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. 2024. № 9.

DOI: http://doi.org/10.32702/2307-2156.2024.9.10

УДК 343.3

Я. Ю. Цимбаленко,

к. держ. упр., доцент, уповноважена особа з питань запобігання та виявлення корупції в КПІ ім. Ігоря Сікорського, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна

ORCID ID: https://orcid.org/0000-0002-2717-4321

С. А. Манзюк,

проректор з адміністративно-фінансової роботи,

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна

ORCID ID: https://orcid.org/0009-0003-7166-8198

ЧУТЛИВА ІНФОРМАЦІЯ ЯК ПРОГАЛИНА У СИСТЕМІ ІНФОРМАЦІЙНИХ ВІДНОСИН

Y. Tsymbalenko,

PhD in Public Administration, Associate Professor, Authorized Person for the Prevention and Detection of Corruption, in Igor Sikorsky Kyiv Polytechnic Institute,National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",Kyiv, Ukraine

S. Manziuk,

Vice-rector for administrative and financial work, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine

SENSITIVE INFORMATION AS A GAP IN THE SYSTEM OF INFORMATION RELATIONS

У статті проаналізовано інформаційні відносини та статус інформації, що має значення для збереження обороноздатності країни.

Зазначено, що введення у діловий обіг поняття «чутливої інформації» не відповідає чинному законодавству та потребує подальшого вдосконалення управлінських механізмів, що відповідають за інформаційну політику в Україні.

Визначено, що управління публічними закупівлями під час збройної агресії не враховує необхідності віднесення інформації до інформації з обмеженим доступом.

Визначено, що державні реєстри та бази даних потребують системного аналізу щодо інформаційної безпеки та протидії можливих розвідувальних заходів країни-агресора.

Доведено, що віднесення інформаційних потоків до вимог законодавства є позитивним кроком для формування стандартизованої системи управління ними.

The article examines the impact of the development of digital technologies on important elements of state functioning, in particular on public procurement. It was determined that digital technologies positively transformed the process of public procurement by shortening the period of their implementation, saving money and reducing corruption risks. It is noted that in the conditions of martial law, security has become a key factor for conducting procurements, and the issue of access and protection of information regarding the details of these procurements has become even more urgent at the level of state management.

Are analyzed the information relations and the status of information, which is important for maintaining the country's defense capability. Have been studied the prerequisites for the emergence of the concept of "sensitive information". It is noted that the introduction of this concept into business circulation does not correspond to the current legislation and requires further improvement of management mechanisms responsible for information policy in Ukraine. Are distinguished two methods for obtaining and analyzing information from open sources, namely: OSINT – searching for data using social networks, blogs, news, legal acts, etc.; SOCMINT (SMI) – intelligence of social networks, textual photo and video content.

Is analyzed Ukrainian legislation on information, access to public information, state secrets, features of conducting public procurement through electronic registers and under martial law. It was determined that the management of public procurement during armed aggression does not take into account the need to classify information as information with limited access.

It is noted that state registers and databases require a systematic analysis of information security and countermeasures against possible intelligence measures of the aggressor country in order to preserve national ideas and freedoms.

It has been proven that the attribution of information flows to the requirements of legislation is a positive step for the formation of a standardized system of their management.

Ключові слова: *управління, публічні закупівлі, чутлива інформація, інформація з обмеженим доступом, цифровізація, OSINT, SOCMINT.*

Keywords: *governance, public procurement, «sensitive information», information with restricted access, digitalization, OSINT, SOCMINT.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. У цій статті проаналізовано основні види інформації, увагу зосереджено на виникненні в діловому обігу публічних закупівель поняття «чутлива інформація».

Досліджено негативні наслідки розміщення чутливої інформації на онлайн-платформі публічних закупівель. Розглянуто проблему публікації інформації, що безпосередньо не може належати до інформації з обмеженим доступом, але в разі здійснення достатнього аналізу дає можливість зробити висновки щодо кінцевого об'єкта закупівлі.

Прозорість і доступність інформації є гарантією мінімізації корупційних ризиків та посадових зловживань, а також її негативним наслідком, що створює потенційні загрози для національної незалежності. Саме тому в статті розглянуто прогалини в системі інформаційного

забезпечення управління публічними закупівлями в умовах збройної агресії з боку рф.

