
ЕКОЛОГІЧНИЙ МОНІТОРИНГ

УДК 004.56.5

DOI <https://doi.org/10.32846/2306-9716/2023.eco.1-46.4>

ЗАХИСТ НАЦІОНАЛЬНИХ ГЕОПРОСТОРОВИХ ЕКОЛОГІЧНИХ ДАНИХ УКРАЇНИ ПІД ЧАС ВОЄННОГО СТАНУ ТА ПОВОЄННОГО УСТРОЮ

Шевченко Р.Ю.

Державна екологічна академія післядипломної освіти та управління
вул. Митрополита Василя Липківського, 35, корп. 2, 03035, м. Київ
azimut90@ukr.net

Розглянуті підходи та механізми захисту даних відкритих та корпоративних картографічних сервісів інтернету екологічного та природоохоронного тематичного змісту з урахуванням специфіки геопросторових екологічних даних, їх побудови, функціонування та зберігання під час активних фаз бойових дій російсько-української війни. Окреслені проблемні питання безпеки тематичних банків екологічних даних відкритих геоінформаційних систем України, що функціонують у відкритих (краудсорсингових) картографічних сервісах інтернету, демонструючи всю повноту еколого-географічної, топографічної та аерокосмічної інформації про Україну. Це, зокрема, геопортали : Google Map, Google Earth, OpenStreetMap, WikiMapia, Panoramio, Mapillary.

Висвітлені питання забезпечення безпеки геоданих, як тематичних шарів у картографічних сервісах інтернету, що є науковою новизною та своєрідним поштовхом до подальших наукових розробок в галузі екологічної геоінформатики та безпеки формування баз даних під час здійснення геоінформаційного еколого-природоохоронного картографування території України.

Розроблена методика забезпечення захисту національних геопросторових екологічних даних України в умовах воєнного стану та повоєнного устрою. Математичний апарат та методику визначення коефіцієнтів безпечності геоданих необхідно розглядати як інструкцію із забезпечення безпеки інтернет-картографування стратегічних галузей господарства України, оцінку їх впливу на довкілля та для потреб стратегічного екологічного проектування. Описується апробація методики аналізу безпеки тематичних баз даних екологічних геопорталів за допомогою систем забезпечення кібербезпеки.

Розглянуті питання стратегії захисту геоінформаційних баз даних відкритих та закритих корпоративних геопорталів із врахуванням специфіки способів використання даних користувачами. Відображено впроваджений мандатний принцип доступу до геоінформаційних систем управління екологічних баз даних України, що дозволяє підвищувати ступінь захищеності геоінформаційних картографічних сервісів (геопорталів) екологічного тематичного спрямування. *Ключові слова:* екологічні геопросторові дані, кібербезпека екологічної інформації, інфраструктура геопросторових даних, захист інформації, геоінформація, сигнатури екологічних баз.

**Protection of the National Geospatial Environmental Data of Ukraine during the martial status and the post-war regime.
Shevchenko R.Y.**

The purpose of the research presented in the article is to consider the approaches and mechanisms of data protection of open and corporate online cartographic services of environmental and nature protection thematic content, taking into account the specifics of geospatial environmental data, their construction, functioning and storage during the active phases of the Russian-Ukrainian war. Special technical attention and emphasis was placed on the security of the thematic banks of environmental data of open geoinformation systems of Ukraine, which function in open (crowdsourced) mapping services of the Internet, which have not stopped demonstrating all the completeness of ecological-geographical, topographical and aerospace information about Ukraine. This means geoportals: Google Map, Google Earth, OpenStreetMap, WikiMapia, Panoramio, Mapillary.

A special place in the content of the publication is the issue of ensuring the safety of geodata as thematic layers in Internet mapping services. This is a scientific novelty and has progressive interest in further scientific developments in the field of environmental geoinformatics and security of database formation in geoinformational environmental and environmental protection mapping of the territory of Ukraine.

The methodology for ensuring the protection of National Geospatial Ecological Data of Ukraine during the martial law and post-war regime was developed. The mathematical apparatus and methodology for determining geodata safety factors should be considered as instructions for ensuring the safety of online mapping of strategic branches of the economy of Ukraine, assessing their impact on the environment, and for the needs of strategic environmental design. Approbation of the methodology of security analysis of the thematic databases of ecological geoportals with the help of cyber security systems is described.

