Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2025. № 11.

DOI: http://doi.org/10.32702/2307-2156.2025.11.19

УДК 351.72:004.056.5

А. В. Кузьменко,

аспірант, ДЗВО «Університет менеджменту освіти» НАПН України

ORCID ID: https://orcid.org/0009-0000-4159-355X

ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІВ ПУБЛІЧНОГО УПРАВЛІННЯ

A. Kuzmenko,

Postgraduate Student, State Educational Institution "University of Educational Management" of the National Academy of Sciences of Ukraine

FEATURES OF INFORMATION SECURITY OF PUBLIC ADMINISTRATION BODIES

Стаття присвячена дослідженню особливостей інформаційної безпеки (ІБ) органів публічного управління (ОПУ) в умовах цифрової трансформації (Digital Transformation). Перехід до цифрового формату діяльності перетворює дані на ключовий актив, а кібератаки на державні ресурси стають критичною загрозою національній безпеці та інтересам невладних суб'єктів. Метою роботи є визначення ключових особливостей та механізмів забезпечення ІБ

ОПУ на основі порівняльно-правового аналізу досвіду України, США та Франції.

Аналіз актуальних публікацій (В. Д. Цимбалюк, О. В. Корченко, О. С. Карпенко та ін.) підтверджує глибоку розробленість нормативно-правових та загальнотехнічних аспектів ІБ ОПУ. Водночас, дослідники констатують розрив між декларативними нормами високого рівня (стратегії, доктрини) та ефективністю їх практичного впровадження на місцях. Особливо недостатньо вивченими залишаються практичні аспекти формування стійкої системи ІБ в умовах обмеженого фінансування, військової агресії та впливу людського фактора як найслабшої ланки захисту.

Дослідження виявляє тенденцію до централізації регулювання інформаційної сфери, де визначення політики ІБ належить до компетенції глави держави у всіх досліджуваних країнах.

1. Стандартизація та регулювання: У США (Ніціональний інститут стандартів і технологій, NIST) та Франції існують єдині узагальнюючі довідники та фреймворки (наприклад, Спільний посібник з безпеки у Франції, Фреймворк NIST у США), "що спрощує послідовне впровадження елементів ІБ. В Україні такі узагальнюючі документи відсутні, що ускладнює формування єдиного плану. Обґрунтовується доцільність закріплення за Службою безпеки України повноважень щодо узагальнення вимог різних стандартів та публікації єдиних довідників.

2. Організаційна структура: У досліджуваних країнах формуються спеціалізовані штатні одиниці (Senior Agency Official for Security у США; un fonctionnaire de sécurité des systèmes d'information у Франції та відповідні підрозділи в Україні) для безперервного забезпечення ІБ. Досвід США, заснований на утворенні Ради головних управителів інформаційної безпеки, свідчить про важливість кооперації та обміну найкращими практиками між ОПУ, що є слабким місцем в українському регулюванні.

3. Обмін інформацією про інциденти: Виявлено централізований механізм обміну інформацією про інциденти: у Франції – через Національне агентство безпеки інформаційних систем, у США – через Федеральний центр інцидентів інформаційної безпеки. В Україні, Франції та США спостерігається тенденція до посилення законодавства у цій сфері.

4. Перспективи: Аналізується вплив нових технологій (штучний інтелект, квантові комунікації) на ІБ, що потенційно може призвести до збільшення автономії ОПУ щодо своїх інформаційних систем, але вимагає значних інвестицій та фахівців.

5. Правове регулювання е-Уряду: Порівняльний аналіз регулювання електронного уряду показав, що країни з традицією розвиненого адміністративного права (Франція, Швеція) не приймають окремих законів про електронний уряд, інтегруючи його норми у загальне адміністративне законодавство. Країни, що акцентують увагу на підвищенні ефективності діяльності (США, Італія, Німеччина), "приймають спеціальне законодавство. З огляду на пошук Україною нової моделі регулювання, прийняття окремого закону про е-Уряд в Україні визнається недоцільним, оскільки краще сприяє розвитку інтеграція цих положень у рамках більших правових інститутів.

Дослідження підтверджує динаміку та централізацію регулювання ІБ ОПУ. Для України доцільним є запозичення досвіду щодо створення єдиних довідників стандартів ІБ та дорадчих органів для обміну практиками. Подальший розвиток е-Уряду, що характеризується платформним підходом, вимагає посиленого регулювання електронного обміну даними та державної електронної ідентифікації.

The article is devoted to the study of the features of information security (IS) of public administration bodies (PAB) in the context of digital transformation. The transition to a digital format of activity turns data into a key asset, and cyberattacks on state resources become a critical threat to national security and the interests of non-governmental entities. The aim of the work is to identify the key features and mechanisms for ensuring IS of PAB based on a comparative legal analysis of the experience of Ukraine, the USA and France.

The analysis of current publications (V. D. Tsymbalyuk, O. V. Korchenko, O. S. Karpenko and others) confirms the deep development of the regulatory, legal and general technical aspects of IS of PAB. At the same time, researchers note the gap between high-level declarative norms (strategies, doctrines) and the effectiveness of their practical implementation on the ground. The practical aspects of forming a sustainable IS system in the context of limited funding, military aggression and the influence of the human factor as the weakest link of protection remain particularly poorly studied.

The study reveals a tendency towards centralization of information sphere regulation, where the definition of IS policy is the competence of the head of state in all the countries studied.

1. Standardization and regulation: In the USA (National Institute of Standards and Technology, NIST) and France, there are single generalizing guides and frameworks (for example, the Common Security Guide in France, the NIST Framework in the USA), "which simplifies the consistent implementation of IS elements. In Ukraine, such generalizing documents are absent, which complicates the formation of a single plan. The expediency of assigning the Security Service of Ukraine the authority to generalize the requirements of various standards and publish single guides is substantiated.

2. Organizational structure: In the countries studied, specialized staff units are being formed (Senior Agency Official for Security in the USA; un fonctionnaire de

sécurité des systèmes d'information in France and corresponding units in Ukraine) for continuous IS support. The experience of the USA, based on the formation of the Council of Chief Information Security Officers, indicates the importance of cooperation and exchange of best practices between the OPUs, which is a weak point in Ukrainian regulation.

