід для пояснення намірів співробітників дотримуватися вимог, а також пояснення поведінки, пов'язаної з порушенням правил. Такий підхід дозволяє з'ясувати основні фактори та теорії, які можуть впливати на обидві форми поведінки N. B., Balagopal, S. K. Mathew [5].

Джерельною основою даного дослідження слугують наукові публікації з бази Scopus. Пошук, попередній аналіз та відбір списку наукових публікацій здійснено з використанням ресурсу Scopus AI. Достовірність та точність даних, отриманих за допомогою Scopus AI, перевірена та підтверджена автором

5. Results and Discussion

Поведінка людини традиційно вважається однією з головних загроз інформаційній безпеці протягом останніх трьох десятиліть. Наукова проблема поведінки персоналу у сфері інформаційної безпеки розробляється у кількох взаємопов'язаних напрямах, які становлять теоретичну основу цього дослідження:

1) традиційні когнітивні моделі;
2) багатовимірні операційні моделі;
3) моделі управління ризиками.

5.1. Традиційні поведінкові теорії (knowledge–attitude–behavior, KAB)

Історично розуміння безпекової поведінки працівників базувалося на когнітивному підході, фундаментом якого виступила теорія обґрунтованої дії (Theory of Reasoned Action, TRA) M. Fishbein, I. Ajzen [9] та теорія запланованої поведінки (Theory of Planned Behavior, TPB) I.Ajzen [10]. Відповідно до теорії запланованої поведінки характер поведінки визначається намірами, що формуються під впливом ставлення людини до поведінки та суб'єктивних норм. Зокрема, B.Bulgurcu, H Cavusoglu, I Benbasat довели, що раціональні переконання службовців є значущими індикаторами наміру дотримуватися вимог політик інформаційної безпеки [11].

Досить часто традиційний управлінський підхід до забезпечення інформаційної та кібербезпеки базується на жорсткому регламентуванні, що найкраще описано в загальній теорії стримування (General Deterrence Theory, GDT) [12]. Розроблена в галузі кримінології для пояснення поведінки або наміру, у 1980-х роках теорія стримування була запозичена для досліджень в галузі інформаційної безпеки. Згідно з цією теорією, страх перед майбутнім покаранням диктує дії, які люди обирають. Суб'єкти утримуються від порушень через суворість покарань.

На сьогодні теорія стримування залишається однією з найбільш часто використовуваних теорій у дослідженнях безпеки інформаційних систем. Дослідники J. D'Arcy, T. Herath [13] підтверджують значну доказову базу цієї теорії, хоча й вказують на її фрагментарність. За розумінням поведінки як реакції на покарання, ефективність інформаційної та кібербезпеки найчастіше спрямовується на забезпечення нормативно-правового регулювання та адміністративного контролю. Основним недоліком цієї моделі називають ігнорування ролі позитивної мотивації як фактора поведінки людини та емоційного виміру загрози.

Щоб компенсувати обмеження теорії стримування, управлінці часто звертаються до теорії мотивації захисту (Protection Motivation Theory, PMT) RW. Rogers [14], яка охоплює оцінку загроз (серйозність і вразливість) та оцінку реагування (ефективність реагування і самоефективність).

5.2. Багатовимірні операційні моделі

Все частіше в ході наукових пошуків вчені застосовують та обґрунтовують переваги інтегративних підходів у дослідженні безпекової поведінки. Зокрема, T. Herath, H. R. Rao доводять успішність результатів від застосування теорії мотивації у поєднанні із загальною теорією стримування [15]. G. D. Moody, M. Siponen, S. Pahnila, A. Toward [16] запропонували уніфіковану модель дотримання політики інформаційної безпеки (unified model of information security policy compliance, UMISPC), що синтезує одинадцять поведінкових теорій і виокремлює

рольові цінності службовця як найсильніший фактор наміру виконувати вимоги безпеки. Ключовим внеском цієї праці є розмежування між «наміром» (проактивна відповідність) і «реактивним опором» (заперечення проблем безпеки) як самостійними результатами, що вимагають різних управлінських рішень.

Уніфікована модель дотримання політики інформаційної безпеки UMISPC пройшла емпіричну перевірку у шведських державних установах. На основі результатів такої перевірки M. Gerdin [17] підтвердив, що в публічному секторі рольові цінності й соціальні норми мають вищу пояснювальну силу, ніж санкції.