Особливу увагу приділено питанням прозорості інформації з питань публічних закупівель та її використання під час практики збору інформації з відкритих джерел (OSINT) та соціальних мереж (SOCMINT) і їхній вплив на безпеку держави та її громадян.

Аналіз останніх досліджень і публікацій. Дослідженнями публічних закупівель, зокрема в цифрову епоху, займаються такі науковці: В. Марков, Н. Хорунжак, С. Герасимов, Д. Ізосімов, М. Галущак, А. Пантелеймоненко, А. Мілька.

Формулювання цілей статті (постановка завдання). Метою нашого дослідження є визначення прогалин у системі управління публічними закупівлями під час оприлюднення в електронній системі закупівель інформації, розголошення якої під час дії правового режиму воєнного стану в Україні може загрожувати національній безпеці та/або громадській безпеці.

Виклад основного матеріалу дослідження. У сучасному світі цифрові технології відіграють ключову роль у забезпеченні розвитку та стійкості держави. Пріоритетом цифрової трансформації нашої держави є її незалежність, адже з одного боку впровадження новітніх технологій дозволяє зміцнити економіку, підвищити ефективність державного управління та забезпечити національну безпеку, а з іншого – не контрольоване та стратегічно не продумане цифрове управління певними галузями публічного управління загрожує державній таємниці, обороноздатності й суверенітету країни.

Цифрова трансформація публічних закупівель є прогресивним етапом розвитку управління видатками Державного бюджету України.

Впровадження цифрових інструментів у публічні закупівлі значно змінило й продовжує змінювати традиційний підхід до організації цього процесу. Україна стала лідером з впровадження електронних систем

закупівель, і переваги такого підходу вже добре зарекомендували себе як на вітчизняному так і на міжнародному ринку. Використання цифрових інструментів забезпечує низку суттєвих переваг для всіх учасників процесу – від замовників до постачальників.

У першу чергу – це економія бюджетних коштів: зниження вартості адміністрування витрат на проведення процедур закупівель; можливість обрання дешевшої пропозиції та проведення аукціону зі зниження ціни.

Цифрові інструменти роблять процес участі в закупівлях більш доступним для всіх учасників ринку. Закупівельні платформи та уніфіковані правила участі в закупівлях спрощують цей процес, дозволяючи підприємствам брати участь у тендерах із мінімальними витратами часу й ресурсів.

Використання цифрових інструментів дозволяє значно скоротити час, необхідний для проведення закупівель. Автоматизація процесів, зокрема реєстрації учасників, подання пропозицій та проведення аукціонів, дозволяє швидше і ефективніше проводити та закінчувати закупівлі. Це особливо важливо в умовах, коли час є критичним фактором для реалізації державних проєктів.

Цифровізація закупівель забезпечує більшу прозорість процесу. Усі учасники мають рівний доступ до інформації про процедури закупівель, а всі етапи процесу документуються та можуть бути перевірені. Це знижує ризик корупційних дій та забезпечує чесну конкуренцію серед постачальників.

Гаслом цифрової платформи закупівель тривалий час було: «Усі бачать все». І це дійсно революційний крок до розбудови демократичного суспільства.

Впровадження цифрових систем закупівель стимулює розробку нових інструментів і технологій, що роблять процес закупівель ще більш ефективним. Використання аналітичних інструментів для аналізу даних про

закупівлі, розробка нових платформ для електронних аукціонів та інші інновації допомагають удосконалювати систему державних закупівель.

Так, цифрова трансформація є новітнім та корисним явищем у розвитку сучасного соціуму, але до нього треба готуватися та бути сприйнятливим до можливих викликів.

Недостатні інвестиції в кібербезпеку, прогалини в управлінні публічними закупівлями, брак стратегічного бачення наслідків інноваційного розвитку управління публічними закупівлями в умовах збройної агресії шкодить незалежності держави.

Протягом усього періоду існування цифрової платформи публічних закупівель у відкритому просторі знаходилась інформація про всіх замовників України, серед яких є органи державної влади і місцевого самоврядування, організації та установи публічного сектору й державні та комунальні підприємства.

