УДК 342.9 (477)
DOI https://doi.org/10.32844/2618-1258.2025.2.19

ОКСЮТЕНКО К.В.

АДМІНІСТРАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ЕЛЕКТРОННОГО УРЯДУВАННЯ В УМОВАХ ВОЄННОГО СТАНУ

ADMINISTRATIVE AND LEGAL REGULATION OF ELECTRONIC GOVERNMENT IN THE CONDITIONS OF MARTIAL STATE

Наукова публікація присвячена дослідженню актуальних питань адміністративно-правового регулювання електронного урядування в умовах воєнного стану.

Зазначається, що повномасштабна війна російської федерації проти України включає в себе і багаточисельні кібератаки, що становить загрозу інформаційній безпеці та нормальному функціонуванню держави та суспільства в цілому.

У вказаних умовах особливої актуальності набуває питання забезпечення кібербезпеки та інформаційної безпеки в цілому. Зазначається, що найчастіше об'єктом ворожих кібератак є державні реєстри, автоматизовані інформаційно-телекомунікаційні системи, офіційні сторінки органів публічної адміністрації та Єдиний портал державних послуг «Дія», які в сукупності складають національний механізм електронного урядування.

Формулюється висновок про те, що в умовах дії правового режиму воєнного стану питання забезпечення кібербезпеки та національної інформаційної безпеки в цілому є одними із пріоритетних напрямів державної політики та потребують особливої уваги органів публічної адміністрації. З метою надійного захисту всіх елементів механізму електронного урядування пропонується нормативно врегулювати питання використання технології штучного інтелекту у сфері забезпечення кібербезпеки. Алгоритми технології штучного інтелекту здатні ефективно відстежувати шпигунські програми, а також інформацію, яка не відповідає дійсності (фейкові повідомлення, дезінформацію), протидіяти спам-атакам шляхом блокування зовнішніх інформаційних ресурсів та небажаних повідомлень, відстежувати факти несанкціонованого втручання в роботу автоматизованих інформаційно-телекомунікаційних систем тощо.

З метою забезпечення збереження національних інформаційних ресурсів пропонується зберігати їх на декількох альтернативних серверах, використовувати засоби криптографічного захисту інформації та незалежність від Інтернет (можливість блокування доступу до них зі всесвітньої мережі). Зокрема, копії державних реєстрів та інформаційно-телекомунікаційних систем бажано зберігати на кількох альтернативних та незалежних один від одного серверах, які розташовані як в Україні, так і в цивілізованих зарубіжних країнах, з якими національними органами публічної адміністрації укладені відповідні договори про надання цифрових послуг.

Ключові слова: *електронне урядування, воєнний стан, органи публічної адміністрації, правове регулювання, інформаційні технології, інформаційна безпека, кібербезпека, суб'єкти владних повноважень, цифровізація, штучний інтелект.*

The scientific publication is devoted to the study of topical issues of administrative and legal regulation of e-government under martial law.

It is noted that the full-scale war of the russian federation against Ukraine includes numerous cyberattacks, which poses a threat to information security and the normal functioning of the state and society as a whole.

© ОКСЮТЕНКО К.В. – кандидат юридичних наук, докторант (Інститут держави і права імені В.М. Корецького Національної академії наук України)

In these conditions, the issue of ensuring cybersecurity and information security in general becomes particularly relevant. It is noted that the most common objects of hostile cyberattacks are state registers, automated information and telecommunications systems, official pages of public administration bodies and the Unified Portal of Public Services «Diya», which together constitute the national mechanism of e-government.

