DOI: 10.46299/ISG.2024.MONO.ECON.2.8.3

8.3 Забезпечення захисту цифрових технологій в публічному управлінні

Вступ. У сучасному світі, де інформаційні технології проникають у всі сфери життя, безпека використання цих технологій у публічному управлінні стає вкрай важливою проблемою. Створення безпечних умов для використання інформаційних технологій має першочергове значення для забезпечення надійності, конфіденційності та цілісності даних, що використовуються у різних державних інституціях. В епоху «Індустрії 4.0», яка характеризується складними мережевими технічними засобами, потрібні гнучкі практики безпеки, які потребують нового системного розуміння безпеки. Оцінка ризиків більше не обмежуються оцінкою індивідуальних факторів ризику для машин, обладнання, що працює під тиском, захисту від вибуху, протипожежного захисту та передачі даних. Натомість управління ризиками вимагає комплексного розгляду інтерфейсів і системного підходу до безпеки. Розвиток мегатренду підключення також тягне за собою додаткові системні небезпеки та ризики, наприклад, у сфері кібербезпеки. Вагомий внесок у дослідженні інновацій у сфері державного управління здійснили А. Азарова [213], Н. Чередніченко [214], О. Хошаба [215], Л. Їнг [216], Н. Карпчук, Б. Юзьків, О. Пелех [217]. Дослідження ключових аспектів забезпечення безпеки в інформаційному просторі публічного управління, враховуючи сучасні виклики та стратегії, спрямовані на запобігання потенційним загрозам та атакам на інформаційні системи та дані державних органів набуває великого значення.

Виклад основного матеріалу. Сьогодні інновації та безпека розвиваються одночасно: симбіоз замість протиріччя. Новий тренд «Технологія довіри» привертає підвищену увагу. Майбутні технічні інновації повинні забезпечувати прозорість, довіру та безпеку – вимоги, які є необхідними для розвитку публічного управління. Застосування технологій штучного інтелекту, забезпечення безпеки телекомунікаційних мереж в умовах війни є важливим

фактором у формуванні стійкої інформаційної політики. Через дигіталізацію нинішнє оточення та умови для державного управління відчутно змінюються. Рамки для місткості, якості та одиничних витрат, що стосуються зберігання, обробки та комунікації даних, значно трансформуються. За останні роки витрати на використання інформаційних технологій падають, у той же час вдосконалюються можливості обробки, зберігання та комунікації даних. Внаслідок цього в переважно технологічно орієнтованому розвитку з'являються нові пропозиції, сервіси та платформи, доступні світовому співтовариству через Інтернет та хмарні обчислення, що також може мати руйнівний вплив на структури та процеси організацій.

За останні роки спостерігається стабільний та значний ріст у користувачів інтернету у всьому світі. З 2005 по 2023 рік кількість користувачів зросла з 1,023 мільярда до 5,400 мільярда осіб, а частка населення, яка користується інтернетом, збільшилася з 15,7% до 67,1%. Це свідчить про те, що інтернет стає все більш доступним та важливим засобом спілкування, навчання та розваг для людей у всьому світі (рис.1) [218-222]