Станом на сьогодні в Україні налічується приблизно 35 тисяч державних замовників. Вони є активними учасниками системи державних закупівель, через яку здійснюються різноманітні закупівлі для державних потреб [1].

Протягом повномасштабного вторгнення у кожного з державних замовників є потреба в швидкому реагуванні на постійні виклики та загрози. Безпека стала абсолютним пріоритетом, що обумовило кардинальні зміни в процесах державних закупівель. Повністю виведені з електронної системи Prozorro оборонні закупівлі, аби забезпечити оперативність і конфіденційність. Це рішення дозволило прискорити процеси та мінімізувати ризики, пов’язані з можливими витоками інформації.

У 2023 році обсяги закупівель, які були проведені через систему Prozorro, порівняно з минулим роком зросли втричі – до 480 млрд грн. Сьогодні, в умовах стабілізації ситуації, приблизно 80 % коштів знову витрачаються через систему Prozorro [2].

Відновлення закупівель незбройних оборонних засобів через систему Prozorro стало непростим завданням, яке супроводжувалося значними труднощами. Відродження довіри до електронної платформи вимагало від державних установ і підприємств проведення значної роботи. Основними проблемами стали забезпечення відповідного рівня захисту даних, удосконалення процедур закупівель, а також підвищення професійної компетентності спеціалістів, що беруть участь у закупівлях.

Ключовим чинником успішного повернення оборонних закупівель до Prozorro стало оновлення нормативно-правової бази. Уряду довелося впровадити нові регуляторні акти, що враховували специфіку оборонної галузі та водночас відповідали принципам прозорості й відповідальності. Крім того, велика увага приділялася моніторингу та контролю за закупівельними процесами, що забезпечило раціональне використання бюджетних коштів і запобігання можливим зловживанням. Важливим елементом було також використання сучасних технологій та аналітичних інструментів, що спростили процес оцінювання тендерів і контролювання за виконанням контрактів. Сьогодні Україна продовжує рухатися шляхом вдосконалення системи державних закупівель. Відновлення оборонних закупівель на Prozorro не лише підвищує ефективність використання коштів, але й сприяє зміцненню демократичних інститутів, забезпечуючи більшу прозорість та підзвітність влади. Це важливий крок у напрямі досягнення стабільності й розвитку країни в умовах постійних викликів та загроз.

Постановою Кабінету Міністрів України № 1275 від 11.11.2022 року «Деякі питання здійснення оборонних закупівель на період дії правового режиму воєнного стану» [3] внесено певні зміни до процесу публічних закупівель, що остаточно зобов’язали оборонних замовників використовувати електронну систему Prozorro для незбройних закупівель. Ці зміни спрямовані на підвищення прозорості та ефективності

використання державних коштів, а також на покращення процесу закупівель у сфері оборони.

Крім того, було запроваджено рамкову угоду для оборонних закупівель, яка спрямована на захист українських виробників від ризиків. Інформація про конкретних учасників, які змагаються за закупівлю, доступна лише контролюючим органам, що дозволяє мінімізувати ризики витоку конфіденційних даних. Також дані про переможця торгів є захищеними.

У суспільства є зрозумілий запит на прозорість державних закупівель, особливо в контексті оборони. Проте інформація про системних постачальників сил оборони України становить великий інтерес для ворога, який прагне зірвати забезпечення армії та отримувати інформацію про оборонну інфраструктуру.

Водночас кожен має доступ до інформації про ціни, за якими придбали товар, а також ціни, запропоновані іншими учасниками тендеру. Це забезпечує прозорість процесу закупівель та дозволяє громадськості контролювати використання державних коштів, а також мінімізувати корупційні ризики.

В умовах збройної агресії теза про публічний доступ до інформації про закупівлі набула нового значення у контексті забезпечення оборони держави та її незалежності. Забезпечення прозорості діяльності організацій та підприємств, зокрема публічного сектору, покликано мінімізувати корупційні ризики у їх роботі та підвищити відкритість діяльності публічних інституцій, але водночас впливає на доступність для аналітики розвідувальних органів країни-агресора. В умовах сучасних гібридних воєн ці ризики мають підвищену небезпечність.