3. Information exchange on incidents: A centralized mechanism for exchanging information on incidents has been identified: in France - through the National Agency for Information Systems Security, in the USA - through the Federal Information Security Incident Center. In Ukraine, France and the USA, there is a tendency to strengthen legislation in this area.

4. Prospects: The impact of new technologies (artificial intelligence, quantum communications) on IS is analyzed, which can potentially lead to increased autonomy of the OPUs regarding their information systems, but requires significant investments and specialists.

5. Legal regulation of e-Government: A comparative analysis of e-government regulation has shown that countries with a tradition of developed administrative law (France, Sweden) do not adopt separate laws on e-government, integrating its norms into general administrative legislation. Countries that focus on increasing the efficiency of their activities (USA, Italy, Germany) adopt special legislation. Given Ukraine's search for a new regulatory model, the adoption of a separate law on e-Government in Ukraine is considered inappropriate, since the integration of these provisions within larger legal institutions is better conducive to development.

The study confirms the dynamics and centralization of the regulation of IS of the OPU. It is advisable for Ukraine to borrow experience in creating unified directories of IS standards and advisory bodies for the exchange of practices. Further development of e-Government, characterized by a platform approach, requires enhanced regulation of electronic data exchange and state electronic identification.

Ключові слова: *Інформаційна безпека, публічне управління, кібербезпека, цифрова трансформація, електронний уряд, стандартизація, кібератаки, кіберзахист, державні реєстри, централізація регулювання, США, Франція, Україна, електронні послуги, людський фактор, стандарти NIST, обмін інформацією про інциденти, критична інфраструктура, квантові комунікації, нормативно-правове регулювання.*

Keywords: *Information security, public administration, cybersecurity, digital transformation, e-government, standardization, cyberattacks, cyberdefense, state registries, centralization of regulation, USA, France, Ukraine, electronic services, human factor, NIST standards, exchange of information about incidents, critical infrastructure, quantum communications, regulatory regulation.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями.

Перехід до цифрового формату діяльності органів публічного управління формує нове середовище, основним активом у якому виступають дані, які у розпорядженні суб'єктів інформаційних відносин. Кібератака на інформаційні ресурси державного органу може завдати шкоди як державі, так і окремим невладним суб'єктам (наприклад, у разі заміни відомостей у державному реєстрі). Інформаційна безпека - один із напрямків посиленої централізації регулювання інформаційної сфери в цілому. Визначення політики у сфері інформаційної безпеки у досліджуваних країнах (США, Франція, Україна) належить до компетенції голови держави.

Для сприяння голові держави у реалізації його повноважень щодо забезпечення інформаційної безпеки у досліджуваних країнах формуються окремі державні органи чи посади. Такі органи можуть формуватися і за уряду (Франція) з метою сприяння главі держави у реалізації його повноважень щодо визначення політики у сфері національної безпеки.

Якщо система інформаційної безпеки в цілому охоплює як зовнішній вплив уповноважених органів виконавчої влади на інформаційну сферу, так і внутрішню взаємодію між ними, обов'язки органів виконавчої влади у сфері інформаційної безпеки належать переважно до вузької сфери забезпечення кібербезпеки.

Аналіз останніх досліджень і публікацій.

Актуальні публікації (наприклад, праці В. Д. Цимбалюка, М. А. Дем'янця, О. А. Баранова) активно досліджують вплив нового законодавства (зокрема, щодо кіберзахисту та захисту персональних даних) на функціонування ОПУ. Більшість робіт констатують розрив між декларативними нормами високого рівня (стратегії, доктрини) та ефективністю їх практичного впровадження на регіональному та локальному рівнях управління.

Науковці (зокрема, О. В. Корченко, Є. А. Фролова) приділяють значну увагу технологічній складовій інформаційної безпеки органів публічного управління (ІБ ОПУ), “особливо в контексті цифрової трансформації (Digital Transformation) та впровадження електронних послуг. Обговорення ефективності вітчизняних криптографічних стандартів та необхідності їх інтеграції в сучасні системи захисту.

Сучасні дослідження (наприклад, роботи О. С. Карпенко, Ю. С. Жданенка) підкреслюють, що "людський фактор" залишається найслабшою ланкою в системі ІБ.

Таким чином, аналіз останніх публікацій свідчить про глибоку розробленість нормативно-правових та загальнотехнічних аспектів ІБ ОПУ. Однак, недостатньо вивченими залишаються практичні особливості формування ефективної та стійкої системи ІБ в умовах обмеженого фінансування, військової агресії та швидкого впровадження електронних послуг. Саме ці прогалини (недостатня увага до комплексної системи навчання персоналу та захисту

периферійних вузлів) визначають актуальність вашого подальшого дослідження.

Формулювання цілей статті. Метою статті є визначення особливостей інформаційної безпеки органів публічного управління.

Виклад основного матеріалу дослідження.

На відміну від координації та контролю у сфері інформаційної безпеки, стандартизація здійснюється професійною спільнотою, а органи виконавчої влади затверджують необхідність застосування того чи іншого технічного стандарту. У досліджуваних країнах (Франція, США) спостерігається тенденція до прийняття єдиних узагальнюючих різні практики довідників у сфері інформаційної безпеки.

У Франції застосовні стандарти затверджено Спільним посібником з безпеки [1], прийнятим на підставі статті 9 Ордонансу Президента Французької Республіки № 2005-1516 від 08.12.2005 р. [2].

У США розробкою стандартів інформаційної безпеки агентств займається Національний інститут стандартів і технологій, утворений у складі Міністерства торгівлі [3]. Зокрема, Інститутом розроблено Фреймворк удосконалення безпеки критичної інформаційної інфраструктури [4], який можна використовувати для побудови системи інформаційної безпеки.

В Україні такі узагальнюючі документи відсутні. Зведений перелік застосовних до інформаційної сфери стандартів розміщено на сайті Національної бібліотеки імені В.І. Вернадського [5].

