DOI 10.52363/2414-5866-2024-2-37
УДК 351:37

***Сеідова-Богословська Е.Г.**, аспірант, НАУ ім. М.Є. Жуковського, «ХАІ», м. Харків, ORCID: 0000-0002-3334-5959*

***Seidova-Bohoslovska E.**, graduate student, National Aerospace University H.E. Zhukovsky «Kharkiv Aviation Institute», Kharkiv*

МЕХАНІЗМИ ПУБЛІЧНОГО УПРАВЛІННЯ ЗАХИСТОМ ЦИФРОВИХ ТЕХНОЛОГІЙ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ ТА МІСЦЕВОГО САМОВРЯДУВАННЯ

MECHANISMS OF PUBLIC ADMINISTRATION OF PROTECTION OF DIGITAL TECHNOLOGIES OF STATE AUTHORITIES AND LOCAL GOVERNMENTS

У статті здійснено вдосконалення механізмів публічного управління захистом цифрових технологій органів державної влади та місцевого самоврядування. Зокрема, виявлено загрози цифровим технологіям органів державної влади та місцевого самоврядування; окреслено напрями закордонної допомоги щодо захисту цифрових технологій органів державної влади та місцевого самоврядування; виокремлено напрями вдосконалення механізмів захистом цифрових технологій органів державної влади та місцевого самоврядування. Зазначено, що кібератаки були характерною рисою зусиль росії щодо спричинення складнощів у функціонуванні Уряду України як до, так і протягом повномасштабного вторгнення. За кілька тижнів до та після вторгнення російські урядові хакери та приватні особи здійснили кілька кібератак на український Уряд та приватний сектор. Підкреслено, що Україна відповіла на ці загрози, запровадивши найсучасніші засоби захисту кібербезпеки, які досі підтримували державні послуги онлайн і захищали персональні дані. «Дія», наприклад, не зберігає інформацію, що мінімізує можливості витоку даних, а найсучасніша криптографія Трембіти забезпечує безпечну передачу інформації. Акцентовано увагу на тому, що інвестиції урядів союзників також зіграли ключову роль у зміцненні захисту кібербезпеки. Незабаром після початку конфлікту американські приватні компанії співпрацювали з українськими урядовими міністерствами та неурядовими організаціями, щоб забезпечити критично важливі державні та приватні системи. Підкреслено, що разом із відновленням та покращенням доступу до Інтернету Україна має інвестувати в партнерства, які розширюють доступ українців до цифрових пристроїв. Відносно високе використання мобільних пристроїв серед населення України сприяє використанню таких програм для смартфонів, як «Дія».

***Ключові слова:** публічне управління, механізми, кіберзагрози, цифрові технології, органи державної влади та місцевого самоврядування.*

The article improves the mechanisms of public administration of protection of digital technologies of state authorities and local governments. In particular, the threats to digital technologies of state authorities and local governments are identified; the directions of foreign assistance for the protection of digital technologies of state authorities and local governments are outlined; the directions of improvement of mechanisms of protection of digital technologies of state authorities and local governments are allocated. It is noted that cyberattacks were a characteristic feature of Russia's efforts to cause difficulties in the functioning of the Government of Ukraine both before and during a full-scale invasion. In the weeks before and after the invasion, Russian government hackers and individuals carried out several cyber-attacks on the Ukrainian Government and private sector. It is emphasized that Ukraine has responded to these threats by introducing the most modern cybersecurity protection tools, which until now have supported public services online and protected personal data. "Diya," for example, does not store information that minimizes the possibility of data leakage, and the most modern Trembita cryptography ensures the safe transmission of information. It is emphasized that the investments of the allied governments also played a key role in strengthening the protection of cybersecurity. Shortly after the conflict began, American private companies collaborated with Ukrainian government ministries and non-governmental organizations to provide critical public and private systems. It is emphasized that, together with the restoration and improvement of access to the Internet, Ukraine should invest in partnerships that expand the access of Ukrainians to digital devices.