Пошук і виявлення прихованих дій та рішень, розкриття таємниць, відслідковування джерел, перевірка отриманої інформації, а також доступ до інформації, яка має обмежений доступ, – усе це належить до сфери діяльності, яка називається збором даних з відкритих джерел [4] (соціальні

мережі, блоги, дискусійні групи, нормативно-правові акти, інформація з теле- та радіопередач, новини, комунікаційні онлайн-платформи тощо) – OSINT. Така практика не є прерогативою спеціальних агентів, а є загальнодоступною та долучитися до неї може кожен.

Інший тип розвідки на основі відкритих джерел – це SOCMINT (SMI) [5], або розвідка соціальних мереж. Простір спілкування розширюється і звичайною дією є розміщення персональної інформації (текстовий, фото- та відеоконтент) про себе в соціальних мережах, зокрема про свою професію, місце роботи, друзів, хобі тощо. Така інформація формує не лише власний профіль у соціальних мережах, а також створює інформаційне поле для використання його з метою дослідження та розвідки. Наші дії в цифровому просторі залишають цифровий відбиток – метадані, які можуть бути використані агентами розвідки для наповнення своїх даних. SOCMINT (SMI) використовується переважно в урядовому секторі для забезпечення інтересів безпеки держави, забезпечення функціонування правоохоронних органів, а також для отримання безцінних розвідувальних даних із відкритих джерел.

У сучасних умовах глобальної цифровізації питання захисту інформації, зокрема конференційної, набувають особливого значення. Правове регулювання цих відносин є необхідною умовою для забезпечення національної безпеки, економічної стабільності та захисту прав і свобод громадян.

Згідно зі статтею 20 Закону України «Про інформацію» [6], інформація за порядком доступу поділяється на відкриту інформацію та інформацію з обмеженим доступом, а статтею 1 цього закону визначено, що інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

Законодавство України чітко регламентує порядок віднесення інформації до категорій таємної або службової. Порядок віднесення інформації до таємної або службової регулюється законами України, які встановлюють критерії для віднесення інформації до цих категорій.

Зокрема, Законом України «Про державну таємницю» визначено, що державна таємниця – це різновид таємної інформації, яка охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національним інтересам України [7].

Водночас службова інформація включає відомості, які є власністю держави, але не належать до державної таємниці.

Відносини, пов’язані з правовим режимом конфіденційної інформації, регулюються законами України, які визначають основні принципи, порядок віднесення інформації до категорії конфіденційної, а також порядок доступу до такої інформації.

Це здійснюється відповідно до законів України «Про інформацію», «Про доступ до публічної інформації» та інших нормативно-правових актів. Так, Закон України «Про інформацію» визначає поняття конфіденційної інформації –конфіденційною вважається інформація, доступ до якої обмежено законом або власником інформації, і яка не підлягає розголошенню без згоди відповідних суб’єктів [6].

Доступ до інформації регулюється також спеціальними законами та нормативно-правовими актами, які визначають порядок надання доступу до такої інформації. Наприклад, Закон України «Про доступ до публічної інформації» встановлює порядок надання доступу до інформації, яка знаходиться у розпорядженні органів державної влади, органів місцевого самоврядування та інших суб’єктів публічного права [8]. У цьому законі визначено процедури запиту інформації, терміни її надання та підстави для відмови у наданні інформації.

Так, правовий режим конфіденційної інформації в Україні базується на системі законодавчих актів, які забезпечують регулювання порядку віднесення інформації до цієї категорій, а також визначають порядок доступу до інформації. Ці закони спрямовані на забезпечення балансу між

відкритістю та прозорістю діяльності державних органів і захистом національних інтересів, прав і свобод громадян.

Закон України «Про здійснення публічних закупівель» визначає обов'язок замовників (перелік замовників передбачено статтею 2 Закону України «Про здійснення публічних закупівель») оприлюднювати інформацію про здійснення публічних закупівель, крім тих, що здійснюються в межах оборонного замовлення [9]. Тобто інформація, що супроводжує процедури закупівель, є відкритою та доступною.

Інформація, яка підлягає оприлюдненню під час проведення процедури закупівлі це, зокрема, але не виключно, місцезнаходження замовника та учасника, місце знаходження об'єкта будівництва або реконструкції, місце постачання товарів, опис предмету закупівлі (назва, номенклатура, обсяг), інформація про виконання учасником аналогічних договорів, наявність в учасника матеріально-технічної бази.