Система інформаційної безпеки вибудовується динамічно та потребує реагування на різні виклики нових технологій, удосконалення кібератак. Розрізнене стандартизоване регулювання не дозволяє побудувати єдиний послідовний план впровадження окремих елементів системи інформаційної безпеки та ускладнює особливості їх застосування. У зв'язку з цим доцільним закріпити за Службою безпеки України повноваження щодо узагальнення вимог

різних стандартів інформаційної безпеки як загалом, так окремих галузей, і опублікування єдиних довідників стандартів у сфері інформаційної безпеки органів виконавчої влади. Саме практика визначає формування технологічних і стандартів. У зв'язку з цим важливим напрямом регулювання у сфері інформаційної безпеки органів публічного управління є започаткування дорадчих органів, що об'єднують фахівців різних органів публічного управління у сфері забезпечення інформаційної безпеки.

Необхідність формування системи інформаційної безпеки органів публічного управління передбачає також формування окремих структурних підрозділів та штатних одиниць, які безперервно зі стадії проектування забезпечують дотримання умов інформаційної безпеки та оцінку можливих ризиків та загроз. Грамотний облік даних у розпорядженні органів публічного управління дозволяє більш точно визначати можливі ризики та наслідки їх витоку та аналізувати ступінь суспільної небезпеки кібератаки.

В Україні утворення окремих структурних підрозділів, відповідальних за інформаційну безпеку, в органах виконавчої влади здійснюється на підставі Наказу Служби безпеки України Міністерства внутрішніх справ України «Про затвердження Порядку електронної інформаційної взаємодії Служби безпеки України, Міністерства внутрішніх справ України та центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України» від 13.10.2022 р. № 360/657 [6].

У США в кожному агентстві відповідно до Закону про модернізацію федеральної інформаційної безпеки від 2014 року затверджено посаду старшого керуючого з безпеки агентства у підпорядкуванні Головного керуючого у сфері інформації [7]. До повноважень старшого управителя з безпеки агентства належить як розробка внутрішніх документів з інформаційної безпеки, і навчання інших службовців агентства правилам інформаційної безпеки.

У Франції застосовується інший підхід, заснований на розподілі технічних фахівців та управлінців у сфері інформаційної безпеки у структурі органу виконавчої влади. Відповідно до Декрету Прем'єр-міністра № 2022-513 від 08.04.2022 р., кожне міністерство зобов'язане призначити державного службовця, відповідального за безпеку інформаційних систем (un fonctionnaire de sécurité des systèmes d'information) [8]. Такий службовець відповідає за вироблення спільної політики інформаційної безпеки міністерства та підвідомчих йому організацій та контроль її виконання [9]. Додатково кожен міністр зобов'язаний призначити одну або кілька кваліфікованих осіб, які безпосередньо забезпечують безпеку інформаційних систем міністерства. Кваліфіковані особи координуються державним службовцем, відповідальним за безпеку інформаційних систем.

Українське законодавство приділяє менше уваги формам кооперації та обміну найкращими практиками між різними посадовими особами в органах виконавчої влади. У цьому прикметний досвід США, заснований на освіті таких порад. Зокрема, для координації діяльності старших управителів з безпеки агентств та обміну практиками при Адміністративно-бюджетному управлінні утворено Раду головних управителів інформаційної безпеки, якою керує Федеральний головний управитель інформаційною безпекою [10]. Надається позитивна можливість запозичення різних дорадчих органів між посадовими особами органів виконавчої влади, відповідальними за інформаційну безпеку, що дозволить узагальнювати проблеми та обмінюватися кращими практиками.

Розвиток штатних одиниць, спеціалізованих на забезпеченні інформаційної безпеки, у структурі органу публічного управління, дозволяє організувати систему обміну інформацією та повідомленнями про інциденти або уразливості інформаційних систем різних органів виконавчої влади [11]. Як правило, такий обмін здійснюється централізовано. У Франції установа в обов'язковому порядку в міністерствах посада державного службовця,

відповідального за безпеку інформаційних систем, передбачає його обов'язок повідомляти Національне агентство безпеки інформаційних систем про будь-які інциденти, пов'язані з інформаційними системами органу виконавчої влади [12].

У США у підпорядкуванні Міністерства внутрішньої безпеки утворено Федеральний центр інцидентів інформаційної безпеки (Federal information security incident center), "з яким усі агентства зобов'язані ділитися інформацією про інциденти відповідно до секції 3556(b) Закону про модернізацію федеральної інформаційної безпеки від 2014 р. [13]. Повідомляти про інциденти можуть також штати та їх органи місцевого самоврядування [14]. Система взаємодії Міністерства внутрішньої безпеки США з органами штатів була закріплена в 2021 році в Законі про кібербезпеку штатів та місцевого самоврядування [15]. Додатково у 2022 році було введено обов'язок агентств повідомляти приватні організації про витікання, які можуть суттєво вплинути на дотримання конфіденційності даних таких організацій [16].

Питання необхідності інформування державою громадян, і організацій про витоках даних, що відбулися, мають значні наслідки їхньої діяльності, залишається дискусійним. Соціологічні дослідження показують, що громадяни, які зазнали витоку даних, що спричинило значну шкоду, схильні вважати, що держава повинна забезпечити систему належного повідомлення громадян про витоки, що спричинили значну шкоду, у той час як громадяни, які зазнали меншої шкоди через витоку, займають більше. Однак розкриття інформації про витік може викликати додаткові суспільні хвилювання, що тільки посилить несприятливі наслідки кібератаки.

Вибудовування єдиних механізмів обміну інформацією про інциденти та розвиток структурних підрозділів, які відповідають за забезпечення інформаційної безпеки, що спостерігаються в досліджуваних країнах (Україна, Франція, США), "свідчать про тенденцію до централізації регулювання інформаційних систем органів публічного управління загалом. Якщо Франція

схильна вносити менше змін у підхід до регулювання інформаційної безпеки органів виконавчої влади, Україна та США активно змінюють та посилюють законодавство у цій сфері. Найбільша динаміка регулювання відзначається у США.

Зазначена тенденція може змінитися із впровадженням нових технологій та засобів забезпечення інформаційної безпеки. Зокрема, потенціал має використання технологій штучного інтелекту для запобігання інцидентам інформаційної безпеки [17]. Крім того, квантові технології, що набирають популярності, виключають будь-яку можливість несанкціонованого доступу до комп'ютерної інформації [18]. Як наслідок, у разі застосування квантових технологій для передачі та обробки даних органами виконавчої влади може збільшитися частка автономії органу виконавчої влади щодо інформаційних систем, що знаходяться в його розпорядженні. Проте використання квантових комунікацій вимагає на початкових етапах як фінансування, і виховання фахівців, здатних працювати з квантовими комунікаціями [19].