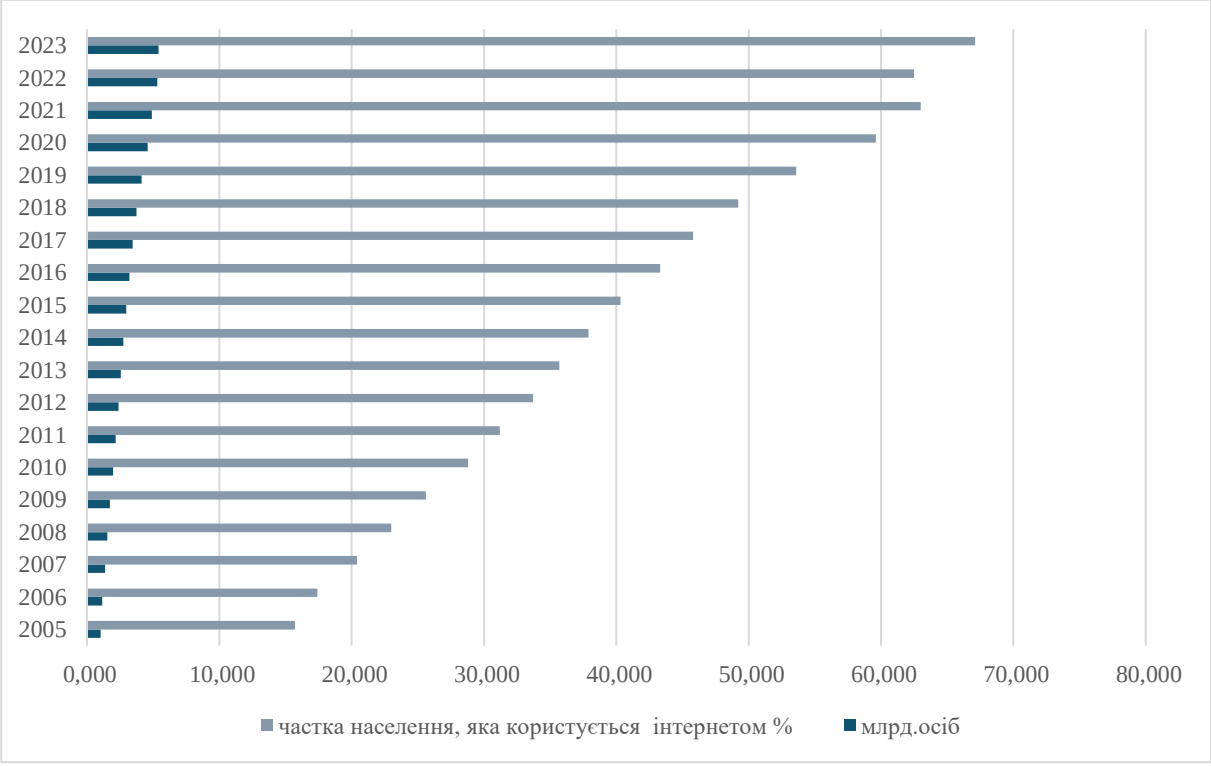

Рис.1 Динаміка і частка користувачів у світі за період з 2005 по 2023рр.

У минулому вже стало очевидним, що інформаційні системи стають цільовою зоною для атак. Це не тільки підтверджується нападами хакерів і крадіжками даних клієнтів і платежів у компаній. Державні організації також стали жертвами і все частіше стають об'єктом кібератак. Якщо державні органи у майбутньому будуть ще більше спиратися на цифрові технології при виконанні своїх обов'язків, атаки можуть завдати ще більше шкоди. Тому особлива увага повинна бути приділена безпеці архітектури та важливих систем із залученням штучного інтелекту. Також варто звернути увагу на те, що самі розробники додатків зі штучним інтелектом можуть вбудовувати в свої складні продукти певні додатки для отримання доступу до даних або навіть впливу на прийняття рішень. Цей аспект також потребує особливої уваги з боку держави.

Так, застосування штучного інтелекту можливе в різних ситуаціях. Через складну технологічну границю, здається, що більш цільовим є визначення ШІ на основі їх здатностей. Вони будуть описані як базові технології ШІ, оскільки вони надають основні здатності. Проте варто зауважити, що ШІ також можна описати з технічної точки зору. Наприклад, підходи до ШІ можна відрізнити за категоріями використовуваних методів навчання, архітектур систем та алгоритмів. Методи навчання ШІ включають глибоке навчання (Deep Learning), навчання з наглядом (Supervised Learning), навчання без нагляду (Unsupervised Learning), посилене навчання (Reinforcement Learning) та мета-навчання (Meta Learning). Системи та архітектури можна поділити на розумних агентів, експертні системи, системи підтримки прийняття рішень, системи управління правилами, штучні імунні системи та квантові логічні системи. Технології, на яких базуються ці системи, також дуже різноманітні. Окрім штучних нейронних мереж, можна використовувати Машини опорних векторів, можливісні мережі, багатоконтекстні системи або генетичні алгоритми.

