**Лазарів Владислав Олегович**

*аспірант кафедри управління та бізнес адміністрування, Прикарпатський національний університет імені Василя Стефаника,* [*https://orcid.org/0009-0008-6812-6124*](https://orcid.org/0009-0008-6812-6124)

**Політики захисту даних у публічному секторі: кращі світові практики для безпеки електронних послуг**

У сучасному світі публічне управління активно трансформується під впливом цифровізації, а електронні послуги стають важливим інструментом комунікації між державою та громадянами. Захист інформації стає важливим фактором довіри, особливо з огляду на зростання обсягів чутливих персональних даних, які обробляються державними установами. Забезпечення кібербезпеки та впровадження ефективних політик захисту даних стає пріоритетним завданням для органів публічного управління.

Метою роботи є дослідження кращих світових практик у сфері захисту даних у публічному секторі, оцінка їхнього потенціалу для підвищення безпеки електронних послуг.

Захист даних у публічному секторі передбачає застосування правових, технічних і організаційних заходів для забезпечення конфіденційності, цілісності та доступності інформації. Ключовими принципами захисту даних є [1]:

* *Прозорість:* громадяни мають право знати, які дані збираються, з якою метою і як вони обробляються.
* *Мінімізація даних*: збирання лише тих даних, які необхідні для виконання конкретних завдань.
* *Захист за дизайном*: інтеграція механізмів безпеки на етапі розробки систем.
* *Регулярний моніторинг і аудит*: перевірка дотримання стандартів захисту.

Основні вимоги до створення, впровадження, підтримки і постійного поліпшення захисту даних визначаються міжнародними стандартами, такими як ISO/IEC 27001 та адаптуються відповідно до національних правових систем.

Міжнародний досвід наочно демонструє різноманітність підходів до забезпечення захисту даних [2]. Так, найбільш всеосяжним стандартом у світі є Загальний регламент захисту даних (GDPR) у Європейському Союзі, який охоплює обробку персональних даних як у межах ЄС, так і за ними, якщо йдеться про дані громадян ЄС. Основними перевагами GDPR є чітке визначення прав громадян, обов’язків організацій, а також суворі санкції за недотримання вимог регламенту. У державному секторі держави-члени ЄС зобов’язані забезпечити впровадження політик захисту даних на всіх рівнях управління, що сприяє прозорості та підвищує довіру громадян.

У США велика увага приділяється кібербезпеці. Захист даних у державному секторі регулюється Федеральним законом про управління інформаційною безпекою (FISMA) та стандартами Інституту стандартів і технологій (NIST). Ця нормативна база створює рамкові умови для забезпечення безпеки інформації, з особливим акцентом на оцінці ризиків. Гнучкість підходу дозволяє адаптувати заходи захисту до специфіки конкретних організацій, що підвищує ефективність їх застосування.

Естонія є визнаним лідером у впровадженні електронного урядування. Естонія вважається однією з найуспішніших країн у впровадженні електронного уряду. Її система X-Road забезпечує безпечний обмін даними між державними установами та громадянами. Політика захисту даних базується на принципах прозорості, мінімізації даних та цифрових ідентифікацій.

Сінгапур також демонструє значний прогрес у сфері кібербезпеки та захисту даних за допомогою штучного інтелекту. Уряд країни інвестує значні ресурси у створення спеціалізованих агентств, які займаються моніторингом кіберзагроз і впровадженням освітніх програм для підвищення обізнаності громадян. Унікальним аспектом є тісна співпраця з приватним сектором, що сприяє впровадженню інноваційних рішень та розвитку передових технологій захисту даних.

Ці приклади демонструють різноманітність підходів до захисту інформації, що враховують особливості правових систем, технологічного розвитку та організаційної культури. Впровадження таких практик може стати основою для підвищення рівня безпеки даних і в інших країнах, зокрема в Україні.

Для України, яка стикається з низкою викликів у сфері захисту даних, важливим є використання досвіду цих країн. Низький рівень обізнаності громадян і посадових осіб про важливість захисту даних, недостатнє фінансування заходів кібербезпеки та потреба у гармонізації національного законодавства із міжнародними стандартами наразі є основними питаннями[3]. Для вирішення цих питань доцільним було б впровадження децентралізованих платформ для обробки даних, навчання і підвищення обізнаності населення, обмін досвідом з міжнародними партнерами та інше.

Аналіз кращих світових практик показав, що успішні політики захисту даних у публічному секторі базуються на прозорості, інтегрованих підходах та інноваціях. Впровадження кращих світових практик у сфері захисту даних сприятиме не лише підвищенню безпеки електронних послуг, але й зміцненню довіри громадян до державних інституцій. Для України важливо перейняти цей досвід, адаптуючи його до національних реалій, що дозволить підвищити безпеку електронних послуг, зміцнити довіру громадян і сприяти розвитку цифрового урядування.

**Список викорситаних джерел:**

1. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT).
2. Нагорняк М. ІНФОРМАЦІЙНА БЕЗПЕКА НАДАННЯ ЕЛЕКТРОННИХ ПОСЛУГ: СВІТОВИЙ ДОСВІД ПУБЛІЧНОГО УПРАВЛІННЯ. Наукові перспективи (Naukovì perspektivi). 2024. № 12(42). URL: <https://doi.org/10.52058/2708-7530-2023-12(42)-225-235> (дата звернення: 11.12.2024).
3. Лазарів В. КОНЦЕПТУАЛЬНІ ЗАСАДИ ПУБУЛІЧНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ЕЛЕКТРОННИХ ПОСЛУГ: ТЕОРІЯ ТА ВИКЛИКИ. Наукові перспективи (Naukovì perspektivi). 2023. № 6(36). URL: <https://doi.org/10.52058/2708-7530-2023-6(36)-143-150> (дата звернення: 12.12.2024).