У зв'язку зі зростанням актуальності завдань щодо удосконалення політики інформаційної безпеки та впливом поведінки людини на її забезпечення, значна увага у дослідженнях була присвячена розробленню шкал вимірювання політики інформаційної безпеки. У 2023 році вчені R. Rohan, D. Pal, J. Hautamäki, S. Funilkul, W, Chutimaskul та H. Thapliyal [18] здійснили системний огляд літератури, присвяченої вивченню обізнаності у сфері інформаційної безпеки, та запропонували дев'ятивимірну операційну рамку вимірювання обізнаності з інформаційної безпеки (Таблиця 1).

Таблиця 1. Операційна рамка вимірів обізнаності з інформаційної безпеки

Вимірів політики інформаційної безпеки	**Обізнаність та поведінкові практики**
Управління паролями (password management)	Створення надійних паролів, їх регулярна зміна та нерозголошення
Використання соціальних мереж (social media use)	Безпечна поведінка в соціальних мережах, зокрема захист особистих даних та обережність щодо шкідливого контенту
Використання електронної пошти (email use)	Розпізнавання фішингових листів і безпечне поводження з вкладеннями та посиланнями від невідомих відправників
Використання інтернету (internet use)	Обізнаність щодо ризиків при роботі в мережі, включно з доступом до підозрілих веб-сайтів та незахищених мереж
Доступ до даних та поводження з інформацією (data access and information handling)	Безпечне зберігання, передача та обробка конфіденційних даних організації
Звітування про інциденти (incident reporting)	Знання і готовність до своєчасного повідомлення про підозрілі події або порушення безпеки
Оновлення та захист пристроїв (updating and device securement)	Практика регулярного оновлення програмного забезпечення та фізичного й програмного захисту пристроїв
Використання мобільних пристроїв (mobile device use)	Безпечні практики при роботі зі смартфонами та іншими мобільними пристроями
Обізнаність із політиками та індивідуальні обов'язки (awareness of policies and individual responsibilities)	Розуміння співробітниками своїх обов'язків і дотримання всіх організаційних правил та процедур інформаційної безпеки.

Джерело: складено автором на основі [**Ошибка! Источник ссылки не найден.**].

Для забезпечення прозорості запропонованої моделі, автори сформували підвиміри кожного з вимірів обізнаності щодо інформаційної безпеки (рис. 1).

Як показано на рис. 1, рамка вимірів охоплює весь спектр конкретних технологічних практик (загалом 34 підвиміри) і слугує ґрунтовним діагностичним каталогом поведінкових індикаторів обізнаності з інформаційної безпеки.

Подальша операціоналізація запропонованої структури у вимірювальному інструменті та експериментальна перевірка методики сприяли тому, що у 2025 році R. Rohan, D. Pal, J. Hautamäki, S. Funilkul, W. Chutimaskul, H. Thapliyal [19] запропонували п'ятикомпонентну вимірювальну шкалу, яка інтегрує всі представлені у попередній моделі поведінкові практики у більш абстраговані та теоретично обґрунтовані конструкти: знання (knowledge), ставлення (attitude), поведінка (behavior), індивідуальна відповідальність (individual responsibility) та соціальний вплив (social influence).

Важливою перевагою оновленої рамки є те, що вона враховує відмінності між різними соціальними групами та забезпечує можливості для вимірювання обізнаності з інформаційної безпеки для кожної групи. Це дозволяє пріоритизувати ресурси не лише з урахуванням найбільш важливих напрямів – від знань до соціального впливу, але й визначати ключові завдання

політики інформаційної безпеки на основі персональних особливостей представників різних груп.