Ця безпечна інформація в умовах збройної агресії є ефективною базою інформації при реалізації SOCMINT (SMI) та OSINT з метою створення інтерактивної оборонної карти України ворожими агентами.

Проблему, що пов'язана з можливостями ворожих країн консолідувати інформацію у розвідувальних цілях, розглядало Міністерство економіки України та Prozorro [10].

У зв'язку з невизначеністю статусу інформації, що може нанести шкоду національній безпеці та обороні країни, у діловому обігу управління публічними закупівлями почав використовуватися термін – «чутлива інформація» [11].

Станом на сьогодні Постанова Кабінету Міністрів України № 1275 від 11.11.2022 року «Деякі питання здійснення оборонних закупівель на період дії правового режиму воєнного стану» [3] дає дозвіл замовникам приховувати інформацію про власне місцезнаходження та місцезнаходження об'єкту будівництва або ремонту, а також конкретне місце постачання товарів.

Під час проведення відкритих торгів зі специфічними умовами замовник має право не розкривати деталі щодо місця постачання товару на рівні населеного пункту. Це допускається відповідно до пункту 27 Постанови Кабінету Міністрів України № 1178 від 12.10.2022 року: «Якщо оприлюднення в електронній системі закупівель інформації про місце постачання (оприлюднення якої передбачено законом) може загрожувати безпеці замовника, то ця інформація може бути вказана лише як найменування населеного пункту, до якого здійснюється доставка товару (де виконуються роботи або надаються послуги)» [12].

Проте, на нашу думку, це було недостатнім кроком для вирішення проблеми використання відкритої інформації ворогом, адже цей дозвіл порушує вимоги статті 21 Закону України «Про інформацію» (абзац 2, частина 2) [6], а саме: відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом, а не постановою уряду.

Автори проаналізували нормативно-правову базу, зокрема закони України «Про інформацію», «Про публічні закупівлі», «Про основи національного супротиву», «Про доступ до публічної інформації» та зробили висновок, що інформація, яка стосується замовників, діяльність яких не стосується системи управління сил оборони України, а також інформація, за допомогою якої можна зробити висновок щодо пов'язаних з обороною заходів, не належить до інформації з обмеженим доступом, а тому повинна бути опублікована в повному обсязі на загальних підставах.

Станом на сьогодні та відповідно до пункту 9^1 «Порядку функціонування електронної системи закупівель та проведення авторизації електронних майданчиків» (далі – порядок), затвердженому постановою Кабінету Міністрів України від 24.02.2016 року № 166 (Офіційний вісник України: 2016 рік, № 22, стаття 855; 2019 рік, № 66, стаття 2258, № 90, стаття 3000): «У разі оприлюднення в електронній системі закупівель інформації з обмеженим доступом або інформації, розголошення якої під час дії правового режиму воєнного стану в Україні може нести загрозу

національній безпеці та/або громадській безпеці і порядку, за зверненням замовника, що оприлюднив таку інформацію в електронній системі закупівель, адміністратор вчиняє дії в електронній системі закупівель з припинення публічного доступу до такої інформації на підставі рішення комісії про надання адміністраторові дозволу на припинення публічного доступу до інформації з обмеженим доступом або інформації, розголошення якої під час дії правового режиму воєнного стану в Україні може загрожувати національній безпеці та/або громадській безпеці і порядку» [13].

Комісія щодо розгляду питань діяльності електронної системи закупівель (далі – комісія) – постійно чинна комісія, що утворюється Уповноваженим органом з метою розгляду питань діяльності електронних майданчиків, авторизованих електронних майданчиків в електронній системі закупівель та інших питань.

Відповідно до наказу Міністерства розвитку економіки, торгівлі та сільського господарства України «Про затвердження Положення про комісію щодо розгляду питань діяльності електронної системи закупівель» (далі – положення) № 381 від 14.11.2019 року члени комісії беруть участь у її роботі на громадських засадах і на безоплатній основі [14]. Засідання комісії є відкритими. Відкритість засідання комісії забезпечується шляхом вільного доступу осіб, які бажають узяти в ньому участь, без права виступу та голосу на засіданнях комісії. Особи, присутні на засіданні комісії, можуть використовувати засоби фото-, відео- та звукозапису. Засідання комісії можуть проводитися в режимі відеоконференції з використанням інформаційно-комунікаційних технологій.

