Тетяна Кузь
West Ukrainian National University, Ukraine
ORCID: 0000-0002-6854-9230

Нормативно – правове забезпечення інформаційної безпеки в процесі організації та надання адміністративних послуг в Україні

Вступ

В сучасному світі спостерігається стрімкий розвиток інформаційно-комунікаційних технологій та розширюються можливості участі громадян в державотворчих процесах. На шляху розбудови інформаційного суспільства активно впроваджується електронне урядування, яке покликане підвищувати ефективність, відкритість і прозорість діяльності органів публічної адміністрації з використанням інформаційно-комунікаційних технологій та передбачає можливість громадян отримувати електронні адміністративні послуги.

Впровадження і використання е-урядування вимагає обов'язкового формування нормативно-правової бази, а також забезпечення інформаційної безпеки в процесі взаємодії органів держави та громадян через надання доступу до державних інформаційних ресурсів.

Актуальність теми дослідження зумовлена потребою вдосконалення діючих програм та завдань державної політики в сфері надання електронних адміністративних послуг та забезпечення інформаційної безпеки. Необхідним є створення безпечного інформаційного середовища та особливих вимог до ідентифікації і автентифікації, а також інтеграція інформаційних систем, різних технологій інформаційної безпеки при вирішенні завдань, широке використання мобільних інформаційно-комунікаційних технологій, упор як на інформаційну безпеку системи, так і кінцевого користувача.

Інформаційна безпека адміністративних послуг, в силу її визначальної ролі у забезпеченні національної безпеки, знаходяться у фокусі наукових досліджень вчених правників, економістів та політологів. Теоретичні проблеми, пов'язані з різними аспектами процесу надання послуг досліджувались в наукових роботах наступних зарубіжних авторів: М. Вебера, І. Фішера, А. Маршалла, А. Сміта, Д. Коатса, С. Нілсона, та ін.

У національній правовій науці досі залишається дискусійним питання про сутність інформаційної безпеки процесу надання адміністративних послуг. Результатом аналізу наукового доробку фахівців різних галузей наукових досліджень стало формування близько двох десятків визначень різних за своїм змістовим навантаженням. Серед вітчизняних авторів, які досліджували інформаційну безпеку адміністративних послуг, можна виділити Бендікова М.А., Г. Гулака, Гончаренко Л.П., Драга А.А., Вишнякова Я.Д., Клейнера Г.Б., Костицького В.,Олейникова Е.А., М. Єрмошенко, В. Мунтіян, Клімушина П.С., Тамбовцева В.Л., Черкавав В.В. та ряд інших.

Мета наукового дослідження полягає в проведенні комплексного аналізу нормативно-правових основ адміністративно-правового регулювання в сфері інформаційної безпеки під час організації та надання електронних адміністративних послуг, в розробці рекомендацій щодо його вдосконалення.

Передумови впровадження електронного урядування в Україні

Інформаційно-комунікаційні технології стали основним інструментом електронного урядування, яке має на меті впровадити нові форми взаємодії між громадянами та владою, забезпечити швидкий та безперешкодний доступ до публічної інформації та надання якісних адміністративних послуг. Запровадження електронного урядування покликане прискорити і спростити інформаційні процеси в державі, знизити прояви корупції та підвищити відкритість влади та виконавчих функцій держави, зокрема в сфері надання адміністративних послуг.

У сучасному розумінні термін «e-government» тлумачиться як електронний уряд або ж як електронне управління державою, тобто використання органами публічного управління сучасних Інтернет-технологій в процесі надання адміністративних послуг.[1]

В теорії адміністративного права прийнято виокремлювати певні рівні (сектори) взаємодій між державою та громадянами в процесі е-урядування. В основному виділяють чотири сектори взаємодії:

1. G2G «government to government» - передбачає надання адміністративних послуг одним державним органом іншим адміністративним органам;
2. G2C «government to citizens» - надання адміністративних послуг громадянам;

[1] Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2017. Частина 2: Електронне урядування: основи та стратегії реалізації / [А.І. Семенченко, А.О. Серенок]. – К.: ФОП Москаленко О.М., 2017. – с. 7.

3. G2B «government to business» - надання адміністративних послуг господарюючим суб'єктам;
4. G2E «government-to-employees» - надання адміністративних послуг державним службовцям.[2]

Саме сектор G2C (уряд – громадяни) призначений для полегшення взаємодії громадян та органів влади під час здійснення процедури надання органами влади адміністративних послуг, в тому числі за допомогою мережі Інтернет. Електронні послуги повинні бути доступними постійно в форматі 24/7/365.