The conclusion is formulated that under the legal regime of martial law, the issues of ensuring cybersecurity and national information security in general are one of the priority areas of state policy and require special attention from public administration bodies. In order to reliably protect all elements of the e-government mechanism, it is proposed to regulate the use of artificial intelligence technology in the field of cybersecurity. Artificial intelligence technology algorithms are able to effectively track spyware, as well as information that does not correspond to reality (fake messages, disinformation), counteract spam attacks by blocking external information resources and unwanted messages, track facts of unauthorized interference in the work of automated information and telecommunications systems, etc. In order to ensure the safety of national information resources, it is proposed to store them on several alternative servers, use cryptographic information protection tools and independence from the Internet (the ability to block access to them from the World Wide Web). In particular, it is desirable to store copies of state registers and information and telecommunication systems on several alternative and independent servers located both in Ukraine and in civilized foreign countries with which national public administration bodies have concluded relevant agreements on the provision of digital services.

Key words: *e-government, martial law, public administration bodies, legal regulation, information technologies, information security, cybersecurity, subjects of government authority, digitalization, artificial intelligence.*

Актуальність теми. Повномасштабна війна російської федерації проти України поставила перед національними органами публічної адміністрації велику кількість нових завдань, серед яких не останнє місце посідає питання забезпечення кібербезпеки та національної інформаційної безпеки в цілому. Сучасна війна включає в себе масштабні кібератаки на офіційні веб-ресурси органів публічної адміністрації, інформаційно-телекомунікаційні системи, державні реєстри, портали державних цифрових послуг, які в сукупності складають механізм електронного урядування.

Отже, завданням держави є правова регламентація розробки та впровадження в практичну діяльність реальних ефективних інструментів протидії кіберзагрозам та пошук оптимальних правових засобів забезпечення інформаційної безпеки.

Різні аспекти правового забезпечення електронного урядування завжди були в центрі уваги науковців. Із останніх наукових праць, пов'язаних із темою даної публікації слід виділити роботи Д. Біленької, М. Бабик, О. Берназюка, М. Віхляєва, О. Гунбіної, Т. Ковальової, О. Комарова, А. Краковської, Т. Коломоєць, Р. Мельника, А. Омельченка, Р. Стефанчука, В. Пилипчука, І. Тищенкової, В. Цимбалюка та інших науковців.

Окрему увагу дослідженню зарубіжного досвіду упровадження електронного урядування приділила С. Чукут.

Проте, питання адміністративно-правового регулювання електронного урядування в умовах дії правового режиму воєнного стану ще не були предметом окремого наукового дослідження, що актуалізує підготовку даної публікації.

Постановка завдання. Метою наукової публікації є дослідження актуальних питань адміністративно-правового регулювання електронного урядування в умовах дії правового режиму воєнного стану.

Методологія даної публікації включає філософські (методи діалектики та метафізики), загальнонаукові (прийоми логіки, системний та структурно-функціональний методи) та спеціально-юридичні методи дослідження (формально-юридичний метод, метод юридичного моделювання тощо). Також в процесі дослідження використовуються такі наукові підходи як інструментальний, цивілізаційний, антропоцентричний, телеологічний та синергетичний.

Результати дослідження. Війна, яка триває в Україні вже понад три роки, змусила переосмислити та змінити орієнтири в державній політиці. Наразі всі зусилля органів публічної адміністрації спрямовані на зміцнення обороноздатності та захист України від повномасштабної

збройної агресії російської федерації. Одним із ключових завдань є забезпечення кібербезпеки, тобто захист національних комп'ютерних, телекомунікаційних мереж, автоматизованих інформаційних систем від протиправного втручання, вірусних та спам-атак. Не менш важливим є забезпечення інформаційної безпеки, тобто забезпечення збереження та автентичності інформаційних ресурсів, протидія поширенню інформації, яка не відповідає дійсності тощо.

Зважаючи на актуальність вищевказаних питань, в науковому середовищі спостерігається тенденція щодо активізації наукових досліджень окремих аспектів забезпечення інформаційної безпеки в умовах дії правового режиму воєнного стану.

Так, питання інформаційної безпеки в умовах воєнного стану у аспекті забезпечення інформаційних прав і свобод дослідив І. Котерлін [1]. Роль інформаційних технологій та цифрових інструментів в умовах викликів війни та післявоєнного відновлення економіки України проаналізувала С. Боліла [2].