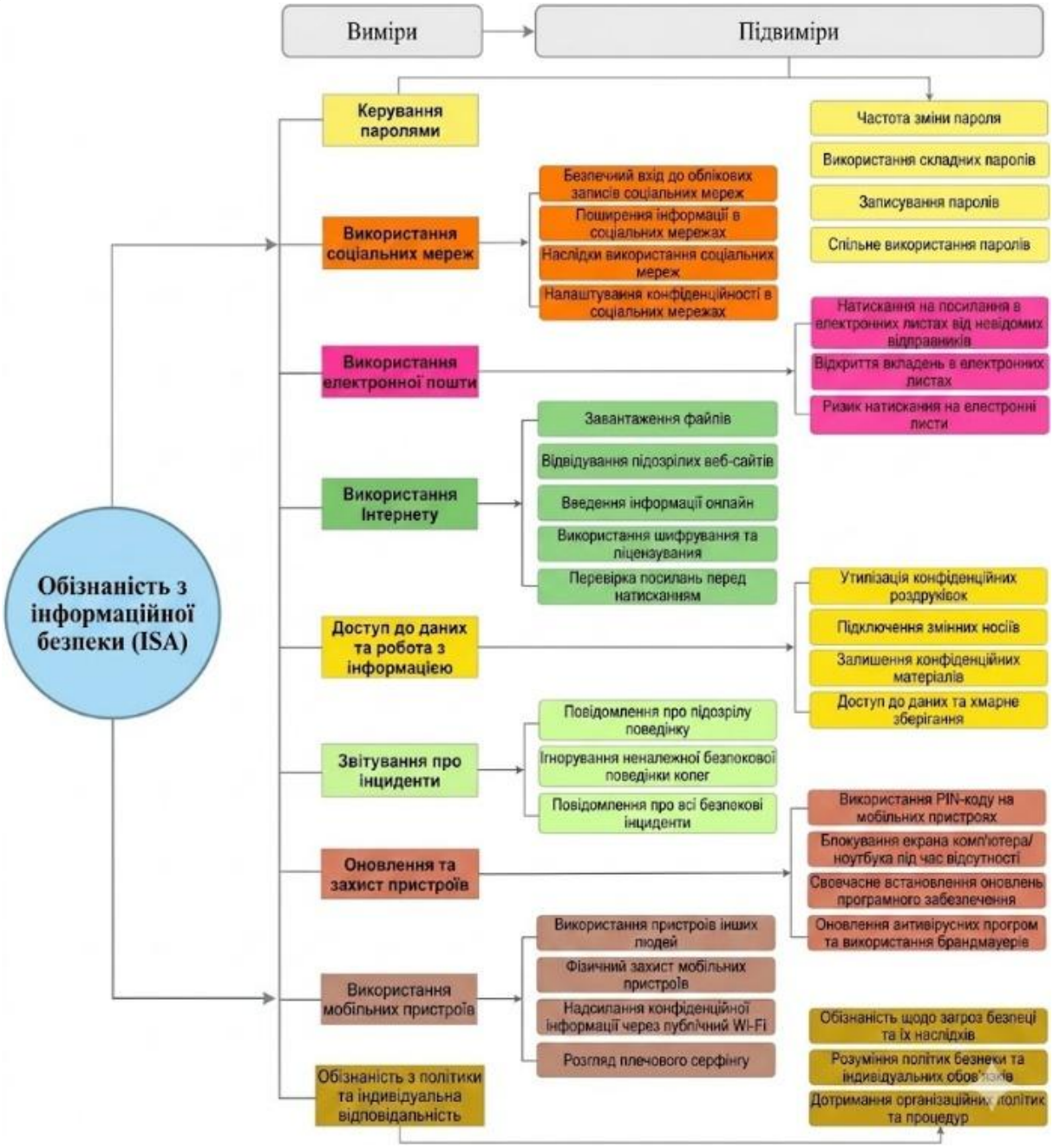

Рисунок 1. Виміри та підвиміри ISA

Джерело: [**Ошибка! Источник ссылки не найден.**]

На окрему увагу у нашому дослідженні заслуговує вивчення концептуальної рамки для дослідження управлінського ландшафту інформаційної безпеки, запропонованої S. Goodman, D. W. Straub, R. Baskerville, R. Baskerville. При побудові стратегій безпеки, вчені розмежовують два критерії [20]:

1) критерій продукту – орієнтований на досягнення фіксованого захищеного стану як кінцевого результату;

2) критерій процесу – трактує безпеку як динамічну організаційну практику, що постійно адаптується до змінних загроз.

Саме процесний критерій в системі управління інформаційною безпекою, на думку авторів, є концептуально більш адекватним, оскільки жодна організація не може досягти остаточного стану захищеності – вона може лише підтримувати безпекову зрілість як безперервну інституційну функцію. У межах процесної концепції вчені виокремлюють три взаємопов'язані складові управління інформаційною безпекою:

1) стратегічне планування;
2) управління ризиками;
3) забезпечення відповідності.

