4. European Court of Human Rights. CASE OF GUZZARDI v. ITALY. STRASBOURG. 6 November 1980. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57498%22]}

5. European Court of Human Rights. Eur. Court H.R., De Wilde, Ooms and Versyp Cases («Vagrancy» Cases), judgment of 18 November 1970 (Question of procedure). 18.06.1971 р. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57606%22]}

6. Конвенція про захист прав людини і основоположних свобод : Конвенція Ради Європи від 04.11.1950 р. : станом на 1 серп. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 26.04.2024).

Віктор Батіг

студент третього курсу освітньої програми

«Суспільне і приватне врядування», НаУКМА

ЕЛЕКТРОННЕ ВРЯДУВАННЯ В УКРАЇНІ: ЦИФРОВИЙ УРЯД, ТРАНСФОРМАЦІЙНІ РИЗИКИ, ТРЕНДИ РОЗВИТКУ

Ключові слова: цифровий уряд, електронне врядування, кібербезпека, захист персональних даних, ризики, тренди.

Мета дослідження полягає у виявленні та аналізі ризиків, які супроводжують процеси впровадження та експлуатації цифрового уряду.

Виклад основного матеріалу.

«Цифровий уряд» означає використання цифрових технологій як інтегрованої частини урядових стратегій. Він ґрунтується на використанні цифрової екосистеми країни для залучення урядових суб’єктів, неурядових організацій, бізнесу, громадянського суспільства та приватних осіб для підтримки виробництва та доступу до даних, послуг і контенту через взаємодію з урядом. Цифровий уряд поділяється на три категорії систем, які використовуються для управління внутрішніми системами та процесами, надання державних послуг та взаємодії із зацікавленими сторонами» [1].

Електронне врядування трансформує підходи держави до управління та надання послуг, впроваджуючи інформаційні технології для підвищення ефективності, прозорості та доступності. Водночас, ця технологічна трансформація супроводжується значними ризиками, які потребують ретельного аналізу та управління.

Одним із ключових аспектів у сфері електронного врядування є захист персональних даних. Регулювання, такі як General Data Protection Regulation (GDPR), встановлюють строгі вимоги до обробки персональних даних, включаючи право на приватність за замовчуванням та право на забуття. Однак, у сфері електронного врядування, де обробка даних є масштабною та комплексною, існує ризик невідповідного зберігання та використання даних, що може призвести до порушень приватності. Оцінка впливу на захист даних (DPIA) є обов'язковою для систем, які потенційно можуть викликати високий ризик для прав і свобод осіб. Така оцінка допомагає ідентифікувати та мінімізувати ризики при проектуванні та впровадженні нових технологій. Проте, викликом є забезпечення компетентності та о’єктивності DPIA, особливо у контексті швидкого технологічного розвитку [2].

Захист цифрового середовища від несанкціонованого доступу та зловживань є критично важливим. Ризики кібербезпеки включають вразливість до атак, які можуть призвести до втрати або спотворення критичних даних. Належні контрольні механізми, такі як удосконалення платформ, архітектура мережі, та моніторинг безпеки, є обов'язковими для забезпечення конфіденційності та цілісності систем. Дотримання законодавчих та регуляторних вимог є іншим важливим аспектом. Електронне врядування має відповідати різноманітним технологічним, секторальним законам та регуляціям. Невідповідність може призвести до юридичних наслідків та втрати довіри громадськості [2].

Ризик зриву операцій або недоступності послуг через високу залежність від технологій вимагає розробки та імплементації ефективних планів бізнес-

континуїтету та кіберстійкості. Кризове управління та відновлення після інцидентів є критичними для забезпечення безперебійної роботи електронного врядування [3].

У контексті електронного врядування, значна кількість ризиків уже визначена і врегульована через такі законодавчі акти, як General Data Protection Regulation (GDPR), які встановлюють високі стандарти захисту даних і кібербезпеки. Однак, глобальна неоднорідність у дотриманні та впровадженні цих правил є очевидною. Високий рівень дотримання стандартів кібербезпеки та захисту даних, як правило, спостерігається в країнах з високим рівнем добробуту, де існують ресурси та технологічна інфраструктура для ефективного впровадження цих правил.

Проте, багато країн, особливо ті, що розвиваються, все ще зіштовхуються з викликами, пов'язаними з недостатньою технологічною інфраструктурою, обмеженим доступом до ресурсів та відсутністю строгих регуляторних рамок, що стосуються захисту даних та кібербезпеки. Це створює розрив у глобальних стандартах безпеки і приватності, підвищуючи ризики не тільки для внутрішніх користувачів, але і для міжнародної взаємодії.

Для забезпечення більшої універсальності та безпеки, важливо розширити впровадження регуляцій у всіх країнах незалежно від рівня їхнього добробуту. Також потрібно просувати глобальне співробітництво для створення спільних стандартів і практик в області кібербезпеки та захисту даних.

Крім того, нові технологічні тренди, такі як штучний інтелект та блокчейн, представляють нові виклики і можливості для регуляції. Розвиток регуляторних рамок, які враховують ці нові технології, є критично важливим для забезпечення безпеки, прозорості та довіри в контексті електронного врядування. Потреба у стандартизації та юридичній ясності використання цих технологій стає все більш актуальною, оскільки вони починають інтегруватися в основні аспекти суспільного та економічного життя. Такий підхід дозволить забезпечити не

тільки захист даних і приватності, але й сприятиме інноваційному розвитку та технологічній інтеграції на глобальному рівні.

Висновки. Електронне врядування відкриває нові можливості для підвищення ефективності, доступності та прозорості управлінських процесів, водночас вносячи значні виклики, пов'язані з кібербезпекою, захистом персональних даних та регуляторним дотриманням. Регуляції, такі як GDPR, задають високі стандарти для обробки даних, проте їхня ефективність обмежена відсутністю глобальної універсальності та однаковим дотриманням в усіх країнах.

Успіх цифрового врядування залежить від спроможності країн розвивати технологічну інфраструктуру та законодавчі бази, що зможуть захистити громадян та підтримати довіру до уряду. Це включає розширення впровадження міжнародно визнаних регуляцій та практик в області кібербезпеки та захисту даних, а також адаптацію до нових технологій, таких як штучний інтелект і блокчейн.

Список використаних джерел

1. Scholl H. J. Digital Government. Digital Government: Research and Practice. 2020. Vol. 1, №. 1. P. 1–12. URL: https://doi.org/10.1145/3352682 (date of access: 23.04.2024).

2. The GDPR and Cybersecurity – CrowdStrike. crowdstrike.com. URL: https://www.crowdstrike.com/cybersecurity-101/data-security/general-data-protection-regulation-gdpr/ (date of access: 23.04.2024)

3. Addressing the Digital Divide | UN-Habitat. UN-Habitat – A Better Urban Future. UN-Habitat. URL: https://unhabitat.org/programme/legacy/people-centered-smart-cities/addressing-the-digital-divide (date of access: 23.04.2024).

Іванна Бурдун

студентка другого курсу освітньої програми

«Суспільне і приватне врядування», НаУКМА

УКРАЇНСЬКО-ЕСТОНСЬКИЙ ОБМІН ТЕХНОЛОГІЯМИ ЦИФРОВОГО ВРЯДУВАННЯ