У відповідності до Закону України «Про правовий режим воєнного стану», воєнний стан – це особливий правовий режим, що вводиться в Україні або в окремих її місцевостях у разі збройної агресії чи загрози нападу, небезпеки державній незалежності України, її територіальній цілісності та передбачає надання відповідним органам державної влади, військовому командуванню, військовим адміністраціям та органам місцевого самоврядування повноважень, необхідних для відвернення загрози, відсічі збройної агресії та забезпечення національної безпеки, усунення загрози небезпеки державній незалежності України, її територіальній цілісності, а також тимчасове, зумовлене загрозою, обмеження конституційних прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень [3].

Таким чином, в умовах дії правового режиму воєнного стану органи публічної адміністрації мають більш широкі повноваження, що обумовлено необхідністю захисту національної безпеки, включаючи інформаційну безпеку та кібербезпеку, та нагальною потребою оборони країни від зовнішньої агресії.

Особливістю сучасної війни є активне використання інформаційних технологій, адже сучасне суспільство по праву називають інформаційним, а існуюча система органів публічного адміністрування має свій цифровий формат у вигляді електронного урядування.

Так, у відповідності до загальнодержавної Концепції розвитку електронного урядування в Україні, схваленій розпорядженням Кабінету Міністрів України від 20 вересня 2017 р. № 649-р., розвиток електронного урядування визначено одним з першочергових пріоритетів реформування системи державного управління. Також у рамках реалізації Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, Україна має забезпечити комплексний розвиток електронного урядування відповідно до європейських вимог [4].

Також у вказаній Концепції зазначено, що електронне урядування – це форма організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян [4].

Таким чином, електронне урядування є окремою сферою діяльності органів публічної адміністрації, яка потребує посиленого захисту в умовах дії правового режиму воєнного стану.

Крім того, інформаційні технології активно використовуються в Україні для ведення активної оборони та контрнаступальних операцій. Цьому сприяє цифровізація публічного управління у сфері оборони.

Так постановою Кабінету Міністрів України від 04 лютого 2023 р. № 139 «Деякі питання підвищення рівня цифровізації сил безпеки та сил оборони України у період воєнного стану» затверджено порядок використання системи військових продуктів DELTA [5]

Згідно із вказаною постановою Кабінет Міністрів України постановив погодитися з пропозицією Міністерства оборони та Міністерства цифрової трансформації щодо підвищення рівня цифровізації сил безпеки та сил оборони України у період воєнного стану для забезпечення їх оперативної сумісності з відповідними структурами держав – членів НАТО шляхом використання комплексу спеціалізованого програмного забезпечення «Інтеграційна платформа «Дельта» Збройних Сил України» з урахуванням того, що: сили безпеки та сили оборони України у разі потреби можуть використовувати комплекс «Дельта»; комплекс «Дельта» може розміщуватися на хмарних ресурсах та/або в центрах обробки даних, що розташовані на території держав – членів НАТО; комплекс «Дельта» забезпечує: інтеграцію різнотипних інформаційних (автоматизованих) систем для створення єдиного геоінформаційного та інформаційно-аналітичного середовища

органів військового управління, військових частин та підрозділів сектору безпеки та оборони України згідно із стандартами НАТО; інформаційну сумісність та взаємодію між різнотипними інформаційними (автоматизованими) системами, які використовуються силами безпеки та силами оборони України та/або розробляються в їх інтересах; ситуаційну обізнаність органів військового управління всіх рівнів у результаті використання інформаційних технологій, інтеграції сенсорів (датчиків) та систем з використанням стандартів НАТО [5].

