УДК 342.9.23:351.746
DOI https://doi.org/10.32782/ln.2024.23.18

Махмурова-Дишлюк О.П.
кандидат юридичних наук,
докторант
Науково-дослідний інститут публічного права

ЦИФРОВА БЕЗПЕКА ЯК ОДИН ІЗ ВАГОМИХ ЧИННИКІВ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ПРАВ, СВОБОД І ЗАКОННИХ ІНТЕРЕСІВ ГРОМАДЯН В УМОВАХ ВІЙН ТА ВОЄННИХ КОНФЛІКТІВ

Вступ. Цифрова безпека, як один із вагомих чинників адміністративно-правового забезпечення прав, свобод і законних інтересів громадян в умовах війн та воєнних конфліктів, набуває все більшого значення в сучасних умовах. Російсько-українська війна, викликає необхідність посилення захисту інформаційного простору та впровадження ефективних механізмів забезпечення цифрової безпеки. Це включає захист від кіберзагроз, запобігання використанню ворожих технологій для стеження, зломів та видалення контенту, а також боротьбу з дезінформацією та фейковими новинами.

Цифрова безпека відіграє ключову роль у захисті прав і свобод громадян, забезпеченні національної безпеки та стабільності. В умовах сучасних гібридних загроз важливим є використання безпечних технологій, регулярне оновлення систем захисту, шифрування конфіденційної інформації та моніторинг кіберзагроз.

Огляд останніх досліджень. До проблеми інформаційно-правового та адміністративно-правового забезпечення прав свободи людини і громадянина в умовах війни в Україні звертали свою увагу вітчизняні та зарубіжні вчені М. Алексійчук, Н. Армаш, В. Бібік, С. Бескоровайний, Ю. Бисага, Я. Букреєв, А. Вишневський, В. Галунько, І. Глобенко, П. Діхтієвський, Т. Доцюк, Я. Журавель, М. Доненко, І. Дзюба. В. Біла, В. Колпаков, Т. Короткий, М. Кравцова, О. Кузьменко, О. Куракін, С. Кучевська, В. Іванченко, О. Романова, В. Зьолка, О. Осауленко. С. Марущено, Д. Михайлов, І. Підберезних, О. Правоторова, Ю. Радковець, Є. Руденко, О. Савинець, Т. Сандерс, С. Сірий, О. Сікорський, Т. Тарахонич, А. Хамдо, Г. Христова на ін. Проте вони аналізовану нами проблематики безпосередньо не аналізували, а зосереджували свої наукові пошуки на більш загальних, спеціальних чи суміжних викликах.

Отже, запропонована тематики є вкрай актуальним як для вдосконалення національної правової системи, так і для зміцнення міжнародних зусиль у боротьбі з безкарністю за найтяжчі злочини, що загрожують миру та безпеці людства.

Мета статті полягає в тому щоб на основі теорії та норм інформаційного та адміністративного права розкрити місце і роль цифрової безпеки, як одного з чинників адміністративно-правового забезпечення прав, свобод і законних інтересів громадян в умовах війн та воєнних конфлікт.

Виклад основних положень. В системі адміністративно-правового забезпечення прав, свобод і законних інтересів громадян в умовах війн та воєнних конфлікт, яка здійснюється в інформаційному суспільстві в умовах використання гібридних засобів протистояння, цифровій безпеці належить провідне місце.

Перше, на що ми маємо звернути увагу та цифрову ідентифікація осіб, як одним із най-

важливіших способів виявлення, затримання та притягнення до кримінальної відповідальності осіб, які є винними у порушенні прав громадян, скоєнні воєнних злочинів та злочинні в проти людяності. Адже, суб'єкти скоєння цих злочинів, намагатимуться приховати свої порушення, надаючи недостовірну інформацію або фальшиві документи та свідчення. В Україні такі заходи отримали назву стабілізаційні заходи. Перевірка вимагає поглибленого дослідження та спілкування з місцевими правозахисними органами, фахівцями та дослідницькими центрами. Результати яких невідворотно переводяться в цифрову форму. Аналіз біографій та історії діяльності може виявити підказки, що ведуть до неповідомленої інформації, що може призвести до розслідувань, здатних створити підзвітність і вплив. Зокрема певну інформацію дають платформи соціальних мереж [1].