Keywords: *public administration, mechanisms, cyber threats, digital technologies, public authorities and local governments.*

Постановка проблеми. Оскільки уряд України та її міжнародні партнери дивляться у післявоєнне майбутнє та починають планувати реконструкцію, швидка та широкомасштабна цифровізація створює як безпрецедентні можливості, так і ризики. Однак сьогодні всі державні бази даних України працюють онлайн. Це розширює доступність послуг і створює більш ефективний і підзвітний уряд, але також створює ризики кібератак. Порушення можуть скомпрометувати особисті дані або позбавити громадян доступу до державних веб-сайтів і програм. Оскільки українці не можуть відмовитися від онлайн-зберігання своєї особистої інформації, здатність уряду постійно захищати ці системи від атак є життєво важливою для побудови інституційної довіри.

Кібератаки можуть порушити діяльність уряду та поставити під загрозу критичну інфраструктуру майже в будь-якій країні. Однак існує небагато країн, де державні служби настільки залежні від цифрової інфраструктури, як Україна. Таким чином, система електронного врядування та її величезний вплив на суспільну довіру до уряду, як описано вище, є основною мішенню державних і недержавних суб’єктів, які прагнуть завдати Україні військової поразки чи іншим чином підірвати її суверенітет і стабільність. Все це обумовлює актуальність обраної теми дослідження.

Аналіз останніх досліджень і публікацій. Питання цифровізації діяльності органів держвної влади та місцевого самоврядування досліджували численні вчені та практики, зокрема, Н. Бондарчук, Н. Петренко, Г. Разумей та ін. Однак механізми публічного управління в зазначеній сфері в сучасних реаліях все ще залишаються недостатньо розробленими.

Постановка завдання. Враховуючи описану вище актуальність теми дослідження, метою статті є вдосконалення механізмів публічного управління захистом цифрових технологій органів державної влади та місцевого самоврядування.

Для досягнення поставленої мети в роботі вирішуються наступні завдання:

- виявити загрози цифровим технологіям органів державної влади та місцевого самоврядування;
- окреслити напрями закордонної допомоги щодо захисту цифрових технологій органів державної влади та місцевого самоврядування;
- виокремити напрями вдосконалення механізмів захистом цифрових технологій органів державної влади та місцевого самоврядування.

Виклад основного матеріалу. Кібератаки були характерною рисою зусиль росії щодо спричинення складнощів у функціонуванні Уряду України як до, так і протягом повномасштабного вторгнення. За кілька тижнів до та після вторгнення російські урядові хакери та приватні особи здійснили кілька кібератак на український Уряд та приватний сектор. Серед них – розподілені атаки типу «відмова в обслуговуванні» (DDoS), які вивели з ладу Міністерство закордонних справ України та посольство України в США. Крім того, російські кіберзлочинці також поширювали дезінформацію про те, що українські банкомати не працюють, ймовірно, намагаючись підірвати довіру суспільства до банківської системи. Ці атаки тривають протягом усього періоду повномасштабного вторгнення. Так, тільки в період з лютого по грудень 2022 року було здійснено 1655 російських кібератак проти України. З цих атак понад 300 були спрямовані на сектор безпеки та оборони, 500 були спрямовані на інші державні установи, а 400 були спрямовані на приватні організації з прямим впливом на цивільних осіб (включаючи енергетичні, телекомунікаційні, фінансові та програмні компанії). Одна з кібератак порушила доступ до найбільшої в Україні стільникової мережі «Київстар» та пошкодила систему оповіщення про повітряну тривогу [2; 5].

Україна відповіла на ці загрози, запровадивши найсучасніші засоби захисту кібербезпеки, які досі підтримували державні послуги онлайн і захищали персональні дані. «Дія», наприклад, не зберігає інформацію, що мінімізує можливості витоку даних, а найсучасніша криптографія Трембіти забезпечує безпечну передачу інформації. Інвестиції урядів союзників також зіграли ключову роль у зміцненні захисту кібербезпеки. Сполучені Штати Америки, Сполучене Королівство Великої Британії і Північної Ірландії та

Європейський Союз співпрацюють з Україною над її зусиллями з цифровізації з 2016 року через проєкт «Прозорість і підзвітність у державному управлінні та послугах» (TAPAS) та проєкт EGOV4UKRAINE, який реалізується через Естонську академію електронного урядування. У червні 2023 року Сполучені Штати Америки пообіцяли надати Україні щонайменше 37 мільйонів доларів на підтримку кібербезпеки [1; 3].