Таким чином, цифровізація сил безпеки та сил оборони України у період воєнного стану передбачає цілий комплекс заходів, серед яких ключовим є використання комплексу спеціалізованого програмного забезпечення «Інтеграційна платформа «Дельта». Цей комплекс є унікальним цифровим продуктом, який забезпечує ведення бойових дій з інтеграцією різних інформаційних (автоматизованих) систем для створення єдиного геоінформаційного та інформаційно-аналітичного середовища органів військового управління, чим забезпечується оперативне реагування на пересування ворожих підрозділів та їх ефективне знищення.

Пунктом 2 вказаної постанови Кабінету Міністрів України від 04 лютого 2023 р. № 139 на Міністерство оборони України покладено обов'язки: забезпечити технічну можливість підключення до комплексу «Дельта» суб'єктів сил безпеки та сил оборони України, що виявили бажання використовувати комплекс «Дельта»; здійснити розміщення комплексу «Дельта» на хмарних ресурсах та/або в центрах обробки даних, що розташовані на території держав – членів НАТО; визначити порядок ведення та функціонування комплексу «Дельта»; забезпечити розробку на базі комплексу «Дельта» та введення в дослідну (тестову) експлуатацію інформаційно-комунікаційної системи «Інтеграційна платформа «Дельта» Збройних Сил України», визначити порядок її ведення та функціонування [5].

Таким чином, саме на Міністерство оборони України покладено обов'язок щодо нормативного врегулювання порядку ведення та функціонування інформаційно-комунікаційної системи «Інтеграційна платформа «Дельта» Збройних Сил України», проте допоміжну роль у цьому процесі повинно відігравати і Міністерство цифрової трансформації України, однією з функцій якого є координація діяльності інших органів публічної адміністрації у сфері цифровізації.

На окрему увагу заслуговує питання використання технології штучного інтелекту в процесі організації та здійснення електронного урядування в умовах дії правового режиму воєнного стану.

Так, в Україні розпорядженням КМУ від 2 грудня 2020 р. № 1556-р схвалено Концепцію розвитку штучного інтелекту в Україні. Як зазначено в самій Концепції розвитку штучного інтелекту в Україні, впровадження інформаційних технологій, частиною яких є технології штучного інтелекту, є невід'ємною складовою розвитку соціально-економічної, науково-технічної, оборонної, правової та іншої діяльності у сферах загальнодержавного значення [6].

Крім того, розпорядженням Кабінету Міністрів України від 9 травня 2025 р. № 457-р. затверджено План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025-2026 роки [7].

Вказаним Планом, серед іншого, передбачено:

- розроблення та подання Кабінетові Міністрів України законопроекту щодо правового врегулювання у сфері розвитку штучного інтелекту (відповідальне за виконання – Міністерство цифрової трансформації України);

- розроблення рекомендацій з кібербезпеки, які передбачатимуть пропозиції з використання технологій штучного інтелекту, зокрема щодо захисту моделей машинного навчання від несанкціонованого втручання в роботу (відповідальні за виконання – Мінцифри та Адміністрація Держспецзв'язку);

- проведення оцінки стану захищеності інформаційно-комунікаційних систем, які використовують штучний інтелект для виявлення та протидії кіберзагрозам (відповідальна за виконання – Адміністрація Держспецзв'язку);

- застосування технологій штучного інтелекту для проведення державними органами аналізу, прогнозування та моделювання розвитку системи державного управління у відповідних сферах, розрахунок показників ефективності (відповідальні за виконання – Мінцифри, Держстат, Мінекономіки, державна установа «Центр обробки статистичних даних», Секретаріат Кабінету Міністрів України);

- забезпечення використання технологій штучного інтелекту у сфері оборони (відповідальні за виконання – Міноборони, Апарат Ради національної безпеки і оборони України, Адміністрація Держспецзв'язку, Фонд розвитку інновацій) [7].

Таким чином, технологію штучного інтелекту планується активно використовувати у сфері електронного урядування, включаючи реалізацію державної політики у сфері захисту національної безпеки та оборони.