Електронне урядування активно впроваджується в Україні. В 2012 році було прийнято Закон України «Про адміністративні послуги», який започаткував реформування системи адміністративного управління і формування правових, організаційних та економічних передумов для цього. В 2013 році було схвалено Стратегію розвитку інформаційного суспільства в Україні до 2020 року, якою були визначені засади щодо надання електронних адміністративних послуг в Україні, враховуючи сучасні особливості розвитку інформаційного простору. Сенс їх у тому, щоб реалізувати адміністративні послуги в електронному вигляді на основі нових інформаційних систем і рішень. Ці документи заклали фундамент розвитку електронного урядування в нашій країні. Згодом Урядом була затверджена Концепція розвитку електронного урядування, якою було визначено напрямок, механізми та строки формування ефективної системи електронного урядування в Україні.[3]

На сьогодні прийнято більше, ніж 300 нормативно-правових актів, що стосуються електронного урядування та інформаційної політики в Україні. Таким чином, можна стверджувати, що робота над необхідною нормативно-правовою базою в цій галузі в нашій державі активно ведеться.

«Дія» – інтегрований портал електронних адміністративних послуг в Україні

В 2019 році в Україні було утворене Міністерство цифрової трансформації для реалізації проєкту «держава в смартфоні». Відтак було розроблено застосунок «Дія» (Держава і Я), який став інтегрованим порталом для отримання низки адміністративних послуг онлайн. Головною метою застосунку

[2] Y.N. Chen, H. M. Chen, W. Huang, E-Government Strategies in Developed and Developing Countries: An Implementation Framework and Case Study. // Journal of Global Information Management 2009 Vol. 14 №1. P. 23.

[3] Концепція розвитку електронного урядування, затверджена розпорядженням Кабінету Міністрів України від 20 вересня 2017 № 649-р URL: https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text.

є створення інфраструктури електронного уряду, що забезпечує доступ до інформації про діяльність та послуги органів державної влади в електронному вигляді, міжвідомчу електронну взаємодію і єдиний державний контроль результативності діяльності органів державної влади.

Через застосунок «Дія» громадянам надається можливість відвідувати державні портали, подавати податкові декларації і заявки на отримання соціальних пільг, сплачувати податки та штрафи, отримувати ліцензії і дозволи, оформляти персональні документи, реєструвати автотранспорт, свідоцтва та інші. Для здійснення цих операцій необхідним є онлайн звернення, під час якого весь подальший обмін документами і інформацією відбуватиметься у визначені терміни безпосередньо між органами влади.

Авторизуватися в «Дії» може лише особа, яка співпрацює з одним із банків в Україні, оскільки, на думку розробників застосунку, банк є найбільш надійним способом ідентифікації. Авторизація через банк потрібна для того, щоб лише користувач міг побачити свої документи, а не хтось інший.

В березні 2021 року Верховною Радою України було ухвалено закон, згідно з яким електронні паспорти у Дії стали застосовуватися на рівні із паперовими документами. А з липня 2021 року в Україні було запущено внутрішні та міжнародні сертифікати вакцинації від COVID-19, що стали доступні в мобільному додатку «Дія».

Таким чином, ми спостерігаємо активну роботу законодавчих і виконавчих органів нашої держави в сфері електронного урядування. Це є високим показником належності держави до світового інформаційного суспільства та являється головним інструментом стабілізації системи надання адміністративних послуг. За результатами дослідження Організації Об'єднаних Націй «E-Government Survey» в рейтингу країн, які мають високий рівень розвитку електронного урядування, Україна посідає 69-е місце із 193 країн. А за рівнем електронної участі наша держава на 46 місці.[4] Це свідчить про позитивну динаміку в порівнянні з минулими роками.

Основні компоненти безпечного інформаційного середовища в процесі е-урядування.

З активним розвитком системи адміністративних послуг населенню в електронній формі, виникла необхідність забезпечення безпечної електронної інформаційної взаємодії між громадянами, які використовують інфор-

[4] UN E-Government Survey 2020 Digital Government in the Decade of Action for Sustainable Development URL: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020.

маційно-комунікаційні технології, з одного боку, і державою та муніципалітетами, які використовують інформаційні технології, з іншого боку.

Щорічно збільшуються масштаби використання громадянами мобільних пристроїв для отримання послуг в електронній формі. У багатьох вже є засоби ідентифікації. Це банківські пластикові картки, USB-ідентифікатори, відбитки пальців, номер мобільного телефону, логін і пароль e-mail. Сьогодні все частіше використовується електронний цифровий підпис, тобто *електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис.*[5] Його можуть використовувати як фізичні, так і юридичні особи для ідентифікації чи підтвердження цілісності даних в електронному документі.