ШІ -базоване сприйняття визначається як аналіз даних для виявлення змін в оточенні, настроїв і емоцій. Для цього система обробляє згенеровані (сенсорні) дані і відносить їх до категорій, щоб окремі дані могли бути агреговані в події або емоційні стани.

У випадку ШІ-базованих повідомлень, реакція системи є основним. Визначені шаблони, події або емоції використовуються для спрямованого сповіщення користувачів. Відповідно до призначених категорій, користувачі отримують сповіщення про події або стани, щоб вчасно реагувати на них відповідним чином.

ШІ-базовані рекомендації розширюють аналіз даних, щоб не тільки відобразити поточний стан, але також дати рекомендації щодо дій для користувача, спрогнозувати розвиток можливих подій. Для цього необхідно не тільки віднести дані до категорій, але також порівняти сприйнятий фактичний стан з бажаним станом, щоб на основі виявлених відхилень дати рекомендації щодо досягнення бажаного стану або уникнення ризиків.

Також ШІ можна використовувати для прогнозів і передбачень. Виходячи з виявлених у даних шаблонів, можна зробити прогнози щодо подальшого розвитку, які будуть надані користувачеві на відповідному рівні деталей.

Коли ці основні питання будуть вирішені, на операційному рівні виникне завдання класифікації адміністративних процедур з точки зору їх придатності для підтримки або автоматизації. Оскільки існує різноманітність підходів на основі штучного інтелекту, можна припустити, що багато процесів потребуватимуть перегляду. Для цього важливо забезпечити баланс між технічною експертизою, законодавством і практичним досвідом у сфері управління. На законодавчому рівні необхідно обумовити використання ШІ, тоді стане можливо застосування цих систем штучного інтелекту в різних місцевостях через центри обробки даних або хмарні сервіси як спільно використовувані сервіси. Забезпечення безпеки вже є фундаментальною передумовою сталого розвитку.

Ще одною важливою складовою є створення безпекових умов у застосування телекомунікаційних технологій. Функціонуюча адміністрація є важливою для громадян та економіки, тому державні та місцеві органи та адміністрації слід визначити як критичну інфраструктуру у публічному секторі. Безпека телекомунікацій у публічному секторі включає в себе комплекс заходів, спрямованих на захист інформації, що передається, оброблюється та зберігається

у системах телекомунікаційних та інформаційних мереж. Основна мета безпеки телекомунікацій полягає у забезпеченні конфіденційності, цілісності та доступності інформації, а також у захисті від несанкціонованого доступу, втрати чи пошкодження даних.

У публічному секторі, де обробка та передача великих обсягів чутливої інформації, такої як особисті дані громадян, фінансова інформація, державні секрети тощо, є надзвичайно важливою, безпека телекомунікацій відіграє критичну роль. Адже досліджуючи індекс розвитку електронного врядування, одним із складових є індекс розвитку телекомунікаційної інфраструктури. Загострена увага до розвитку телекомунікаційної інфраструктури пов'язана із війною в Україні, адже – це є і інформаційна війна. Індекс телекомунікаційної інфраструктури в Україні від 2003 до 2022 року зріс з 0,11568 до 0,727, що свідчить про значний прогрес у розвитку телекомунікаційних технологій та інфраструктури в країні протягом цього періоду (рис.2) [222].