Основні засади стабілізаційних заходів включають комплексність та взаємопов'язаність, що передбачає сукупність узгоджених та взаємозв'язаних заходів, які проводяться військовими підрозділами у тісній взаємодії з органами Національної гвардії та Національної поліції. Усі ці дії здійснюються під єдиним керівництвом та за єдиним планом, що забезпечує координацію та ефективність виконання завдань. Завдання включають охорону та прикриття ділянок державного кордону, важливих об'єктів та комунікацій; недопущення нападів на військові бази; запобігання диверсіям та терористичним актам; охорону та супровід вантажів; надання допомоги населенню у ліквідації наслідків надзвичайних ситуацій. Надання допомоги населенню та підтримка громадського порядку є важливими компонентами стабілізаційних дій. Виконання режимних заходів та підтримка законності і правопорядку, що покладені на військове командування, що є невід'ємною частиною стабілізаційних заходів [2].

Отже, ідентифікація осіб та їх послідуюча інформації є важливим інструментом публічного адміністрування для забезпечення прав громадян в умовах російсько-української війни. Цей процес відіграє ключову роль у протидії російській агентурі та у виявленні осіб, причетних до злочинів, терористичних актів чи інших порушень. Стабілізаційні заходи, включаючи ідентифікацію та перевірку документів, спрямовані на виявлення недостовірної інформації та фальшивих документів, які можуть бути використані для хибних тверджень або приховання злочинів. Перевірка вимагає не лише технічної експертизи документів, але і глибокого аналізу біографій та історії діяльності осіб. Для ефективної ідентифікації та перевірки можуть бути використані наступні кроки: здійснення поглибленого аналізу спільно з місцевими правозахисними організаціями, які можуть надати додаткову інформацію та експертну допомогу. Взаємодія з експертами та дослідницькими центрами для обміну інформацією та отримання поглиблених аналітичних даних. Використання інформації з платформ соціальних мереж для аналізу зв'язків, здійснення моніторингу та виявлення можливих підказок. Сприяння розслідуванням, які можуть бути ініційовані громадськістю, для забезпечення підзвітності та виявлення порушень.

Про наступний напрямок цифрової безпеки мова йдеться тоді коли розслідуються факти росії обійти міжнародні санкції, які введенні щодо неї за нічим не спровоковану військову агресію щодо України. Першим кроком є пошук документів, які стосуються справжніх бенефіціарів. Ті, хто причетний до порушення санкцій, як правило, мають можливість приховати офіційні документи та дані та розробили методи, щоб захистити себе від відповідальності. Тому поряд з інформаційним пошуком рекомендується звернутися до людських джерел, щоб з'ясувати факти. Країни, на які поширюються міжнародні санкції, зазвичай уникають санкцій, використовуючи брокерів і підставні корпорації або засновуючи компанії зі штаб-квартирами в різних географічних районах, особливо в податкових гаванях. Потрібно шукати справжніх власни-

ків цих компаній і знаходити інформаційні сліди, щоб розслідувати факти порушень міжнародних санкцій державою агресоркою [3].

Отже, протидія обходу санкцій є важливою складовою публічного адміністрування при забезпеченні прав громадян в умовах російсько-української війни. Як свідчить світовий досвід для ефективного публічного адміністрування в цьому напрямку можна вжити кілька ключових заходів: Розвиток інформаційно-аналітичних систем, шляхом забезпечення доступу до різноманітних джерел інформації та використання аналітичних інструментів для виявлення та аналізу документів, що стосуються бенефіціарів.

По-третє, розвиток цифрових платформ та алгоритмів сприяти ефективному виявленню схем обходу санкцій. Міжнародне співробітництво, як взаємодія з іншими країнами та міжнародними організаціями для обміну інформацією та координації заходів. Спільні зусилля дозволяють краще виявляти та припиняти спроби обходу санкцій. Створення ефективних механізмів верифікації, як розробки та впровадження механізмів перевірки документів і власників компаній. Це може включати в себе створення баз даних та реєстрів, що легко доступні для публічності, а також регулярне оновлення цієї інформації. залучення громадянського суспільства, незалежних журналістів та громадських розслідувачів та активістів для моніторингу та розкриття випадків обходу санкцій. Так як громадськість може виконувати роль важливого контрольного механізму. Застосування безпосередньо правових інструментів для покарання тих, хто порушує санкції. Ефективна комунікація, забезпечення прозорості та активної комунікації з громадськістю, щоб збільшити свідомість про ситуацію, ризики обходу санкцій та здійснені заходи для їх запобігання [4].