Технологія штучного інтелекту активно використовується в умовах дії правового режиму воєнного стану для виявлення шпигунських програм, несанкціонованого втручання в роботу інформаційно-комунікаційних систем, виявлення недостовірної інформації, яка поширюється в Інтернет російською пропагандою і завдає шкоди національним інтересам. Отже, алгоритми штучного інтелекту, які використовуються в процесі здійснення електронного урядування, є потужними інструментами ведення інформаційної війни, забезпечення інформаційної безпеки та кібербезпеки України.

Правовою основою діяльності органів публічної адміністрації у сфері кібербезпеки є Закон України «Про основні засади забезпечення кібербезпеки України», який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [8].

Згідно із ст. 8 вказаного закону національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури. Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України [8].

Кібербезпека в умовах дії правового режиму воєнного стану набуває особливої актуальності, адже об'єктом ворожих кібератак є майже всі елементи механізму електронного урядування: державні реєстри, офіційні веб-сторінки органів державної влади та місцевого самоврядування, портали надання цифрових адміністративних послуг, автоматизовані інформаційно-комунікаційні системи органів публічної адміністрації, поштові скриньки та сторінки в соціальних мережах суб'єктів владних повноважень тощо.

З метою забезпечення кібербезпеки Законом України «Про основні засади забезпечення кібербезпеки України» перебачено, у тому числі: функціонування Національної телекомунікаційної мережі (як сукупності спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань) та Національного центру резервування державних інформаційних ресурсів (як організованої сукупності об'єктів, створених з метою забезпечення надійності та безперебійності роботи державних інформаційних ресурсів, кіберзахисту, зберігання національних електронних інформаційних ресурсів, резервного копіювання інформації та відомостей національних електронних інформаційних ресурсів державних органів, військових формувань, утворених відповідно до законів, підприємств, установ та організацій) [8].

У зв'язку із продовженням систематичних ракетних атак з боку російської федерації доцільно нормативно врегулювати зберігання національних інформаційних ресурсів на окремих серверах в зарубіжних країнах, що убезпечить їх від знищення або пошкодження.

Згідно зі ст. 6 Закону України «Про основні засади забезпечення кібербезпеки України», розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО з обов'язковим залученням представників основних суб'єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій [8].

Крім того, в якості правової основи забезпечення інформаційної безпеки в механізмі електронного урядування слід відзначити Стратегією кібербезпеки України, затверджену Указом Президента України від 26 серпня 2021 року № 447, в якій зазначено, що питома вага кіберзагроз зростає і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Зростання такого впливу

на функціонування структур управління як національних, так і транснаціональних формує нову безпекову ситуацію [9].

В Стратегії кібербезпеки України підкреслюється, що в сучасному світі зростає технічний рівень реалізації кіберзагроз, постійно вдосконалюються та розробляються нові інструменти і механізми кібератак. Посилюється тенденція щодо використання кібератак як інструменту спеціальних інформаційних операцій, маніпулювання суспільною думкою. Глобального масштабу набуває використання кіберпростору терористичними організаціями. Пріоритетними цілями кібертероризму є об'єкти атомної енергетики, електро- та водопостачання, сфери електронних комунікацій, фінансової та банківської сфери, авіа- та залізничного транспорту, сховищ стратегічних видів сировини, хімічні й біологічні об'єкти тощо [9].

Наразі в Україні удосконалено нормативне забезпечення з питань кіберзахисту об'єктів критичної інформаційної інфраструктури, ухвалено порядок її визначення та загальні вимоги до її кіберзахисту. Утворено центри (підрозділи) забезпечення кібербезпеки або кіберзахисту в Державній службі спеціального зв'язку та захисту інформації України, Службі безпеки України, Національному банку України, Міністерстві інфраструктури України, Міністерстві оборони України, Збройних Силах України. З метою покращення координації діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, утворено робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки, рішення якого сприяють вирішенню найбільш складних проблем у цій сфері [9].