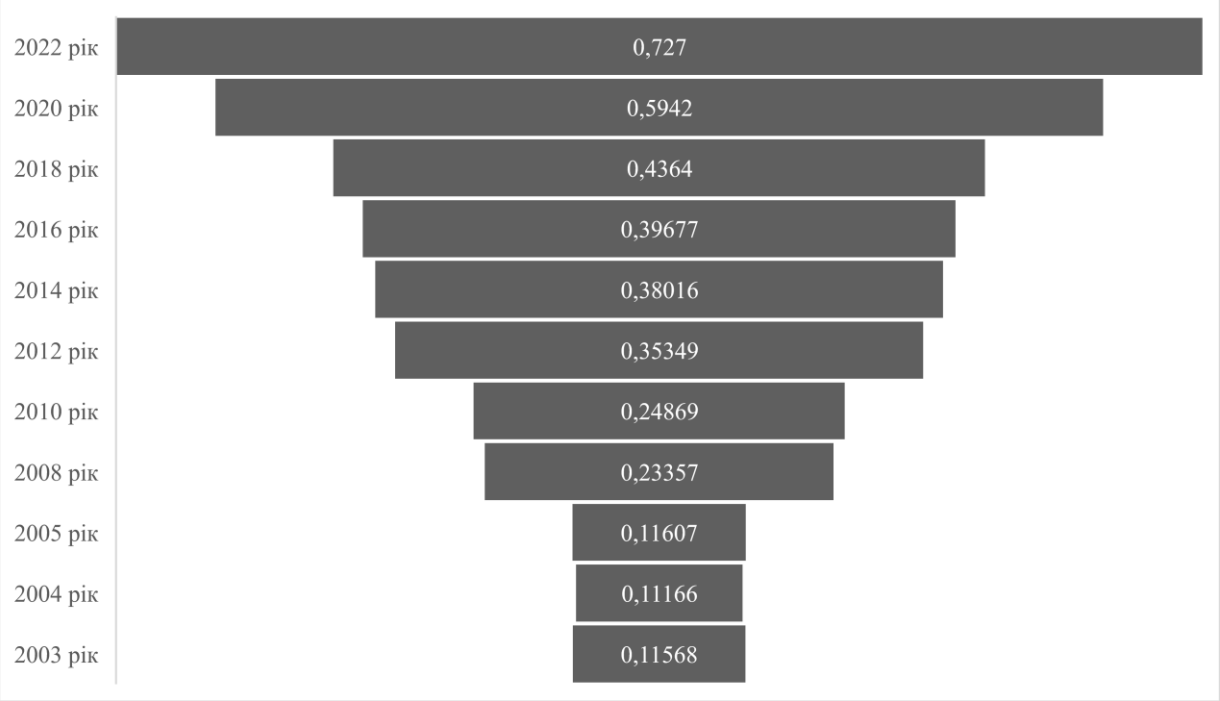

Рис.2 Динаміка індексу розвитку телекомунікаційної інфраструктури в Україні за період з 2003-2022рр.

Інформаційна безпека в публічному управлінні, зокрема в телекомунікаційній складовій, є важливою складовою сучасного

адміністративного процесу. Безпека має на меті забезпечити конфіденційність, цілісність та доступність інформації, а також запобігти небажаним атакам та втратам даних. Успішна реалізація інформаційної безпеки у публічному управлінні дозволить забезпечити ефективність роботи державних структур, підвищити рівень довіри громадян до владних органів, та забезпечити стабільність та надійність державних інформаційних систем. можна виділити групи користувачів та їхні потреби в безпеці. Клієнти та абоненти вимагають впевненості у мережі та послугах, особливо в доступності екстрених послуг. Громадськість та органи влади вимагають захисту через директиви та законодавство для забезпечення доступності послуг, приватності та справедливої конкуренції. Оператори мереж та постачальники послуг потребують безпеки для захисту своєї діяльності та бізнес-інтересів, виконання зобов'язань перед клієнтами, партнерами та громадськістю.

Щодо активів для захисту, вони включають комунікаційні та обчислювальні послуги, інформацію та дані, персонал, а також обладнання та споруди. Загрози безпеки, на які потрібно звернути увагу, включають несанкціоноване розкриття інформації, несанкціоноване знищення або модифікація даних, переривання чи відмова в наданні послуг, а також відображення або видача себе за авторизовану сутність (таблиця 1).

Таблиця 1.

Складові інформаційної безпеки в публічному управлінні

Група користувачі в/зацікавлені сторони	**Потреба в безпеці**	**Активи для захисту**	**Потенційні загрози безпеки**
Клієнти/абоненти	Впевненість у мережі та послугах, особливо в доступності екстрених послуг.	Комунікаційні та обчислювальні послуги	Несанкціоноване розкриття інформації, несанкціоноване знищення або модифікація даних, переривання чи відмова в наданні послуг