Для забезпечення захисту національної безпеки та з метою захисту інформації про закупівлі, що не має статусу конфіденційної або таємної у розумінні Закону України «Про інформацію» та Закону України «Про доступ до публічної інформації», але з метою приховування інформації, що має значення для оборони країни, уповноважена особа з питань здійснення

закупівель приймає рішення про звернення до комісії з метою отримання дозволу приховування такої інформації з публічного доступу.

Відповідно до пункту 24 порядку, питання щодо приховування чутливої інформації розглядаються протягом 10 робочих днів, з дня звернення замовника після публікації такої інформації у відкритому доступі, на відкритому засіданні комісії (Рис. 1) [14].

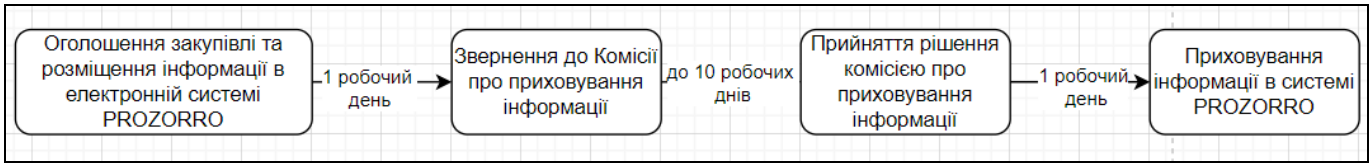

Рис. 1. Максимальний строк прийняття рішення про приховування чутливої інформації

Джерело: сформовано на основі [14].

Приховування цієї інформації в системі адміністратор здійснює відповідно до рішення комісії. Результати розгляду є підставою для прийняття рішення Міністерства економіки України та надання системі Prozorro дозволу на закриття інформації. Міністерство економіки України з урахуванням протоколу засідання комісії приймає рішення відповідно до порядку, яке затверджується наказом Міністерства економіки України та розміщується на офіційному вебсайті міністерства протягом двох робочих днів з дня його прийняття.

Так, можна зробити висновок, що управлінські рішення щодо здійснення захисту чутливої інформації мають суттєві недоліки, а саме:

1. Розміщуються замовником у публічному доступі у системі Prozorro.

2. Замовник позбавлений права самостійно приймати рішення про закриття інформації.

3. Немає алгоритму визначення інформації як «чутливої».

4. Замовник звертається до комісії про приховування інформації після розміщення її у публічному доступі.

5. Комісія є громадським органом, що виконує обов’язки на добровільних засадах.

6. Члени комісії не можуть бути притягнуті до відповідальності за свої рішення.

7. Комісія протягом 10 робочих днів приймає рішення щодо задоволення або відмови в задоволенні клопотання замовника про приховування інформації.

8. Інформація про прийняте рішення комісією розміщується в публічному доступі на сайті Міністерства економіки України.

На 863 день збройної агресії рф (05.07.2024 року) Кабінет Міністрів України вніс зміни до Постанови № 1178 від 12.10.2022 року [13], доповнивши пункт 13 новим абзацом, відповідно до якого визначено перелік закупівель, інформація про які не має статусу інформації з обмеженим доступом, але не підлягає до публічного опублікування.

За таких умов, можна зробити висновок, що Кабінет Міністрів України через перелік закупівель товарів, робіт та послуг, необхідних для забезпечення будівництва військових інженерно-технічних і фортифікаційних споруд, виконання мобілізаційних завдань (замовлень), заходів, пов’язаних із підготовкою і виконанням завдань територіальної оборони, виконання договорів, що містять інформацію з обмеженим доступом, якщо така закупівля здійснюється для нагальних потреб Збройних Сил України, інших військових формувань, правоохоронних органів, ДСНС, вищих військових навчальних закладів на їх запит з подальшим переданням таких товарів, робіт та послуг на облік запитувача визначив інформацію, що має «чутливий» характер.