Розвиток правового регулювання квантових комунікацій в цілому потребує додаткового уточнення у чинному законодавстві. Лідером у розвитку квантових технологій є Китай, який прийняв у 2020 р. у тому числі і Закон про шифрування, що врегулював питання розвитку квантової криптографії [20]. В Україні питання регулювання квантових комунікацій нині носять дискусійний характер, проте їх подальший розвиток є неминучим.

Цифровізація діяльності всіх органів публічного управління характеризуються терміном «електронна держава». Для характеристики особливостей використання інформаційних технологій у діяльності органів публічного управління у вузькому значенні, а також у ширшому сенсі – для характеристики зміни публічного управління у зв'язку з цифровізацією діяльності органів публічного управління, – використовується термін «електронний уряд» [21].

Подальший розвиток цілей електронного уряду привів поряд із цим терміном до виникнення таких суміжних понять як «відкритий уряд» (open government, government 2.0), “«цифровий уряд» (smart government, digital government). У сучасній літературі також застосовуються терміни «екосистема» [22], «платформа» [23]. Проте ці терміни лише конкретизують окремі напрями розвитку електронного уряду в цілому. Зазначений розвиток невипадковий - нові терміни відбивають поступальний рух від інформаційного забезпечення діяльності органів публічного управління до розвитку інтерактивних форм взаємодії органів публічного управління з громадянами та побудові взаємного діалогу.

Лідерами за рівнем розвитку електронного уряду за даними Організації Об'єднаних Націй [24] є країни північної Європи (Данія, Ісландія, Фінляндія, Швеція), “а також США. Китай посідає 43 місце у загальному рейтингу країн. Україна у 2024 році посіла 30 місце порівняно з 46 місцем у 2023 році [25]. Найвищий розвиток електронний уряд отримав у європейському регіоні, де 81% країн має найвищий (very high) індекс розвитку електронного уряду. Азіатські та американські країни також зберігають високий рівень розвитку електронного уряду. Однак в азіатських країнах більш висока частка держав з найвищим («very high») індексом розвитку електронного уряду (32% проти 24% в американських країнах), “тоді як в американському регіоні більше країн із високим («high») індексом розвитку електронного уряду (69% проти 47% в азіатських країнах). Найменш розвинений електронний уряд у країнах Африки та Океанії [24].

Розвиток електронного уряду призводить до змін у законодавстві, яке регулює діяльність органів виконавчої влади. Електронний уряд почав формуватися на певному етапі розвитку конституційної держави, коли вона вже сформувалася і як правова, і як соціальна. З огляду на це електронний уряд є новий етап розвитку конституційної держави загалом, визначаючи особливості

реалізації права і свободи людини і громадянина з урахуванням сформованих конституційно-правових цінностей.

В даний час еволюція електронної держави не вплинула на конституційні зміни, проте визначається інформаційними правами людини і громадянина, що виникають у конституціях. Наприклад, у частині 2 статті 5А Конституції Греції закріплено обов'язок держави сприяти доступу до інформації та електронного обміну для реалізації прав громадян на участь в інформаційному суспільстві [26]. У Конституції України закріплено свободу інформації. Конституції інших країн (Фінляндія, Норвегія, Польща, Естонія) також містять положення, присвячені праву на інформацію та праву на доступ до інформації [27]. На законодавчому рівні регулювання електронного уряду розвивається активніше. Порівняльно-правове дослідження показує, що в одних країнах приймаються закони про електронний уряд (США, Італія, Німеччина, Австрія), “тоді як в інших країнах електронний уряд регулюється в рамках більш загального законодавства про діяльність органів публічного управління (Франція, Швеція, Україна). У Канаді регулювання електронного уряду складає підзаконному рівні.

У випадку, коли норми про електронний уряд включаються до більш загальних актів, використання інформаційних технологій у діяльності органів публічного управління розглядається як один із напрямків розвитку їх діяльності. Норми, що приймаються, лише уточнюють особливості діяльності органів виконавчої влади з урахуванням розвитку електронного уряду.

В Україні прийнято кілька законів, присвячених окремим аспектам публічного управління у цифровій сфері. Вони містять положення про загальний правовий режим інформації [28], загальні особливості надання адміністративних послуг, зокрема у цифровому середовищі, положення про електронної ідентифікації громадян під час надання адміністративних послуг [29]. Встановлюються додаткові вимоги, створені задля забезпечення

інформаційної безпеки найбільш значимих елементів інформаційної інфраструктури держави [30]. Однак єдиного акта, який регулює електронний уряд, не прийнято. В цілому український законодавець шукає нову модель регулювання адміністративних відносин та норми про електронний уряд також включаються до складу більш загальних положень. Про це свідчать і нові реформи у сфері контрольно-наглядової діяльності, розвиток адміністративної юстиції.

Для Франції також характерним є вдосконалення адміністративного законодавства в цілому. У Франції окремі положення, що регулюють інформаційну сферу, було викладено у Законі про цифрову республіку від 7 жовтня 2016 р. [31]. Проте загальне регулювання діяльності органів виконавчої влади визначено Кодексом про відносини між адміністрацією та суспільством [32]. Французький підхід відповідає загальній спрямованості державної політики не так у бік розвитку електронного уряду, скільки до вдосконалення системи державного управління в цілому.

Французький підхід відповідає загальній спрямованості державної політики не так у бік розвитку електронного уряду, скільки до вдосконалення системи публічного управління в цілому. Шведський законодавець, на відміну від Франції та України, повільніше реагує на необхідність регулювання електронного уряду, доповнюючи законодавство з урахуванням правової традиції регулювання та організації системи підпорядкування органів виконавчої влади. У Швеції 2010 р. був прийнятий Білль про громадську адміністрацію, частина якого присвячена окремим особливостям електронного уряду [33]. Якщо в частині доступу до електронних документів органів виконавчої влади Швеція доповнила законодавство у 1970-х роках, інші напрями діяльності органів виконавчої влади у сфері електронного уряду здійснюються без внесення додаткових змін до законодавства та розглядаються в контексті загального регулювання діяльності органів виконавчої влади [34].