Продовження таблиці 1

Громадськість/органи влади	Захист через директиви та законодавство, щоб забезпечити доступність послуг, приватність та справедливу конкуренцію.	Інформація та дані, персонал, обладнання та споруди	Несанкціоноване розкриття інформації, несанкціоноване знищення або модифікація даних, переривання чи відмова в наданні послуг, відображення або видача себе за авторизовану сутність
Оператори мереж та постачальники послуг	Безпека для захисту діяльності та бізнес-інтересів, виконання зобов'язань перед клієнтами, партнерами та громадськістю.	Комунікаційні та обчислювальні послуги, інформація та дані, персонал, обладнання та споруди	Несанкціоноване розкриття інформації, несанкціоноване знищення або модифікація даних, переривання чи відмова в наданні послуг, відображення або видача себе за авторизовану сутність

Уразливість безпеки - це дефект або слабкість, яка може бути використана для порушення системи чи інформації, яку вона містить, а, також, несанкціонований доступ до даних. Якщо уразливість існує, то можлива реалізація загрози з успіхом, якщо в системі немає ефективних засобів протидії. Основна візія полягає в розробці систематичної, всебічної та послідовної загальної системи, яка відображається як керівна ідея з самого початку процесу стандартизації.

Інформаційні технології та телекомунікації в сучасному публічному управлінні є необхідними засобами для забезпечення ефективного функціонування та взаємодії різних гілок влади, органів державного управління та громадськості.

Важливо виділити основні умови створення безпекових умов для використання інформаційних технологій в публічному управлінні.

- впровадити роль відповідальну за нагляд, управління та операції інформаційної безпеки - керівник відділу IT-безпеки, директор з IT-безпеки, головний менеджер з інформаційної безпеки – CISO (Chief Information Security Officer).
- розробка та впровадження комплексних заходів забезпечення кібербезпеки, включаючи виявлення та запобігання кібератакам, захист від витоку даних та шкідливих програм, зокрема розробка системи стандартизації та використання відповідного обладнання;
- використання сучасних методів шифрування для захисту конфіденційної інформації та забезпечення цілісності даних під час їх передачі та зберігання;
- розробка систем аутентифікації та контролю доступу, розмежування рівнів доступу (Role Based Access Control) до інформаційних ресурсів для забезпечення легітимного доступу та захисту від несанкціонованого втручання;
- впровадження систем моніторингу та аналізу безпеки для вчасного виявлення потенційних загроз та інцидентів безпеки з підключенням ШІ-рішень;
- розробка стратегій резервного копіювання даних та планів відновлення після аварій та інцидентів (Business Continuity Plan, Disaster Recovery Plan);
- захист фізичного доступу до обладнання та інфраструктури, включаючи зони з обмеженим доступом та моніторинг відвідувачів
- розробка процедур управління інцидентами та планів реагування на кіберзагрози та інші інциденти безпеки;
- регулярне проведення тренінгів та навчань з питань кібербезпеки для персоналу та користувачів інформаційних систем.
- системне і чітке дотримання законодавства в сфері захисту персональних даних та доступу до державної таємниці.

Висновки. Створення безпечних умов для використання інформаційних технологій в публічному управлінні передбачає реалізацію комплексу заходів, спрямованих на забезпечення кібербезпеки, захисту від кібератак, витоку даних

та інших шкідливих програм. Для цього важливо впровадити сучасні методи шифрування, які забезпечують захист конфіденційної інформації та цілісність даних. Також важливо розробити системи аутентифікації та контролю доступу, що забезпечать легітимний доступ та захист від несанкціонованого втручання. Не менш важливим є впровадження систем моніторингу та аналізу безпеки для вчасного виявлення потенційних загроз та інцидентів безпеки.

Крім того, необхідно розробляти стратегії резервного копіювання даних та плани відновлення після аварій та інцидентів, щоб забезпечити надійність інформаційних систем у випадку непередбачених ситуацій. Захист фізичного доступу до обладнання та інфраструктури, включаючи моніторинг відвідувачів, також є важливим елементом безпеки.

Крім технічних аспектів, важливо розробляти процедури управління інцидентами та плани реагування на кіберзагрози та інші інциденти безпеки. Комплексний підхід до навчання та підвищення обізнаності персоналу та користувачів інформаційних систем з питань кібербезпеки також грає важливу роль у забезпеченні безпеки у цьому контексті.