Таким чином, в умовах дії правового режиму воєнного стану механізм електронного урядування потребує особливого захисту з боку перелічених підрозділів органів публічної адміністрації, відповідальних за кіберзахист, чому має сприяти взаємодія національних інституцій з відповідними підрозділами зарубіжних країн. Одним із основних завдань Національного координаційного центру кібербезпеки має бути запозичення найкращих світових практик протидії кіберзагрозам.

Правовою основою електронного урядування в умовах дії правового режиму воєнного стану є також Стратегія інформаційної безпеки, затверджена Указом Президента України від 28 грудня 2021 року № 685/202, яка визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних [10].

У відповідності до вказаної Стратегії, забезпечення інформаційної безпеки України є однією з найважливіших функцій держави.

В Стратегії інформаційної безпеки наголошено на тому, що значне розширення джерел доступу до інформації в умовах стрімкого розвитку цифрових технологій та водночас недостатнього рівня медіаграмотності (медіакультури) супроводжується зменшенням критичності сприйняття інформації, створює підґрунтя для можливих маніпуляцій громадською думкою, що сприяє зростанню впливу дезінформації та деструктивної пропаганди. Некритичне сприйняття інформації створює загрози політичній та економічній стабільності демократичних держав [10].

Враховуючи вищезазначене, особливої уваги в умовах воєнного стану потребує правова регламентації протидії ворожим інформаційним ресурсам, блокування цифрових джерел інформації, які поширюють російську пропаганду та дезінформацію.

Так, за рішенням Ради національної безпеки і оборони України співробітникам органів публічної адміністрації та військовослужбовцям заборонили користуватися месенджером Telegram. РНБО зокрема було прийнято рішення щодо заборони встановлення та використання Telegram на службових пристроях (комп'ютерах) працівників органів державної влади, військовослужбовців, працівників сектору безпеки і оборони, а також підприємств – операторів критичної інфраструктури [11].

Крім того, відбулося засідання Національного координаційного центру кібербезпеки, який, як було зазначено вище, є ключовим органом координації та контролю у сфері кібербезпеки. У вказаному засіданні взяли участь представники керівного складу Державної служби спеціального зв'язку та захисту інформації України, Національної поліції України, Генерального штабу Збройних Сил України, Служби безпеки України, Міністерства оборони України, Національного банку України, Міністерства цифрової трансформації України, Міністерства закордонних справ України, розвідувальних органів, керівництво регуляторних органів у сфері електронних комунікацій, а також народні депутати України.

Представники Служби Безпеки України та Генерального Штабу ЗСУ зазначили, що Telegram активно використовується ворогом для кібератак, розповсюдження фішингу та

шкідливого програмного забезпечення, встановлення геолокації користувачів, корегування ракетних ударів тощо [11].

Крім того, загальновідомою є інформація про багаточисельні випадки вербування громадян України представниками спецслужб російської федерації для здійснення диверсій та терористичних актів, передачі інформації про переміщення сил та засобів ЗСУ. Тому доцільною є правова регламентація не тільки заборони використання Telegram посадовими особами органів публічної адміністрації, але й регламентація повного блокування даного месенджера на всій території України.

Отже, в Україні вже є позитивний приклад ефективної протидії небезпечним інформаційним ресурсам, які загрожують як нормальному функціонуванню механізму електронного урядування в Україні, так і посягають на загальний стан інформаційної безпеки, що особливо небезпечно в умовах воєнного стану.

Висновки. Проведене дослідження актуальних питань адміністративно-правового регулювання електронного урядування в умовах дії правового режиму воєнного стану дає підстави сформулювати висновок про те, що найчастіше об'єктом ворожих кібератак є державні реєстри, автоматизовані інформаційно-комунікаційні системи, офіційні веб-сторінки органів публічної адміністрації, електронні скриньки та сторінки у соціальних мережах суб'єктів владних повноважень, портали надання цифрових адміністративних послуг, які в сукупності складають національний механізм електронного урядування.