Відповідність охоплює два взаємопов'язані напрями [20]:

1) відповідність зовнішнім регуляторним вимогам, що формуються на наддержавному та державному рівнях: виконання вимог міжнародних договорів, стандартів ISO, галузевих стандартів і практик, законів про інформаційну безпеку, забезпечення національної безпеки, захист персональних даних, вимоги публічного розкриття інформації та ін.;

2) відповідність внутрішньо організаційним вимогам: встановлення та дотримання організаційних етичних стандартів «належної турботи» (due care) щодо захисту інформації як стандарту відповідального управління, якого від них очікує широке коло стейкхолдерів.

5.3 Моделі управління ризиками та інформаційна безпека

Окрему групу моделей управління інформаційною безпекою складають концепції, засновані на теорії управління ризиками. Розглядаючи управління ризиками як безперервний процес, E. Wheeler запропонував семиетапну циклічну програму як операційну основу програм безперервного управління інформаційною безпекою, що охоплює такі цикли [21]:

1) профілювання критичних ресурсів – ідентифікація активів, що потребують захисту, із визначенням їхньої чутливості за принципом аналізу впливу на організацію;
2) оцінювання найбільш вірогідних та значущих ризикових впливів;
3) визначення найбільш доцільного способу реагування на ризик;
4) документування результатів та обґрунтування прийнятих рішень;
5) реалізація плану пом'якшення ризику;
6) верифікація результатів – підтвердження того, що ризик було знижено до очікуваного рівня;
7) моніторинг середовища на предмет змін, що потребують переоцінки.

Адаптація методики до специфіки функціонування інформаційних систем в органах публічної влади дозволяє побудувати безперервну, доказово обґрунтовану та адаптивну програму управління ризиками на основі врахування пріоритетності публічних функцій та владних повноважень, забезпечення регуляторних вимог і підзвітності щодо дотримання міжнародних, національних та інституційних стандартів інформаційної безпеки.

Важливим внеском у вирішення проблеми ефективності політик інформаційної безпеки є обґрунтована K. Razikin, B. Soewito [22] модель для проєктування підтримки рішень у сфері кібербезпеки. Інтеграція аналізу ризиків із вимогами ISO/IEC 27001 дозволяє органам публічної влади визначати пріоритети захисту не формальними вимогами відповідності, а реальним профілем загроз. Така концепція відповідає логіці комплексного підходу до формування політики інформаційної безпеки та ефективного використання публічних ресурсів для її реалізації. За задумом авторів, запропонована модель спрямована на отримання найкращої системи безпеки шляхом зменшення загроз.

6. Conclusions

Узагальнення результатів проведеного дослідження дає підстави для таких висновків.

1. Теоретичну основу поведінкових моделей регулювання інформаційної та кібербезпеки в органах публічної влади становлять:

1) традиційні когнітивні моделі (теорія мотивації захисту R. W. Rodgers [14]; теорія стримування J. P. Gibbs [12]; теорія мотивації поведінкової інформаційної та кібербезпеки R. A. Maalem Lahcen та ін. [3]);

2) багатовимірні операційні моделі (дев'ятикомпонентна поведінкова рамка обізнаності з інформаційної безпеки R. Rohan та ін. [18]; п'ятикомпонентна шкала AIAS R. Rohan та ін. [19]);

3) моделі управління ризиками (управлінська рамкова модель S. Goodman та ін. [20]; семиетапний цикл E. Wheeler [21]; модель підтримки рішень на основі ISO/IEC 27001 K. Razikin та ін. [22]).

2. Поведінкова модель управління інформаційною безпекою в органах публічної влади виступає як система організаційних, регуляторних та освітніх механізмів, спрямованих на формування, вимірювання та корекцію інформаційної безпекової поведінки акторів

інформаційного простору для мінімізації людського чинника як джерела системних вразливостей організаційної інформаційної системи.