У деяких країнах, навпаки, ухвалюються окремі закони про електронний уряд. Більшість країн, які ухвалювали закони про електронний уряд, додатково ухвалювали й інші закони, що регулюють окремі аспекти діяльності органів виконавчої влади в електронній формі. Закон про електронну державу 2002 р. [35] у США встановлює обов'язки агенцій організувати офіційні сайти в мережі Інтернет, визначає правовий режим окремих категорій інформації у розпорядженні агенцій, питання інформаційної безпеки. Проте діяльність електронного уряду регулюють інші закони - наприклад, у частині організації зберігання електронних федеральних документів [36], забезпечення доступу до інформації про діяльність федеральних агентств [37]. Закон про електронну державу встановив умови для запровадження інформаційних технологій у діяльність агентств США. Однак подальший розвиток електронного уряду отримав новий напрямок, пов'язаний із посиленням взаємодії органів виконавчої влади з невладними суб'єктами в інформаційній сфері. Таким чином, закон про електронну державу заклав основи переходу органів виконавчої влади до електронного уряду.

В Італії, на відміну від США, що активно розвиває кодифікацію, в 2005 році був прийнятий Кодекс електронного уряду [38], який регулює взаємодію громадян у відносинах з державою в електронній сфері, організацію електронного документообігу, електронні підписи та електронний обмін даними. Кодекс регулює відносини між громадськими органами в інформаційній сфері та спрямований на підвищення ефективності державного управління. Деякі положення регулюються окремо. Наприклад, обробка персональних даних у громадському секторі регулюються Кодексом про захист персональних даних [39].

Позитивно можна оцінити Федеральний закон Німеччини про електронний уряд 2013 (Gesetz zur Förderung der elektronischen Verwaltung) [40]. Закон передбачає загальні положення про електронний документообіг,

стандартизацію в інформаційній сфері, правовий режим просторових та персональних даних, використання офіційних сайтів у мережі Інтернет та офіційної електронної пошти (De-Mail). Незважаючи на наявність додаткових законів у сфері електронного уряду (наприклад, щодо удосконалення державних послуг онлайн, цифрових підписів, подальшого використання інформації публічного сектору), “зазначений закон у стислій та лаконічній формі зачіпає всі основні аспекти правового регулювання електронного уряду.

Закон про електронний уряд 2004 р. [41] ухвалено також в Австрії, проте він регулює переважно електронні способи посвідчення особи та формування системи електронної ідентифікації. Загалом для регулювання електронного уряду в Австрії діє багато інших законів.

Варто зазначити також прийняття окремих законів про електронний уряд у низці інших країн: Закон про електронний уряд Танзанії 2019 р., який заснував окреме відомство у сфері електронного уряду [42], Закони про цифровий уряд держави Беліз [43] та Незалежної держави Папуа Нова Гвінея від 2022 року [44]. У Канаді, на відміну зазначених раніше країн, регулювання електронного уряду складає підзаконному рівні і орієнтоване насамперед в розвитку цифрових сервісів. Для регулювання електронного уряду приймаються акти органів виконавчої влади: політики, що встановлюють спільні цілі розвитку електронного уряду, та директиви, що конкретизують необхідні заходи для досягнення встановлених політиками цілей. З 1 квітня 2020 р. у Канаді набули чинності Політика про послуги та цифрові технології [45], яка встановлює загальні принципи розвитку інформаційних систем органів виконавчої влади центрального апарату, та Директива про послуги та цифрові технології [46]. Політика, затверджена Казначейством Канади, є обов'язковим для виконання органами центральної адміністрації нормативним актом, а директива, прийнята Головою Казначейства Канади на виконання вимог політики, конкретизує вимоги до органів виконавчої влади з розвитку інформаційних систем.

Основною метою ухваленої політики є удосконалення державної діяльності за допомогою цифрової трансформації, тоді як інші особливості правового регулювання електронного уряду не охоплюються зазначеними актами.

Порівняння досвіду законодавчого регулювання електронного уряду показує, що країни з традицією адміністративного права, що склалася (Франція, Швеція), “не приймають окремі закони про електронний уряд і розглядають електронний уряд у контексті загальної характеристики діяльності органів виконавчої влади.

Висновки

В Україні також розвивається регулювання електронного уряду у складі загальних норм про діяльність органів публічного управління. Однак українське законодавство відображає пошук нового підходу до регулювання діяльності органів публічного управління в цілому: оптимізації адміністративних послуг, організації надання доступу до інформації про діяльність державних органів.

Країни, котрим характерно більшою мірою вирішення питання підвищення ефективності діяльності органів виконавчої, ніж розвитку окремих адміністративно-правових інститутів, приймають спеціальне законодавство, присвячене електронному уряду. Насамперед до таких країн належать США та Канада. Дотримуються зазначеного підходу також Італія та Німеччина.

У зв'язку з цим прийняття окремого закону, присвяченого електронному уряду в Україні, є недоцільним, оскільки не дозволяє розвивати окремі положення про електронний уряд у рамках більших правових інститутів, що регулюють діяльність органів публічного управління. Сучасний етап розвитку електронного уряду характеризується посиленням ролі приватних та державних цифрових платформ у публічному управлінні. У рамках розвитку платформного підходу істотне значення набувають регулювання електронного обміну даними органами публічного управління та державної електронної ідентифікації.

Література

1. Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques. URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000029122964 (Дата звернення: 05.11.2025).

2. Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000636232/ (Дата звернення: 05.11.2025).

3. Sec. 20, National Institute of Standards and Technology Act. As Amended Through P.L. 117-263, Enacted December 23, 2022. URL: https://www.govinfo.gov/content/pkg/COMPS-5388/pdf/COMPS- 5388.pdf (Дата звернення: 05.11.2025).

4. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1 April 16, 2018. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (Дата звернення: 05.11.2025).

5. Національна бібліотека імені В.І. Вернадського (сайт) 25.10.2014. Перелік Національних стандартів України для створення, впровадження та супроводження автоматизованих і інформаційних систем. URL: http://nbuv.gov.ua/node/1469 (Дата звернення: 05.11.2025).

6. Наказ Служби безпеки України Міністерства внутрішніх справ України «Про затвердження Порядку електронної інформаційної взаємодії Служби безпеки України, Міністерства внутрішніх справ України та центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ

України» від 13.10.2022 р. № 360/657. URL: https://zakon.rada.gov.ua/laws/show/z1327-22#Text (Дата звернення: 05.11.2025).