В умовах дії правового режиму воєнного стану питання забезпечення кібербезпеки та національної інформаційної безпеки в цілому є одними із пріоритетних напрямів державної політики та потребують особливої уваги органів публічної адміністрації. З метою надійного захисту всіх елементів механізму електронного урядування доцільно нормативно врегулювати питання використання технології штучного інтелекту у сфері забезпечення кібербезпеки. Алгоритми технології штучного інтелекту здатні ефективно відстежувати шпигунські програми, а також інформацію, яка не відповідає дійсності (фейкові повідомлення, дезінформацію), протидіяти спам-атакам шляхом блокування зовнішніх інформаційних ресурсів та небажаних повідомлень, відстежувати факти несанкціонованого втручання в роботу автоматизованих інформаційно-комунікаційних систем тощо.

З метою забезпечення збереження національних інформаційних ресурсів доцільно зберігати їх на декількох альтернативних серверах, використовувати засоби криптографічного захисту інформації та можливість блокування доступу до них зі всесвітньої мережі. Копії державних реєстрів та інформаційно-телекомунікаційних систем бажано зберігати на кількох альтернативних та незалежних один від одного серверах, які розташовані як в Україні, так і в цивілізованих зарубіжних країнах, з якими національними органами публічної адміністрації укладені відповідні договори про надання цифрових послуг.

Також, з метою забезпечення інформаційної безпеки в цілому та захисту механізму електронного урядування зокрема доцільно заблокувати на території України доступ до месенджера Telegram, який все більше використовується спецслужбами російської федерації для підривної діяльності та ведення інформаційної війни.

Перспективність подальшого дослідження даної тематики обумовлена необхідністю дослідження зарубіжного досвіду адміністративно-правового регулювання електронного урядування в умовах воєнного стану.

Список використаних джерел:

1. Котерлін І.Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав і свобод. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 1. С. 150–155.

2. Боліла С. Роль інформаційних технологій та цифрових інструментів в умовах викликів війни та післявоєнного відновлення економіки України. *Таврійський науковий вісник. Серія: Економіка.* 2023. № 16. С. 265–275. https://doi.org/10.32782/2708-0366/2023.16.35

3. Про правовий режим воєнного стану: Закон України від 12 травня 2015 р. № 389-VIII. Дата оновлення: 08.02.2025. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення: 10.02.2025).

4. Про схвалення Концепції розвитку електронного урядування в Україні: Розпорядження Кабінету Міністрів України від 20 вересня 2017 р. № 649-р. URL: https://www.kmu.gov.ua/npas/250287124 (дата звернення: 01.10.2024).

5. Деякі питання підвищення рівня цифровізації сил безпеки та сил оборони України у період воєнного стану: постанова Кабінету Міністрів України від 04 лютого 2023 р. № 139. URL: https://www.kmu.gov.ua/npas/deiaki-pytannia-pidvyshchennia-rivnia-tsyfrovizatsii-s-a139 (дата звернення: 02.07.2024).

6. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження КМУ від 2 грудня 2020 р. № 1556-р. Дата оновлення: 29.12.2021. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 01.06.2024).

7. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025-2026 роки: розпорядження Кабінету Міністрів України від 9 травня 2025 р. № 457-р. Дата оновлення: 09.05.2025. URL: https://zakon.rada.gov.ua/laws/show/457-2025-р#Text (дата звернення: 10.05.2025).

8. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. Дата оновлення: 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 02.11.2024).

9. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021. Дата оновлення: 28.08.2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12 (дата звернення: 02.11.2024).

10. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2021 р. № 685/2021. Дата оновлення: 30.12.2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 02.11.2024).

11. Працівникам державних органів та військовослужбовцям заборонили користуватися Telegram – РНБО. *Судово-юридична газета*. Публікації. 20.09.2024. URL: https://sud.ua/uk/news/publication/311056-rabotnikam-gosudarstvennykh-organov-i-voennosluzhaschim-zapretili-polzovatsya-telegram-snbo (дата звернення: 11.11.2024).