Сучасні підходи, методи і засоби забезпечення інформаційної безпеки при наданні населенню послуг в електронній формі обумовлені необхідністю створення прозорого інформаційного середовища, використанням віртуалізації і хмарних обчислень, наявністю особливих вимог до ідентифікації і автентифікації, необхідністю забезпечення безперервності бізнес-процесів, інтеграцією різних інформаційних систем, необхідністю інтеграції різних технологій інформаційної безпеки при вирішенні завдань, широким використанням мобільних інформаційно-комунікаційних технологій, акцентом як на інформаційну безпеку системи, так і на кінцевого користувача, збільшенню питомої ваги персональних даних в інформаційному просторі.[6]

Тут виникла необхідність забезпечити не тільки перевірку програм, операційних систем і даних, а й апаратних засобів на предмет їх інформаційної безпеки. Рішення було знайдено наступне: винести ключові операції по забезпеченню безпеки в ізольоване апаратне середовище, що дозволяє перевірити її і прошивки управління без порушення цілісності засобу захисту інформації. Такий засіб отримав назву «резидентний компонент безпеки», а нова концепція безпеки отримала назву «інформаційне середовище на основі резидентних компонентів безпеки». В англомовному варіанті вона позначається як Trasted Platform Module.[7]

Загрози інформаційній безпеці мають місце і в роботі з державними реєстрами в Україні. З появою електронного реєстру прав з'явились особи, які шляхом маніпуляцій з відомостями в ньому незаконно заволодівають

---

[5] Про електронні довірчі послуги: Закон України від 05 жовтня 2017 року № 2155-VIII URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

[6] Alharbi, (2013) E-government security modeling: explain main factors and analyzing existing models, International Journal of Social, Human Science and Engineering Vol: 7 No: 9, P. 7.

[7] K. Layne and J. Lee,(2001) Developing fully functional Egovernment: A four stage model. Government Information Quarterly, vol. 18, no. 3, p. 124.

чужим майном. Тому важливим є дотримання правил безпеки державними службовцями, які мають право доступу до цих реєстрів в системах електронного урядування при роботі онлайн. Фахівці з безпеки мереж повинні звертати увагу на правильний підбір типу шифрування протоколу взаємодії з відповідним роутером мережі, аби зловмисник не мав можливості змінити публічний DNS-сервер на свій.[8]

Поширеним способом викрадення персональних даних є перехоплення інформації з комп'ютера службової особи за допомогою атаки «men-in-the-middle», яка призводить до того, що інформація, яка відправляється до Wi-Fi роутера службовця, перенаправляється зловмиснику, а вже потім потрапляє до вірного адресата. Це призводить до викрадення особистих даних, логінів та паролів.

Найбільш уразливими в даний час з точки зору захисту персональних даних є інформаційні системи муніципального рівня. Основними причинами цього є складність і різнорідність програмного та апаратного забезпечення, що використовуються в системах електронного урядування, велика кількість вузлів корпоративної мережі, їх територіальна розділеність, підключення зовнішніх користувачів (підприємств, організацій, окремих громадян) до відкритих сервісів і надання прав персоналу органу публічного управління щодо віддаленої роботи з внутрішніми інформаційними ресурсами.[9]

На подолання цих проблем і загроз повинна бути спрямована діяльність держави в галузі забезпечення інформаційної безпеки. Нормативно-правову базу в цій сфері складають міжнародні та національні нормативні акти, а також відповідні документи окремих органів публічного адміністрування. Закони України «Про інформацію» та «Про захист інформації в інформаційно-телекомунікаційних системах» є базовими законодавчими актами, що визначають основні напрямки державної інформаційної політики в України. Окрім того Указом Президента України від 14 вересня 2020 року № 392/2020 затверджено Стратегію національної безпеки України, а Указом Президента України від 26 серпня 2021 року Стратегію кібербезпеки України. У вересні 2021 року Уряд схвалив Стратегію інформаційної безпеки України до 2025 року.

Всі ці нормативні документи передбачають створення умов для реалізації державної політики в сфері протидії внутрішнім та зовнішнім загрозам

[8] Y. Zhovnirchyk, & A. Martseniuk, (2020). Electronic governance and electronic workflow in the process of adoption management decisions. Public Administration and Regional Development, (6), p. 807.

[9] J. Fedorowicz, U.J.Jr. Gelinas, J.L. Gogan, Strategic alignment of participant motivations in e-government collaborations: The Internet Payment Platform pilot // Government Information Quarterly, January, 2009. – Vol. 26. – № 1. – P. 51.