3. Порівняльний аналіз існуючих поведінкових моделей дає підстави для рекомендацій щодо удосконалення управління інформаційною поведінковою безпековою органів публічної влади шляхом:

– використання міждисциплінарного підходу до аналізу людського чинника як основного джерела вразливостей в системі управління інформаційною безпекою органів публічної влади;

– застосування верифікованих багатовимірних шкал оцінювання інформаційно-безпекової обізнаності персоналу з метою формування управлінських рішень щодо пріоритетності програм підвищення безпекової компетентності;

– забезпечення управління інформаційною безпекою як безперервного організаційного процесу в органах публічної влади, а не сукупності окремих технічних заходів;

– інтеграції зовнішніх регуляторних стандартів із внутрішніми етичними правилами «due care» як єдиної системи забезпечення ефективності управління інформаційною безпекою органів публічної влади в умовах множинних і динамічно змінюваних нормативних приписів.

Невід'ємним компонентом ефективного управління є наявність чітких зрозумілих «практичних порад» (actionable advice) – інструкцій, які однозначно окреслюють дозволені та заборонені дії щодо конкретних робочих завдань, пов'язаних з ризиками для інформаційної безпеки в органах публічної влади в умовах цифрових трансформацій.

References

1. Gebremeskel, B. Kasahun, Jonathan, G. Mekonnen, & Yalew, S. Demesie (2023). Information security challenges during digital transformation. *Procedia Computer Science*, (219), 44–51. https://doi.org/10.1016/j.procs.2023.01.262
2. Ogbanufe, O., Crossler, R. E., & Biros, D. (2023). The valued coexistence of protection motivation and stewardship in information security behaviors. *Computers & Security*, (124), Article 102960. https://doi.org/10.1016/j.cose.2022.102960
3. Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, *3*(1), Article 10. https://doi.org/10.1186/s42400-020-00050-w
4. Cram, W. A., D'Arcy, J., & Proudfoot, J. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, *43*(2), 525–554. https://doi.org/10.25300/misq/2019/15117
5. Balagopal, N., & Mathew, S. K. (2024). Exploring the factors influencing information security policy compliance and violations: A systematic literature review. *Computers & Security*, (147), Article 104062. https://doi.org/10.1016/j.cose.2024.104062
6. Rostami, E., & Karlsson, F. (2024). Qualitative content analysis of actionable advice in information security policies — introducing the keyword loss of specificity metric. *Information & Computer Security*, *32*(4), 492–508. https://doi.org/10.1108/ICS-10-2023-0187
7. Niemimaa, M. (2024). Incorrect compliance and correct noncompliance with information security policies: A framework of rule-related information security behaviour. *Computers & Security*, (145), Article 103986. https://doi.org/10.1016/j.cose.2024.103986
8. Sharma, A., Koohang, A., & Singh, S. P. (2025). Information security policy compliance: A structured review using scientometric analysis and topic modeling. *Journal of Global Information Management*, *33*(1), 1–32. https://doi.org/10.4018/JGIM.389715
9. Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Addison-Wesley. https://people.umass.edu/aizen/f&a1975.html
10. Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T
11. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. https://www.academia.edu/download/30987003/bulgurcucavusoglubenbasat.pdf
12. Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. Elsevier. https://archive.org/details/crimepunishmentd0000gibb

13. D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643–658. https://doi.org/10.1057/ejis.2011.23
14. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803
15. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6
16. Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1), 285–311. https://doi.org/10.25300/MISQ/2018/13853
17. Gerdin, M. (2025). Validating and extending the unified model of information security policy compliance. *Information and Computer Security*, *33*(1), 25–48. https://doi.org/10.1108/ICS-12-2023-0263
18. Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon*, *9*(3), Article e14234. https://doi.org/10.1016/j.heliyon.2023.e14234
19. Rohan, R., Chutimaskul, W., Roy, R., et al. (2025). Developing a scale for measuring the information security awareness of stakeholders in higher education institutions. *Education and Information Technologies*, *30*(10), 13713–13777. https://doi.org/10.1007/s10639-024-13307-5
20. Goodman, S., Straub, D. W., Baskerville, R., & Baskerville, R. (2008). *Information security: Policy, processes, and practices* (1st ed.). Routledge. https://doi.org/10.4324/9781315288697
21. Wheeler, E. (2011). The risk management lifecycle. In *Security Risk Management* (pp. 43–60). Elsevier. https://doi.org/10.1016/B978-1-59749-615-5.00003-7
22. Razikin, K., & Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Egyptian Informatics Journal*, *23*(3), 383–404. https://doi.org/10.1016/j.eij.2022.03.001