Issues of the strategy of protection of geoinformation databases of open and closed corporate geoportals are considered, taking into account the specifics of how users use data. The mandated principle of access to geoinformation management systems of environmental databases of Ukraine was developed and implemented, which allows to increase the security class of geoinformation cartographic services (geoportals) with ecological thematic content. *Key words:* ecological geospatial data, cybersecurity of ecological information, geospatial data infrastructure, information protection, geoinformation, signatures of ecological databases.

Постановка проблеми. Воєнний стан в Україні змінив певною мірою ставлення до безпеки національної інфраструктури геопросторових даних. Запровадження та реалізація системи захисту екологічної геоінформації напряму пов'язано із національною системою безпеки та оборони України, яка напряму має відношення до розвитку геоінформаційних технологій. Бойові дії та екоцид природно-заповідного фонду України стали наслідком формування нової концепції формулювання інноваційних програм захисту інформації національного значення. Зміна парадигми ставлення до безпеки геопросторових даних природоохоронної тематики стало імпульсом до розв'язання наукових проблем в галузі кібербезпеки національних геоданих.

Актуальність дослідження. В основу захисту екологічних геоданих апіорі покладається твердження про постійну готовність національної інфраструктури геопросторових даних до запобігання загроз та кібератак щодо хмарних геоінформаційних систем (геопорталів). У будь-який час система координування об'єктів ПЗФ України має відбивати загрози DoS-атак, патогенної активності програм-шпигунів із викрадення баз даних відкритих та корпоративних геоінформаційних систем. Цьому сприятимуть інноваційні розробки та реалізація необхідних програмних заходів із захисту, дотримання безпеки системам управління баз геопросторових даних (СУБД), зосередження зусиль із запобігання знищення найбільш цінної державної геоінформації щодо стану довкілля. В сукупності це визначає актуальні напрямки із розробки технічних вимог щодо захисту національних геопросторових екологічних даних України під час активних фаз бойових дій на території України (надзвичайної ситуації воєнного характеру).

Зв'язок авторського доробку із важливими науковими та практичними завданнями. Державна екологічна академія післядипломної освіти та управління є відповідальним адміністратором Національного геопорталу природно-заповідного фонду України. Важливий напрямок підтримки функціонування картографічного сервісу інтернету – захист екологічних баз даних та застосування хмарних технологій захисту геопросторової інформації природоохоронного змісту.

Аналіз останніх досліджень та публікацій. Проблема захисту екологічних геопросторових даних України постала із лютого 2022 р., не розв'язання котрої є новітньою інформаційною кіберг-загрозою для національної екологічної безпеки України. Апіорі, екологічні та природоохоронні геопросторові дані є відкритими до громадянського суспільства, вітчизняних еколого-просвітницьких та міжнародних волонтерських організацій із моніторингу та захисту довкілля. До недавнього часу взагалі не поставало питання секретності екологічної геоінформації в Україні. Тому спеціальних проблемних нау-

кових публікацій вишукано не було, окрім [4; 5; 6]. Бібліографічні матеріали присутні лише в галузі захисту інформації комерційного та корпоративного спрямування, безпеки баз даних фінансового сектору держави, оборонних галузей знань [7; 8; 9].

Виділення не вирішених раніше частин загальної проблеми, котрим присвячена означена стаття. Метою дослідження є розробка теоретико-методичних основ технології підвищення безпеки та захисту геоінтелектуальних ресурсів України під час війни у відповідності до чинного законодавства [1; 2; 3]. Їх швидка розробка та застосування є першочерговим завданням при попередженні несанкціонованого доступу, блокування, псування, знищення, розповсюдження, копіювання, фальсифікування противником картографічних доказів проведеного екоциду щодо довкілля України. За допомогою використання комплексу спеціалізованих програмних опцій буде забезпечено дотримання збереження екологічної геоінформації та обмеження (шлюзування) доступу до національних баз даних про довкілля, об'єкти рекреаційної мережі держави, обсягів завданої шкоди навколишньому природному середовищу України. Це все буде необхідно для комплексної оцінки впливу на довкілля внаслідок російсько-української війни, підготовки картографічних матеріалів та документів-доказів у міжнародному екологічному трибуналі.

Новизна. Зазначена необхідність захисту національної інфраструктури екологічних баз даних. Кожний оператор геоінформації в Україні зобов'язаний забезпечити захист просторових баз даних від хакерських атак за допомогою комплексу розроблених технологічних заходів та прийомів з дотримання, збереження екологічної інформації, а також обмеження доступу до загальнодоступної екологічної інформації під час війни.