Агентство США з міжнародного розвитку (USAID) також пообіцяло виділити додаткові 200 мільйонів доларів США на фінансування роботи з демократії, державного управління та прав людини в Україні, що включає фінансування проєкту «Цифрова екосистема для підзвітного управління відновленням» (DREAM) та інші зусилля з цифровізації для підтримки постконфліктного відновлення України. Проєкт EU4DigitalUA також надав значну підтримку для додаткових функцій «Дії» у відповідь на нові потреби, а Сполучене Королівство також надало підтримку для реагування на кіберінциденти, обміну інформацією, програмного та апаратного забезпечення. У грудні 2023 року Сполучені Штати Америки та дев'ять інших країн офіційно оформили Талліннський механізм – ініціативу, яка має допомогти Україні покращити її довгострокову кіберстійкість та захистити себе в кіберпросторі.

Незабаром після початку конфлікту американські приватні компанії співпрацювали з українськими урядовими міністерствами та неурядовими організаціями, щоб забезпечити критично важливі державні та приватні системи. Google, наприклад, розширив безкоштовне розповсюдження Project Shield, рішення для захисту від DDoS, до додаткових організацій, які знаходяться в безпосередній близькості до війни, серед яких станом на листопад 2023 року знаходилося понад 150 українських установ. Додатково на рівні Cloudflare Project Galileo, який пропонує безкоштовний захист від DDoS для неурядових організацій, у березні 2022 року кількість заявок на отримання послуг від українських організацій зросла на 177 відсотків. Amazon Web Services і Microsoft допомогли приватним і державним організаціям безпечно перенести свої дані на віддалені хмарні сервери, розташовані за межами України, що запобігло знищенню збережених даних на фізичному обладнанні. Станом на червень 2022 року Amazon Web Services повідомила про переміщення 10 петабайт (10 мільйонів гігабайт) даних з державних міністерств, шкіл і промисловості в хмару, і щодня переміщення інформації продовжується [2; 4].

У майбутньому перед Україною постає подвійний виклик: реконструкція інфраструктури, яка була зруйнована під час війни, а також будівництво нових мереж 5G. У 2022 році такі великі інтернет-провайдери, як «Київстар», «Vodafone» і «Lifecell», запропонували покриття 4G для приблизно 90% території України. Хоча ще в 2019 році Уряд України оголосив про план розгортання мереж 5G, його було відкладено в 2020 році, а потім призупинено через російське повномасштабне впровадження у 2022 році. Однак

Україна оголосила про нещодавні плани запровадити пілотне випробування 5G у 2024 році, щоб продовжити розробку найсучаснішої інфраструктури для потреб країни, що зростає в цифровому світі. Договір між Україною та Латвією в жовтні 2023 року також зобов'язався сприяти розгортанню 5G в Україні, спираючись на постійне прагнення України до ширшої реконструкції широкосмугового зв'язку в сільських і міських районах для забезпечення більш рівномірного підключення в міру розширення онлайн-сервісів [3; 5].

Високошвидкісний широкосмуговий доступ має вирішальне значення для того, щоб українці могли скористатися цифровими можливостями, включаючи віддалену роботу, онлайн-освіту та онлайн-ресурси уряду. Швидкосмуговий зв'язок в Україні повільніший, ніж у більшості країн Європейського Союзу та Сполучених Штатах Америки, а це означає, що користувачам може бути важко працювати з кількома пристроями одночасно, транслювати вміст у прямому ефірі чи виконувати інші дії з високою пропускною здатністю. Швидкість фіксованого інтернету в Україні зросла з 2022 по 2023 рік, але швидкість мобільного інтернету за цей же період знизилася [1; 4].