7. Federal Information Security Modernization Act of 2014. URL: https://www.congress.gov/bill/113th-congress/senate-bill/2521/text (Дата звернення: 05.11.2025).

8. Décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics. URL: https://www.legifrance.gouv.fr/loda/id/LEGIARTI000045539964/2022-10-01/ (Дата звернення: 05.11.2025).

9. Arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics. URL: https://www.legifrance.gouv.fr/jorf/id/JORFARTI000046503138#JORFARTI000046503138 (Дата звернення: 05.11.2025).

10. CIO Council - CISO Committee. URL: https://www.tio.gov/about/members-and-leadership/tiso- council/ (Дата звернення: 05.11.2025).

11. Brilingaitè A., Bukauskas L., Juozapavicius A., Kutka E. Overcoming information-sharing challenges in cyber defence exercises // Journal of Cybersecurity. Volume 8. Issue 1. 2022. URL: https://academic.oup.com/cybersecurity/article/8/1/tyac001/6516499 (Дата звернення: 05.11.2025).

12. Décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics. URL: https://www.legifrance.gouv.fr/loda/id/LEGIARTI000045539964/2022-10-01/ (Дата звернення: 05.11.2025).

13. Federal Information Security Modernization Act of 2014. URL: https://www.congress.gov/bill/113th-congress/senate-bill/2521/text (Дата звернення: 05.11.2025).

14. Federal Incident Notification Guidelines. April 1, 2017. URL: https://www.cisa.gov/federal- incident-notification-guidelines (Дата звернення: 05.11.2025).

15. State and Local Government Cybersecurity Act of 2021. URL: https://www.congress.gov/bill/117th- congress/senate-bill/2520/text (Дата звернення: 05.11.2025).

16. Sec. 107, (b), "Strengthening American Cybersecurity Act of 2022. URL: https://www.congress.gov/bill/117th-congress/senate-bill/3600/text#toc-id87c2d95a-b307-45ec-81dd- 09e23e4addc4 (Дата звернення: 05.11.2025).

17. Snider K.L.G., Shandler R., Zandani S., Canetti D. Cyberattacks, cyber threats, and attitudes toward cybersecurity policies // Journal of Cybersecurity. Volume 7. Issue 1. 2021. URL: https://academic.oup.com/cybersecurity/article/7/1/tyab019/6382745 (Дата звернення: 05.11.2025).

18. Dapel M.E., Asante M., Uba C.D., Agyeman M.O. Artificial Intelligence Techniques in Cybersecurity Management. In: Jahankhani, H. (eds) Cybersecurity in the Age of Smart Societies. Advanced Sciences and Technologies for Security Applications. Springer, Cham. 2023.

19. Albataineh, H., Nijim, M. Enhancing the Cybersecurity Education Curricula Through Quantum Computation. In: Daimi, K., Arabnia, H.R., Deligiannidis, L., Hwang, MS., Tinetti, F.G. (eds) Advances in Security, Networks, and Internet of Things. Transactions on Computational Science and Computational Intelligence. Springer, Cham. 2021.

20. Кореспондент.net. (26.10.2019) Перший в історії закон про шифрування даних прийняли в Китаї. URL:

https://ua.korrespondent.net/world/4153691-pershyi-v-istorii-zakon-pro-shyfruvannia-danykh-pryinialy-v-kytai (Дата звернення: 05.11.2025).

21. Баранов О. Електронний уряд в Україні? Буде! Коли?. ZN.UA. 2020. URL: https://dt.ua/SOCIETY/elektronniy_uryad_v_ukrayini_bude_koli.html (Дата звернення: 05.11.2025).

22. Harrison T.M., Pardo T.A., Cook M. Creating open government ecosystems: a research and development agenda. Future Internet. 2012. № 4(4). P. 900-928

23. O'Reilly T. Government as a Platform // innovations. 2010. Vol. 6. №. 1. P. 13-40.

24. UN E-Government Survey 2022. P. 191. URL: https://desapublications.un.org/sites/default/files/publications/2022-09/Chapter%205.pdf (Дата звернення: 05.11.2025).

25. AIN (сайт) 20.09.2024. ООН опублікували рейтинг країн за рівнем розвитку електронного урядування — Україна на п'ятому місці за індексом Online Service. URL: https://ain.ua/2024/09/20/reiting-krayin-za-rivnem-rozvitku-elektronnogo-uriaduvannia/ (Дата звернення: 05.11.2025).

26. The Constitution of Greece. As revised by the parliamentary resolution of May 27th, 2008, of the Vlllth Revisionary Parliament. URL: https://www.hellenicparliament.gr/UserFiles/f3c70a23-7696- 49db-9148-f24dce6a27c8/001 – 156%20aggliko.pdf (Дата звернення: 05.11.2025).

27. Місцеве самоврядування в країнах Скандинавії та Балтії. огляд 2020. SKL International, Hornsgatan 15, SE-118 82 Stockholm, Sweden, 2020. 84 с. URL: https://decentralization.ua/uploads/library/file/720/Ukrainian_finalver_bluebook_compressed.pdf (Дата звернення: 05.11.2025).

28. Закон України «Про інформацію» від 2 жовтня 1992 року № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (Дата звернення: 05.11.2025).

29. Закон України «Про стимулювання розвитку цифрової економіки в Україні» від 15 липня 2021 року № 1667-IX. URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text (Дата звернення: 05.11.2025).

30. Закон України «Про Національну програму інформатизації» від 1 грудня 2022 року № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text (Дата звернення: 05.11.2025).

31. Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. URL: https://www.legifrance.gouv.fr/affichTexte.do;isessionid=91758002E1CCA159BABD6D3F5D4 B33F4.tplgfr34s 2?cidTexte=JORFTEXT000033202746&categorieLien=id (Дата звернення: 05.11.2025).

32. Code des relations entre le public et l'administration. URL: https://www.legifrance.gouv.fr/affichCode.do;isessionid=91C91B1A73A68E15149FA32687E64163.t plgfr34s 2?idSectionTA=LEGISCTA000031367685&cidTexte=LEGITEXT000031366350&dateTex te=20190210 (Дата звернення: 05.11.2025).