Методологічне або загальнонаукове значення. Розроблення вимог щодо безпеки та захисту інфраструктури екологічних геоданих у відкритих геопорталах Google Map, Google Earth, OpenStreetMap, WikiMapia, Panoramio, Mapillary досягається рішеннями запровадження технології координатної затримки точності локалізації об'єктів місцевості, тобто методами, які покладені в адміністрування будь-якого хмарного геоінформаційного сервісу. Це матиме наслідки у визначенні координатних значень для віддалених (незаконних) користувачів геопорталів. Досягається відповідний результат засобами трансформації операційної системи функцією нового регламентування баз даних геоінформаційних серверів зі зміною прав аудиту-доступу до спеціалізованих тематичних банків даних екологічної інформації.

Виклад основного матеріалу. Незважаючи на військові дії в Україні, повноцінно функціонують значна кількість картографічних сервісів, які надають різноформатну геопросторову інформацію про територію України. Це несе загрозу національній

небезпеці та обороні України. Навіть в радянські часи картографічна інформація була жорстко засекречена. Навіть туристичні довідники були оснащені примітивними схемами, особливо при демонстрації території великих міст. Відповідні вимоги не діяли понад тридцять років, що призвело до непоправних наслідків для держави. Це потребує негайних організаційних та технічних заходів для захисту національної геопросторової екологічної інформації.

Технічні аспекти організації безпеки та захисту національної інфраструктури геоданих класифікуються за мірилом просторових даних, які відкрито демонструються в мережі інтернет із тематичним навантаженням екологічного та природоохоронного змісту, призначенням інтернет-карт в залежності від функціонального застосування тематичних шарів геопорталу та особливостями розподілу архітектурних сегментів (сигнатур) геопросторових даних.

Під час воєнного стану в Україні відкриті геоінформаційні портали демонструють всю територію країни або відображаються картографічні моделі за складовими адміністративно-територіального устрою у відповідності до атласу адміністративної реформи [4]. Тобто масштаби геопросторових даних мають загальнонаціональний, регіональний (крайовий), локальний (місцевий) та об'єктовий сегмент.

Регіональні геопортали мають функціональні особливості, які полягають в тому, що еколого-природоохоронна інформація одного картографічного регіонального сервісу буде дублювати географічні бази даних прилеглих громад суміжних областей (країв) України або установ та підвідомчих організацій. Наприклад місто-ексклав Славутич або смт. Коцюбинське Бучанської громади Київської області.

Переважна більшість еколого-природоохоронних геопорталів мають об'єктове мірило. Це плани та карти територіальної організації національних природних парків, заповідників, заказників, експериментальних екологічних полігонів тощо. Але вони функціонують в рамках однієї, наприклад, природно-географічної, кліматичної або рекреаційно-охоронної зони, такої, як, Смарагдова мережа України.

Для забезпечення геоінформаційного захисту геопросторової екологічної інформації рекомендуються наступні першочергові заходи під час активних бойових дій. Це формулювання текстових та графічних вимог до захисту екоінформації з розробки програмних засобів забезпечення безпеки тематичних баз даних відкритого або корпоративного геопорталу. Поетапна їх розробка та впровадження здійснюються з метою захисту екоінформації в ході експлуатації експериментального картографічного ресурсу об'єкту ПЗФ України (www.gis.dea.edu.ua).

Відповідні технічні вимоги вміщують інформацію про значення геопросторової екоінформації та відповідність кадастру національної системи охорони навколишнього природного середовища; документування та реєстрація унікальності та ексклю-

зивності природного об'єкту, його класифікаційні ознаки в системі екологічного туризму та рекреації. Також надається аналіз потенційних загроз безпеки самій програмі захисту геоданих на базі актуальних сигнатур хмарної системи безпеки картографічного сервісу інтернету.

Запроваджені заходи мають стати запобіжником несанкціонованого доступу (викрадення), навмисного псування, видалення, фальсифікування, компіляції, незаконного розповсюдження геоінформації державної екологічної таємниці України. Відповідний модуль повинен також мати аварійну функцію самознищення геоданих при хакерських атаках конфіденційного спрямування, пов'язаних із зазначенням кількісних та якісних показників систем природокористування та біоресурсів України. Шлюзи потоків кібератак повинні автоматично блокуватися на етапі проходження сигналу обміну геоданих у хмарному сервісі геопорталу.