На погляд авторів, інформація, що вдало може бути використана у SOCMINT (SMI) та OSINT, залишає цифровий слід у вигляді метаданих та є «чутливою», повинна бути прирівняна до конфіденційної інформації у розумінні Закону України «Про інформацію».

Така фабула повністю відповідає чинному законодавству, робить процес оперування інформацією зрозумілим та таким, що захищає національну безпеку та оборону.

Автори статті на прикладі публичних закупівель продемонстрували результат недосконалої системи управління інформаційними відносинами. Станом на сьогодні в Україні існує більше ніж 56 відкритих реєстрів та баз даних, що містить інформацію, яка може бути використана ворогом, а тому потребує негайних дій уряду задля захисту національних ідей і свобод.

Висновки та перспективи подальших розвідок у даному напрямі. Подальшим напрямом розвитку дослідження інформаційної безпеки України повинен стати пошук та аналіз чутливої інформації у відкритих реєстрах та базах даних з метою віднесення інформації, що має «чутливий» характер та може бути використана з розвідувальними цілями, до інформації з обмеженим доступом.

Приклад можливості виокремлення чутливої інформації про публічні закупівлі та віднесення її до правового поля – є позитивним, але дуже повільним кроком для захисту українського інформаційного простору.

Віднесення чутливої інформації до інформації з обмеженим доступом є необхідним з погляду управління інформаційними потоками, оскільки дозволяє сформувати єдиний для всіх видів інформації стандарт роботи.

Література

1. Кулик Л. Відкриті реєстри та бази даних України. URL: https://infobox.prozorro.org/articles/perelik-vidkritih-reyestriv-ta-baz-danihukrajini (дата звернення: 12.08.2024).

2. «Підсумки публічних закупівель: У 2023 році обсяги закупівель зросли утричі – до 480 млрд грн». URL: https://www.kmu.gov.ua/news/pidsumky-publichnykh-zakupivel-u-2023-rotsi-obsiahy-zakupivel-zrosly-utrychi-do-480-mlrd-hrn (дата звернення: 12.08.2024).

3. «Деякі питання здійснення оборонних закупівель на період дії правового режиму воєнного стану» : Постанова Кабінету Міністрів України від 11.11.2022 р. № 1275. URL: https://zakononline.com.ua/documents/show/510216___771095 (дата звернення: 12.08.2024).

4. Розвідка з відкритих джерел (Open-source intelligence - OSINT). URL: https://www.maxzosim.com/rozvidka-z-vidkritikh-dzherel-osint/ (дата звернення: 12.08.2024).

5. Everything About Social Media Intelligence (SOCMINT) and Investigations. URL: https://www.maltego.com/blog/everything-about-social-media-intelligence-socmint-and-investigations/ (дата звернення: 12.08.2024).

6. «Про інформацію» : Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 12.08.2024).

7. «Про державну таємницю» : Закон України від 21.01.1994 р. № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 12.08.2024).

8. «Про доступ до публічної інформації» : Закон України від 13.01.2011 р. № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 12.08.2024).

9. «Про публічні закупівлі» : Закон України від 25.12.2015 р. № 922-VIII. URL: https://zakon.rada.gov.ua/laws/show/922-19#Text (дата звернення: 12.08.2024).

10. Литвинчук І. Щодо приховування інформації у закупівлях. URL: https://infobox.prozorro.org/articles/shchodo-prihovuvannya-informaciji-u-zakupivlyah (дата звернення: 12.08.2024).

11. Prozorro TV. (2024, 22 травня). *Захист чутливої інформації під час воєнного стану* [Відео]. YouTube. URL: https://www.youtube.com/watch?v=m7PNQB2Z3lY (дата звернення: 12.08.2024).

12. «Про затвердження особливостей здійснення публічних закупівель товарів, робіт і послуг для замовників, передбачених Законом України “Про публічні закупівлі”, на період дії правового режиму воєнного стану в Україні та протягом 90 днів з дня його припинення або скасування» : Постанова Кабінету Міністрів від 12.10.2022 р. № 1178. URL: https://zakon.rada.gov.ua/laws/show/1178-2022-%D0%BF#Text (дата звернення: 12.08.2024).