33. Joinup. E-Government in Sweden, February 2016, Edition 18.0. URL: https://ioinup.ec.europa.eu/sites/default/files/inline-files/eGovernment%20in%20Sweden%20- %20February%202016%20-%2018 0 v1 00.pdf (Дата звернення: 05.11.2025).

34. Reichel J. Regulating Automation of Swedish Public Administration // CERIDAP. Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche. 2023. N° 1. P. 75-94. (Дата звернення: 05.11.2025).

35. USA. E-Government Act of 2002. URL: https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf (Дата звернення: 05.11.2025).

36. Sec. 3301, (a), "Presidential and Federal Records Act Amendments of 2014. URL: https://www.congress.gov/bill/113th-congress/house-bill/1233/text (Дата звернення: 05.11.2025).

37. USA. Freedom of Information Act. PUBLIC LAW 89-487-JULY 4, 1966. URL: https://www.govinfo.gov/content/pkg/STATUTE-80/pdf/STATUTE-80-Pg250.pdf (Дата звернення: 05.11.2025).

38. Codice dell'amministrazione digitale. Decreto Legislativo 7 marzo 2005, n. 82. URL: https://docs.italia.it/italia/piano-triennale-ict/codice-amministrazione-digitale-docs/it/v2017-12- 13/index.html (Дата звернення: 05.11.2025).

39. Italian Personal Data Protection Code. URL: http://www.privacy.it/archivio/privacycode-en.html (Дата звернення: 05.11.2025).

40. German Act to promote electronic government. Translation provided by Gary Cox for the Federal Ministry of the Interior. The translation includes the amendment(s) to the Act by Article 1 of the Act of 25 July 2013 (Federal Law Gazette I p. 2749). URL: http://www.gesetze-im- internet.de/englisch egovg/englisch egovg.html#p0014 (Дата звернення: 05.11.2025).

41. Österreich. Gesamte Rechtsvorschrift für E-Government-Gesetz, Fassung vom 20.06.2020. URL:

https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=200032
30#:~:text=(1)%20Dieses%20Bundesgesetz%20dient%20der,an%20diese%20Stellen%20erleichtert% 20werden (Дата звернення: 05.11.2025).

42. Tanzania. E-Government Act, 2019. URL: https://gisp.gov.go.tz/assets/docs/e- Government%20Act,%202019.pdf (Дата звернення: 05.11.2025).

43. Beliz. An Act to establish the E-Governance and Digitalization Department and provide for its powers, duties and functions; to promote and regulate the provision of electronic government (e- government) services; to enhance service delivery, citizen's access, and the efficiency and effectiveness of government administrative procedures; and to provide for matters connected therewith or incidental thereto. 2022. URL: https://www.nationalassembly.gov.bz/wp-content/uploads/2022/10/Act-No-24-of- 2022-Digital-Government-Act-2022.pdf (Дата звернення: 05.11.2025).

44. Papua New Guinea. Digital Government Act. 2022. URL: https://www.parliament.gov.pg/uploads/acts/22A 41.pdf (Дата звернення: 05.11.2025).

45. Canada, Policy on Service and Digital. URL: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32603 (Дата звернення: 05.11.2025).

46. Canada. Directive on Service and Digital. URL: https://www.tbs-sct.gc.ca/pol/doc- eng.aspx?id=32601 (Дата звернення: 05.11.2025).

References

1. France (2014), "Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques", available at:

https://www.legifrance.gouv.fr/loda/id/JORFTEXT000029122964 (Accessed 05 November 2025).

2. France (2005), “Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives”, available at: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000636232/ (Accessed 05 November 2025).

3. USA (2022), “National Institute of Standards and Technology Act, Section 20”, available at: https://www.govinfo.gov/content/pkg/COMPS-5388/pdf/COMPS-5388.pdf (Accessed 05 November 2025).

4. NIST (2018), “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1”, available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (Accessed 05 November 2025).

5. Vernadsky National Library of Ukraine (2014), “List of National Standards of Ukraine for the creation and support of automated and information systems”, available at: http://nbuv.gov.ua/node/1469 (Accessed 05 November 2025).

6. Security Service of Ukraine and Ministry of Internal Affairs (2022), “Order No. 360/657 on electronic information exchange”, available at: https://zakon.rada.gov.ua/laws/show/z1327-22#Text (Accessed 05 November 2025).

7. USA (2014), “Federal Information Security Modernization Act of 2014”, available at: https://www.congress.gov/bill/113th-congress/senate-bill/2521/text (Accessed 05 November 2025).

8. France (2022), “Décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat”, available at: https://www.legifrance.gouv.fr/loda/id/LEGIARTI000045539964/2022-10-01/ (Accessed 05 November 2025).

9. France (2022), “Arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI”, available at: https://www.legifrance.gouv.fr/jorf/id/JORFARTI000046503138#JORFARTI000046503138 (Accessed 05 November 2025).

10. CIO Council (2025), “CISO Committee”, available at: https://www.tio.gov/about/members-and-leadership/tiso-council/ (Accessed 05 November 2025).

11. Brilingaitè, A., Bukauskas, L., Juozapavicius, A. and Kutka, E. (2022), “Overcoming information-sharing challenges in cyber defence exercises”, Journal of Cybersecurity, vol. 8(1), available at: https://academic.oup.com/cybersecurity/article/8/1/tyac001/6516499 (Accessed 05 November 2025).

12. France (2022), “Décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics”, available at: https://www.legifrance.gouv.fr/loda/id/LEGIARTI000045539964/2022-10-01/ (Accessed 05 November 2025).

13. USA (2014), “Federal Information Security Modernization Act of 2014”, available at: https://www.congress.gov/bill/113th-congress/senate-bill/2521/text (Accessed 05 November 2025).

14. CISA (2017), “Federal Incident Notification Guidelines”, available at: https://www.cisa.gov/federal-incident-notification-guidelines (Accessed 05 November 2025).

15. USA (2021), “State and Local Government Cybersecurity Act of 2021”, available at: https://www.congress.gov/bill/117th-congress/senate-bill/2520/text (Accessed 05 November 2025).

16. USA (2022), “Strengthening American Cybersecurity Act of 2022, Sec. 107(b)”, available at: https://www.congress.gov/bill/117th-congress/senate-

bill/3600/text#toc-id87c2d95a-b307-45ec-81dd-09e23e4addc4 (Accessed 05 November 2025).