Зазначені технічні засоби забезпечення безпеки екоданих обираються програмістами-геоінформатиками та реалізуються в модулях картографічних сервісів інтернету з прикладною метою захисту самої програмної оболонки геопорталу з урахуванням імовірних загроз безпеці тематичним банкам даних за усіма об'єктами та суб'єктами природоохоронної справи України на апаратному (геоінформаційному), прикладному (картографічному) та мережевому (краудсорсингові, корпоративні та інституціональні топографічні дані) рівнях. Це також має відношення до опцій геовіртуалізації географічної інформації та хмарних обчислювань картометричних опцій геопорталів.

Необхідно окреслити жорсткі умови (вимоги) до забезпечення захисту екологічної інформації природоохоронних установ та організації, які знаходяться в зоні тимчасової окупації. Це насамперед повна заборона доступу до просторової екоінформації (вимкнення геосерверу або його аварійне транспортування до установ державної безпеки України на зберігання). Визначення геолокації за VPN-сервісом та IP-кодом центрів хакерських спроб несанкціонованого доступу (злому) до національної екологічної інформації. Попередження негативних наслідків у разі не конфіденційного доступу до екологічної інформації шляхом припинення передачі даних спеціальними технічними засобами обробки геопросторових сигнатур в мережі інтернет. Відновлення порушеного функціонування тематичних баз даних, яка була знищена в процесі не санкціонованого доступу. Паралельно необхідно здійснювати контроль над рівнями захисту екологічної геоінформації, її перекодування із застосуванням трансферного брандмауера.

Розглянемо детально методи, засоби та прийоми забезпечення кібербезпеки екологічної геопросторової інформації України (рис. 1).

Показники захищеності національної інфраструктури геопросторових екологічних даних України характеризуються функцією захисних



Рис. 1. Система забезпечення кібербезпеки та захисту екологічних геоданих України

модулів, які впливають на фільтрування потоків даних та описуються технічними вимогами до рівнів інформаційної безпеки відкритих баз даних. Пропонується встановити та запровадити в систему інтернет-картографування п'ять класів кібербезпеки геоданих, які визначають спеціалізовані рівні безпеки екологічних банків даних різної тематики. Клас безпеки визначається в залежності від тематичного призначення карти, мірилом геоінформаційної моделі та державним значенням відповідної геоінформації в системі національної безпеки та оборони України. Відповідне відношення можна представити у вигляді формули:

$$L_{(i)} = l * m, \quad (1)$$

де $L_{(i)}$ – ступінь безпеки геоданих, l – рівень державного значення геоінформації, m – мірило картографічної моделі у геопорталі.

Ступінь безпеки геоданих визначається кількісним показником потенційної шкоди державі або користувачу екогеоінформації, або замовнику/оператору геоданих від втрати відповідних баз даних чи порушення геоінформаційної (незаконний доступ, копіювання змістовної частини баз банків, фальсифікація та розповсюдження з метою дискредитації тощо). Відповідний ступінь визначає рівень цілісності збереженої або пошкодженої геоінформації, ранжир зношеності банку даних, геомодифікації координатних систем та обсяг шлюзування відкритої доступності до змісту екологічної інформації у просторовій прив'язці. Математично це виглядає наступним виразом:

$$L_{(i)+N} = (I_{(k)} + L_{(i)}) * \{(I_{(c)} + I_{(i)}) + \{(I_{(d)} + I_{(ts)})\}, \quad (2)$$

де $L_{(i)+N}$ – статус (державне значення) екологічної бази даних геоінформації, $I_{(k)}$ – коефіцієнт індикативності (конфіденційності) геоінформації, $L_{(i)}$ – ступінь шкоди державі за методикою центру сертифікації геоінформації, $I_{(c)}$ – показник цілісності банку екологічних даних, $I_{(i)}$ – ступінь актуалізації геоінформації, якою можна знехтувати, $I_{(d)}$ – індекс доступності (відкритості) картографічного сервісу інтернету, $I_{(ts)}$ – ступінь навмисної фальсифікації геоінформації (застосовується при надзвичайній ситуації воєнного характеру).

Статус (державне значення) екологічної бази даних геоінформації визначається Держгеокадастром, Мінзахистдовкілля та СБУ на Раді національної безпеки та оборони України [1]. Водночас визначається ступінь потенційної шкоди державі від втрати відповідного банку даних. Це визначається експертними методами та має ряд наступних класифікаційних ознак.