По-четверте, електронне врядування з відкритим кодом може стати провідним інструментом публічного адміністрування. Це дозволяє створити «цифрову пам'ять» доказів про підтверджені порушення прав людини, спираючись на публічні джерела, такі як публічні публікації в соціальних мережах [5].

Міжнародний досвід свідчить, електронне врядування в умовах російсько-української війни може відігравати ключову роль у забезпеченні прав громадян при ефективному публічному адмініструванні. Зокрема, використання електронного врядування з відкритим кодом є потужним інструментом, який пропонує кілька важливих переваг. Відкритий код дозволяє створити транспарентну і доступну електронну інфраструктуру, де громадяни мають можливість легко отримувати і надавати інформацію. Це сприяє забезпеченню прозорості в урядових діях та полегшує доступ до важливих даних для громадян. Цифрова пам'ять та архівування доказів, як електронне врядування з відкритим кодом може створити «цифрову пам'ять», яка фіксує та архівує докази порушень прав людини. Це особливо актуально в умовах конфлікту, де зберігання достовірних даних є критично важливим для виявлення порушень та встановлення відповідальності. Використання публічних джерел, таких як соціальні мережі, для виявлення та моніторингу порушень прав може допомогти швидко реагувати на події та розповсюджувати інформацію. Електронне врядування створює можливість для активної участі громадян у процесах управління та контролю за владою. Відкритий код робить технологічні інструменти доступними для широкої аудиторії, сприяючи залученню громадян до вирішення суспільних проблем [6].

Цифрову безпеку шляхом недопущення використання російських технологій для потенційного відстеження, злому та видалення контенту. Щоб підвищити автентичність будь-яких записів або зображень і боротися з заявами про фейковими новинами російської пропаганди.

Висновки. Отже, цифрова безпеку як інструмент публічного адміністрування забезпечення прав громадян в умовах російсько-української війни полягає в недопущені

використання російських технологій для потенційного відстеження, злому та видалення контенту. Щоб підвищити автентичність будь-яких записів або зображень і боротися з заявами про фейковими новинами російської пропаганди.

Цифрова безпека відіграє важливу роль у публічному адмініструванні та забезпеченні прав громадян в умовах російсько-української війни. Запобігання використанню цифрових технологій російськими агресорами для потенційного відстеження, злому та видалення контенту є важливим аспектом цього підходу. Основні заходи в цьому контексті включають: використання безпечних технологій, уникання використання російських технологій та програмного. Вибір безпечних альтернатив та забезпечення їх регулярного оновлення є ключовим для запобігання потенційному відстеженню. Шифрування та захист конфіденційної інформації, шляхом застосування сучасних технологій шифрування для захисту конфіденційної інформації від несанкціонованого доступу. Це може включати шифрування електронної пошти, файлів та інших комунікаційних каналів.

Моніторинг та виявлення кіберзагроз, щодо запровадження систем моніторингу їх виявлення для швидкого реагування на потенційні атаки. Це включає в себе аналіз сумісних технологій, що дозволяє вчасно виявляти та ліквідовувати кіберзагрози. Розвиток та використання інструментів для перевірки автентичності контенту, коли йдеться розробка та впровадження технологій, які дозволяють перевіряти автентичність зображень, відео та інших медіафайлів.

Анотація

В статті розкрито наукові положення щодо цифрової безпеки, як одного з вагомих чинників адміністративно-правового забезпечення прав, свобод і законних інтересів громадян в умовах війн та воєнних конфліктів. Доведено, що цифрова безпека, як інструмент публічного адміністрування полягає в недопущені використання російських технологій для потенційного відстеження, злому та видалення контенту. З'ясовано, що ідентифікація осіб та їх послідуюча інформації є важливим інструментом публічного адміністрування для забезпечення прав громадян в умовах російсько-української війни. Цей процес відіграє ключову роль у протидії російській агентурі та у виявленні осіб, причетних до злочинів, терористичних актів чи інших порушень. Визначено, що протидія обходу санкцій є важливою складовою публічного адміністрування при забезпеченні прав громадян в умовах російсько-української війни. Запропоновано для підвищення автентичності будь-яких записів або зображень боротися з заявами та фейковими новинами російської пропаганди. З'ясовано, що цифрова безпека відіграє провідну роль у публічному адмініструванні та забезпеченні прав громадян в умовах російсько-української війни. Основні заходи в цьому контексті включають використання безпечних технологій, уникання використання російських технологій та програмного забезпечення. Вибір безпечних альтернатив та забезпечення їх регулярного оновлення є ключовим для запобігання потенційному відстеженню. Шифрування та захист конфіденційної інформації, шляхом застосування сучасних технологій шифрування для захисту конфіденційної інформації від несанкціонованого доступу. Це може включати шифрування електронної пошти, файлів та інших комунікаційних каналів. З'ясовано, що моніторинг та виявлення кіберзагроз включає в себе аналіз сумісних технологій, що дозволяє вчасно виявляти та ліквідовувати ці виклики.