13. «Про затвердження Порядку функціонування електронної системи закупівель та проведення авторизації електронних майданчиків» :

Постанова Кабінету Міністрів від 24.02.2016 р. № 166. URL: https://zakon.rada.gov.ua/laws/show/166-2016-%D0%BF#Text (дата звернення: 12.08.2024).

14. «Про затвердження Положення про комісію щодо розгляду питань діяльності електронної системи закупівель» : Постанова Кабінету Міністрів від 14.11.2019 р. № 381. URL: https://zakon.rada.gov.ua/laws/show/z1223-19#Text (дата звернення: 12.08.2024).

References

1. Kulyk, L. (2019), "Open registers and databases of Ukraine", available at: https://infobox.prozorro.org/articles/perelik-vidkritih-reyestriv-ta-baz-danih-ukrajini (Accessed 12 August 2024).

2. Government portal (2023), "Results of public procurement: In 2023, the volume of procurement tripled to UAH 480 billion", available at: https://www.kmu.gov.ua/news/ pidsumky-publichnykh-zakupivel-u-2023-rotsi-obsiahy-zakupivel-zrosly-utrychi-do-480-mlrd-hrn (Accessed 12 August 2024).

3. Cabinet of Ministers of Ukraine (2022), Resolution "Some issues of defense procurement during the period of the legal regime of martial law", available at: https://zakononline.com.ua/documents/show/510216___771095 (Accessed 12 August 2024).

4. Maxym, Z. (2023), "Intelligence from open sources (Open-source intelligence - OSINT)", available at: https://www.maxzosim.com/rozvidka-z-vidkritikh-dzherel-osint/ (Accessed 12 August 2024).

5. Maltego Team (2024), "Everything About Social Media Intelligence (SOCMINT) and Investigations", available at: https://www.maltego.com/blog/everything-about-social-media-intelligence-socmint-and-investigations/ (Accessed 12 August 2024).

6. The Verkhovna Rada of Ukraine (1992), The Law of Ukraine "About information", available at: https://zakon.rada.gov.ua/laws/show/2657-12#Text (Accessed 12 August 2024).

7. The Verkhovna Rada of Ukraine (1994), The Law of Ukraine "About state secrets", available at: https://zakon.rada.gov.ua/laws/show/3855-12#Text (Accessed 12 August 2024).

8. The Verkhovna Rada of Ukraine (2011), The Law of Ukraine “About access to public information”, available at: https://zakon.rada.gov.ua/laws/show/2939-17#Text (Accessed 12 August 2024).

9. The Verkhovna Rada of Ukraine (2015), The Law of Ukraine “About public procurement”, available at: https://zakon.rada.gov.ua/laws/show/922-19#Text (Accessed 12 August 2024).

10. Lytvynchuk, I. (2022), “Regarding concealment of information in purchases”, available at: https://infobox.prozorro.org/articles/shchodo-prihovuvannya-informaciji-u-zakupivlyah (Accessed 12 August 2024).

11. Prozorro TV (2024), “Protecting sensitive information during martial law”, [Video], YouTube, available at: https://www.youtube.com/watch?v=m7PNQB2Z3lY (Accessed 12 August 2024).

12. Cabinet of Ministers of Ukraine (2022), Resolution “On approval of the specifics of public procurement of goods, works and services for customers provided for by the Law of Ukraine "On Public Procurement" for the period of the legal regime of martial law in Ukraine and within 90 days from the date of its termination or cancellation”, available at: https://zakon.rada.gov.ua/laws/show/1178-2022-%D0%BF#Text (Accessed 12 August 2024).

13. Cabinet of Ministers of Ukraine (2016), Resolution “On the approval of the Procedure for the functioning of the electronic procurement system and the authorization of electronic platforms”, available at: https://zakon.rada.gov.ua/laws/show/166-2016-%D0%BF#Text (Accessed 12 August 2024).

14. Cabinet of Ministers of Ukraine (2019), Resolution “On the approval of the Regulation on the commission regarding the consideration of issues of the electronic procurement system”, available at: https://zakon.rada.gov.ua/laws/show/z1223-19#Text (Accessed 12 August 2024).

Стаття надійшла до редакції 10.09.2024 р.