17. Snider, K.L.G., Shandler, R., Zandani, S. and Canetti, D. (2021), "Cyberattacks, cyber threats, and attitudes toward cybersecurity policies", Journal of Cybersecurity, vol. 7(1), available at: https://academic.oup.com/cybersecurity/article/7/1/tyab019/6382745 (Accessed 05 November 2025).

18. Dapel, M.E., Asante, M., Uba, C.D. and Agyeman, M.O. (2023), "Artificial Intelligence Techniques in Cybersecurity Management", Cybersecurity in the Age of Smart Societies, Springer, Cham.

19. Albataineh, H. and Nijim, M. (2021), "Enhancing the Cybersecurity Education Curricula Through Quantum Computation", Advances in Security, Networks, and Internet of Things, Springer, Cham.

20. Korrespondent.net (2019), "China adopts first-ever data encryption law", available at: https://ua.korrespondent.net/world/4153691-pershyi-v-istorii-zakon-pro-shyfruvannia-danykh-pryinialy-v-kytai (Accessed 05 November 2025).

21. Baranov, O. (2020), "E-Government in Ukraine? When will it happen? ", available at: https://dt.ua/SOCIETY/elektronniy_uryad_v_ukrayini_bude_koli.html (Accessed 05 November 2025).

22. Harrison, T.M., Pardo, T.A. and Cook, M. (2012), "Creating open government ecosystems: a research and development agenda", Future Internet, vol. 4(4), pp. 900–928.

23. O'Reilly, T. (2010), "Government as a Platform, Innovations, vol. 6(1), "pp. 13–40.

24. United Nations (2022), "UN E-Government Survey 2022", available at: https://desapublications.un.org/sites/default/files/publications/2022-09/Chapter%205.pdf (Accessed 05 November 2025).

25. AIN (2024), “UN publishes ranking of countries by e-government development – Ukraine ranks fifth in Online Service Index”, available at: https://ain.ua/2024/09/20/reiting-krayin-za-rivnem-rozvitku-elektronnogo-uriaduvannia/ (Accessed 05 November 2025).

26. Greece (2008), “The Constitution of Greece”, available at: https://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/001–156%20aggliko.pdf (Accessed 05 November 2025).

27. SKL International (2020), “Local self-government in the Nordic and Baltic countries: Review”, available at: https://decentralization.ua/uploads/library/file/720/Ukrainian_finalver_bluebook_compressed.pdf (Accessed 05 November 2025).

28. Verkhovna Rada of Ukraine (1992), “Law on Information”, available at: https://zakon.rada.gov.ua/laws/show/2657-12#Text (Accessed 05 November 2025).

29. Verkhovna Rada of Ukraine (2021), “Law on Stimulating the Development of the Digital Economy in Ukraine”, available at: https://zakon.rada.gov.ua/laws/show/1667-20#Text (Accessed 05 November 2025).

30. Verkhovna Rada of Ukraine (2022), “Law on the National Informatization Program ”, available at: https://zakon.rada.gov.ua/laws/show/2807-20#Text (Accessed 05 November 2025).

31. France (2016), “Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique”, available at: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&categorieLien=id (Accessed 05 November 2025).

32. France (2019), “Code des relations entre le public et l'administration”, available at: https://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000031367685&cidTexte=LEGITEXT000031366350&dateTexte=20190210 (Accessed 05 November 2025).

33.European Commission (2016), “Joinup: E-Government in Sweden, February 2016, Edition 18.0”, available at: https://joinup.ec.europa.eu/sites/default/files/inline-files/eGovernment%20in%20Sweden%20-%20February%202016%20-%2018_0_v1_00.pdf (Accessed 05 November 2025).

34.Reichel J. (2023), “Regulating Automation of Swedish Public Administration”, CERIDAP – Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche, vol. 1, pp. 75–94. (Accessed 05 November 2025).

35.USA (2002), “E-Government Act of 2002”, available at: https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf (Accessed 05 November 2025).

36.USA (2014), “Presidential and Federal Records Act Amendments of 2014, Section 3301(a), “available at: https://www.congress.gov/bill/113th-congress/house-bill/1233/text (Accessed 05 November 2025).

37.USA (1966), “Freedom of Information Act, Public Law 89-487”, available at: https://www.govinfo.gov/content/pkg/STATUTE-80/pdf/STATUTE-80-Pg250.pdf (Accessed 05 November 2025).

38.Italy (2005), “Codice dell’amministrazione digitale. Decreto Legislativo 7 marzo 2005, n. 82”, available at: https://docs.italia.it/italia/piano-triennale-ict/codice-amministrazione-digitale-docs/it/v2017-12-13/index.html (Accessed 05 November 2025).

39.Italy (2017), “Italian Personal Data Protection Code”, available at: http://www.privacy.it/archivio/privacycode-en.html (Accessed 05 November 2025).

40.Germany (2013), “Act to Promote Electronic Government (E-Government Act), “translation by Gary Cox for the Federal Ministry of the Interior”, available at: http://www.gesetze-im-internet.de/englisch_egovg/englisch_egovg.html (Accessed 05 November 2025).

41.Austria (2020), “E-Government-Gesetz (Federal E-Government Act)”, available at:

https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230 (Accessed 05 November 2025).

42. Tanzania (2019), “E-Government Act, 2019”, available at: https://gisp.gov.go.tz/assets/docs/e-Government%20Act,%202019.pdf (Accessed 05 November 2025).

43. Belize (2022), “Digital Government Act 2022, An Act to establish the E-Governance and Digitalization Department”, available at: https://www.nationalassembly.gov.bz/wp-content/uploads/2022/10/Act-No-24-of-2022-Digital-Government-Act-2022.pdf (Accessed 05 November 2025).

44. Papua New Guinea (2022), “Digital Government Act”, available at: https://www.parliament.gov.pg/uploads/acts/22A_41.pdf (Accessed 05 November 2025).

45. Canada (2020), “Policy on Service and Digital”, available at: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32603 (Accessed 05 November 2025).

46. Canada (2020), “Directive on Service and Digital”, available at: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32601 (Accessed 05 November 2025).

Стаття надійшла до редакції 05.11.2025 р.