Найвищий рівень небезпеки інфраструктури геопросторових екологічних даних України – червоний рівень. Застосовується в разі порушення одного із вище викладених властивостей безпеки картографічних баз. Це насамперед: конфіденційність, стійкість (цілісність) та закритість (недоступність). Внаслідок поширення відповідного рівня до масштабів області або усієї території України є потенційна імовірність негативних подій у державному управлінні у сфері екологічної та техногенної безпеки держави, викликання соціально-політичної, геополітичної, фінансово-економічної кризи. В цей час оператори та адміністратори геопорталів критичної інфраструктури та провідних установ природоохоронної справи не зможуть виконувати покладені на них державною функції.

Загрозливий рівень небезпеки інфраструктури геопросторових екологічних даних України – жовто-гарячий рівень. Запроваджується із урахуванням вище зазначених факторів червоного рівня з одним виключенням, що стосується підтримки контролю Держгеокадастром конфіденційності (незламності) просторового (координатного) каркасу тематичних банків даних картографічних сервісів України.

Потенційно небезпечний рівень небезпеки інфраструктури геопросторових екологічних даних України – жовтий рівень. Запроваджується при фік-

суванні DoS-атак та координатної локалізації спецслужбами України центрів порушення конфіденційності корпоративних або державних геопорталів.

Висновки. Під час оперативного моніторингу безпеки баз даних національних екологічних геопорталів постійно визначається рівень значимості змістовної частини банків даних та частка державної таємниці геопросторової інформації. Це може бути військова таємниця, економічні секретні дані, матеріали природно-техногенної безпеки тощо. Ці відповідні параметри визначаються окремо по кожному із стратегічних складових національної безпеки та оборони за визначеним алгоритмом. Підсумковий коефіцієнт безпеки зберігання екологічної інформації оброблюється за вищевикладеними формулами і встановлюється за критично допустимими показниками ступенів потенційної шкоди, завданої навколишньому природному середовищу, що визначаються параметрами кон-

фіденційності, цілісності та недоступності національної інфраструктури геопросторових екологічних даних ворожим розвідувальним службам.

Перспективи використання результатів дослідження. Методика захисту просторової геоінформації під час воєнного стану та повоєнного устрою може бути апробована для розробки стратегії подальшого (повоєнного) захисту персональних, мережових та інтернет-картографічних моделей наукових установ та організацій України.

Методика захисту геоданих, отриманих слідчими діями при розслідуванні злочинів екоциду буде затребувана для відповідального зберігання мультимасштабних еколого-природоохоронних ревізійно-аналітичних (аудиторських) геоінформаційних карт зруйнованих промислових майданчиків об'єктів критичної інфраструктури та постраждалих природоохоронних (рекреаційних) територій України, які зазнали втрат внаслідок російсько-української війни.

Література

1. Закон України «Про національну інфраструктуру геопросторових даних» від 23.12.1998 р. № 353-XIV.
2. Закон України «Про топографо-геодезичну і картографічну діяльність» від 23.12.1998 р. № 353-XIV.
3. Постанова Кабінету Міністрів України «Порядок функціонування національної інфраструктури геопросторових даних» від 26.05.2021 р. № 532.
4. Карпінський Ю.О., Лященко А.А. Стратегія формування національної інфраструктури геопросторових даних в Україні. К. : НДІГК. 2022. 106 с.
5. Карпінський Ю. О., Лященко А. А., Макаренко Д. Г. Розвиток інфраструктури геопросторових даних: стан, тенденції та проблеми. XXV Міжнародна науково-технічна конференція «Геофорум-2020», 1–3 квітня 2020 року, Львів. С. 160–163.
6. Руденко Л. Г., Чабанюк В. С., Бондар А. Л. та ін. Концепція багатоцільової національної ГІС України : матеріали науково-практичного семінару з геоінформаційних систем, 22–25 листопада 1993 р., Вінниця – Київ, С. 4–33.
7. Cetl V., Nunes de Lima V., Tomas R., Lutz, J., D'Eugenio M., Nagy A., Robbrecht J. Summary Report on Status of implementation of the INSPIRE Directive in EU, EUR 28930 EN, Publications Office of the European Union, Luxembourg.
8. Gómez P.M., García M.P., Seco G.G., Santiago A.R., Johnson C.T. The Americas' Spatial Data Infrastructure. ISPRS Int. J. Geo-Inf., 8 (10), p. 432.
9. Crompvoets J., Vancauwenberghe G., Ho S., Masser I., Timo de Vries W. Governance of national spatial data infrastructures in Europe. IJSDIR, Vol. 13, pp. 253–285.