Міжнародні державні установи та технологічні компанії вже підтримали доступність як ноутбуків, так і смартфонів в Україні. Ці ініціативи включають програму Європейського Союзу «Ноутбуки для України», яка передала понад 25 000 ноутбуків, телефонів та інших цифрових пристроїв українським школам, лікарням і муніципалітетам. Також UNICEF передав 5 тис. ноутбуків і планшетів українським вчителям та 10 тис. – учням. Крім того, HP і Microsoft у партнерстві з місцевими некомерційними організаціями, USAID і посольством України в Сполучених Штатах Америки здійснили постачання десятків тисяч ноутбуків, планшетів і програмного забезпечення для класів у 12 регіонах України. Європейські оператори також створили точки доступу Wi-Fi поблизу таборів для біженців і громадського транспорту, куди прибувають біженці, і роздали понад 2,5 мільйона безкоштовних SIM-карт. USAID виділив майже 1,2 мільйона доларів США для підтримки технологічного сектора України після російського вторгнення, що підвищило стійкість сектора та допомогло країні продовжити цифрову трансформацію [2; 4].

Разом із відновленням та покращенням доступу до Інтернету Україна має інвестувати в партнерства, які розширюють доступ українців до цифрових пристроїв. Відносно високе використання мобільних пристроїв (орієнтовно 91%) серед населення України сприяє використанню таких програм для смартфонів, як «Дія», але нижчий рівень володіння комп'ютером (приблизно 66% населення) може зменшити здатність українців брати участь у дистанційній роботі чи навчанні [1-3].

Висновки. У цілому, зберігання та захист цифрових даних в органах державної влади та місцевого самоврядування є коштовним, і уряд України зрештою повинен буде розробити довгостроковий план фінансування цих заходів. Коли Україна перейде до процесу реконструкції, вона може розгля-

нути способи найкращого використання партнерства з приватними технологічними компаніями для моніторингу та реагування на тенденції, що розвиваються в ландшафті кіберзагроз.

Список використаних джерел:

1. Бондарчук Н. В. Взаємодія органів публічної влади та громадянського суспільства в умовах цифровізації. *Публічне управління і адміністрування в Україні*. 2022. Вип. 28. С.36-39.
2. Ключевський В. Використання сучасних цифрових технологій при наданні адміністративних послуг на регіональному рівні. *Механізми державного управління*. 2018. № 4 (76). С. 47-51.
3. Петренко Н. О., Машковська Л. В. Цифровізація державних адміністративних послуг в Україні: нормативно-правові аспекти. *Право і суспільство*. 2020. № 2. С. 112-119.
4. Разумей Г. Ю., Разумей М. М. Діджиталізація публічного управління як складник цифрової трансформації України. *Публічне управління та митне адміністрування*. 2020. № 2(25). С.139-145.
5. Тищенкова І. О. Адміністративні процедури надання електронних послуг публічною адміністрацією в Україні. *Форум права*. 2017. № 2. С. 124-129.

References:

1. Bondarchuk N.V. Vzaiemodiia orhaniv publichnoi vlady ta hromadianskoho suspilstva v umovakh tsyfrovizatsii [Interaction of public authorities and civil society in the conditions of digitalization]. Publichne upravlinnia i administruvannia v Ukraini. 2022. Vol. 28. P.36-39.
2. Kliuchevskyi V. Vykorystannia suchasnykh tsyfrovykh tekhnolohii pry nadanni administratyvnykh posluh na rehionalnomu rivni [The use of modern digital technologies in the provision of administrative services at the regional level]. Mekhanizmy derzhavnoho upravlinnia. 2018. Vol. 4 (76). P. 47-51.
3. Petrenko N. O., Mashkovska L. V. Tsyfrovizatsiia derzhavnykh administratyvnykh posluh v Ukraini: normatyvno-pravovi aspekty [Digitization of public administrative services in Ukraine: regulatory and legal aspects]. Pravo i suspilstvo. 2020. Vol. 2. S. 112-119.
4. Razumei H. Yu., Razumei M. M. Didzhytalizatsiia publichnoho upravlinnia yak skladnyk tsyfrovoi transformatsii Ukrainy [Digitization of public administration as a component of digital transformation of Ukraine]. Publichne upravlinnia ta mytne administruvannia. 2020. № 2(25). S.139-145.
5. Tyshchenkova I. O. Administratyvni protsedury nadannia elektronnykh posluh publichnoiu administratsiieiu v Ukraini [Administrative procedures for the provision of electronic services by the public administration in Ukraine]. Forum prava. 2017. Vol. 2. S. 124–129.