інформаційній безпеці, зокрема й в процесі здійснення електронного урядування. Та не менш важливу роль відіграє цифрова грамотність населення, яка передбачає дотримання певних правил безпеки споживачами послуг в системах електронного урядування.

Насамперед слід застосовувати двофакторну автентифікацію при кожній реєстрації та використовувати біометричні дані для активації пристроїв та застосунків.[10] Особливу увагу необхідно приділити паролями, використовуючи складні комбінації. Їх необхідно регулярно оновлювати та використовувати різні для різних сервісів і застосунків. Якщо це можливо – використовувати електронний цифровий підпис.

Висновки

У даній статті ми зупинилися на важливих напрямах забезпечення інформаційної безпеки в процесі організації та надання громадянам послуг в електронній формі. Безпечне інформаційне середовище є основою гарантії інформаційної безпеки держави. Використання безпечного інформаційного середовища позначає перехід до загальнометодологічних підходів забезпечення інформаційної безпеки в сфері застосування інформаційних систем. Основними компонентами безпечного інформаційного середовища є: безпечне середовище передачі даних з сертифікованим комунікаційним обладнанням, сертифіковані обчислювальні комплекси на основі безпечного операційного середовища та безпечні системи зберігання інформації. Важливу роль відіграє цифрова грамотність громадян щодо організаційно-технічних заходів захисту, які застосовуються на рівні певної організації та системи публічного управління.

* * *

Regulatory and legal support of information security in the process of organization and provision of administrative services in Ukraine

(summary)

The article analyzes the provisions of regulations that reflect the official system of views on information security in the organization of administrative services.

[10] G. Rasha (2016), Hassan, Othman O. Khalifa "E-Government - an Information Security Perspective". International Journal of Computer Trends and Technology (IJCTT) V36(1): 1-9, June 2016. ISSN: 2231-2803. www.ijcttjournal.org. Published by Seventh Sense Research Group.

The necessity of their further development and formation of a unified approach to information security as a complex area of activity is substantiated. The threats to information security during the introduction of e-government in Ukraine and the essence of its means of analysis are also analyzed. The author concludes that a secure information environment is the basis for guaranteeing information security of the state. The main components of a secure information environment are: a secure data transmission medium with certified communication equipment, certified computing systems based on a secure operating environment and secure information storage systems. An important role is played by digital literacy of citizens on organizational and technical protection measures applied at the level of a particular organization and system of public administration.

Список використаних джерел:

Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2017. Частина 2: Електронне урядування: основи та стратегії реалізації / [А.І. Семенченко, А.О. Серенок]. – К.: ФОП Москаленко О.М., 2017. – 72 с.

Концепція розвитку електронного урядування, затверджена розпорядженням Кабінету Міністрів України від 20 вересня 2017 № 649-р URL: https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text (Дата звернення 14.11.2021).

Про електронні довірчі послуги: Закон України від 05 жовтня 2017 року № 2155-VIII URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (Дата звернення 14.11.2021).

Alharbi, (2013) E-government security modeling: explain main factors and analyzing existing models, International Journal of Social, Human Science and Engineering Vol: 7 No: 9.

Chen Y.N., Chen H. M., Huang W. E-Government Strategies in Developed and Developing Countries: An Implementation Framework and Case Study. // Journal of Global Information Management 2009 Vol. 14 №1. P. 23–46.

Fedorowicz J., Gelinas U.J.Jr., Gogan J.L. Strategic alignment of participant motivations in e-government collaborations: The Internet Payment Platform pilot // Government Information Quarterly, January, 2009. – Vol. 26. – № 1. – P. 51–59.

K. Layne and J. Lee, (2001) Developing fully functional Egovernment: A four stage model. Government Information Quarterly, vol.18, no.3, pp.122 -136, 2001.

Rasha G. (2016) Hassan, Othman O. Khalifa «E-Government - an Information Security Perspective». International Journal of Computer Trends and Technology (IJCTT) V36(1):1-9, June 2016. ISSN:2231-2803. www.ijcttjournal.org. Published by Seventh Sense Research Group.

UN E-Government Survey 2020 2020 Digital Government in the Decade of Action for Sustainable Development URL: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020 (Дата звернення 14.11.2021).

Zhovnirchyk, Y., & MartseniukA. (2020). Electronic governance and electronic workflow in the process of adoption management decisions. Public Administration and Regional Development, (6), 802-823. https://doi.org/10.34132/pard2019.06.05.