Ключові слова: захист, ідентифікація осіб, інструмент публічного адміністрування, кіберзагрози, конфіденційна інформація, міжнародні санкції, моніторинг, несанкціонований доступ, російська агентура, російська пропаганда, терористичні акти, шифрування.

Makhmurova-Dyshliuk O.P. Digital security as one of the important factors of administrative law support for the rights, freedoms and legitimate interests of citizens in wars and military conflicts

Summary

The article reveals the scientific concepts of digital security as one of the significant factors in the administrative and legal provision of the rights, freedoms, and legitimate interests of citizens during wars and military conflicts. It has been proven that digital security, as a tool of public administration, involves preventing the use of Russian technologies for potential tracking, hacking, and content deletion. It has been established that the identification of individuals and their subsequent information is an important tool of public administration for ensuring the rights of citizens during the Russian-Ukrainian war. This process plays a key role in counteracting Russian espionage and identifying individuals involved in crimes, terrorist acts, or other violations. It is determined that counteracting the circumvention of sanctions is an important component of public administration in ensuring the rights of citizens during the Russian-Ukrainian war. It is proposed to increase the authenticity of any recordings or images to combat the claims and fake news of Russian propaganda. It has been established that digital security plays a leading role in public administration and ensuring the rights of citizens during the Russian-Ukrainian war. The main measures in this context include the use of secure technologies, avoiding the use of Russian technologies and software. The selection of safe alternatives and ensuring their regular updates is key to preventing potential tracking. Encryption and protection of confidential information, through the use of modern encryption technologies to protect confidential information from unauthorized access. This may include encrypting emails, files, and other communication channels. It has been established that monitoring and detecting cyber threats includes the analysis of compatible technologies, which allows timely identification and elimination of these challenges.

Key words: confidential information, cyber threats, encryption, identification of individuals, international sanctions, monitoring, protection, public administration tool, russian espionage, russian propaganda, terrorist acts, unauthorized access.

Список використаних джерел:

1. War crimes committed by Russia, Assad gov't in Syria. *ALJAZEERA.* 2022. URL: https://www.aljazeera.com/news/2020/5/11/war-crimes-committed-by-russia-assad-govt-in-syria-amnesty
2. Дії під час участі у спеціальній операції, стабілізаційних і специфічних діях військ та у спеціальний операції. *Харківський національний університет внутрішніх справ.* 2023. URL: https://univd.edu.ua/
3. Hamdo A. Lessons Learned from Syrian Journalists Investigating Russian War Crimes. *Global Investigative Journalism Network.* 2022. URL: https://gijn.org/resource/lessons-learned-from-syrian-journalists-investigating-russian-war-crimes/#:~:text=Lessons%20Learned%20from,April%206%2C%202022
4. Вплив глобалізаційних процесів та цифрової трансформації на формування міжнародного економічного клімату та фінансової екосистеми: збірник матеріалів Міжнародної науково-практичної інтернет-конференції (м. Полтава, 28 березня 2024 року). Полтава: *ПУЕТ,* 2024. 456 с.
5. Crimes. Global Investigative Journalism Network. *RESOURCE.* 2022. URL: https://gijn.org/resource/lessons-learned-from-syrian-journalists-investigating-russian-war-crimes/#:~:text=Lessons%20Learned%20from,April%206%2C%202022
6. Sanders T. In Ukraine and Syria, Civilians Pay for Russia's Crimes The horror unfolding now in Ukraine is both indiscriminate and illegal, but it is not unprecedented. *INKSTICK.* 2022. URL: https://inkstickmedia.com/in-ukraine-and-syria-civilians-pay-for-russias-crimes/