УДК 346.24: 656.073

ТРАНСПОРТНА СИСТЕМА ЯК ОБ'ЄКТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В РЕАЛІЯХ ТЕХНОСФЕРИ ВИСОКОУРБАНІЗОВАНОЇ ТЕРИТОРІЇ

TRANSPORT SYSTEM AS A CRITICAL INFRASTRUCTURE OBJECT IN THE REALITIES OF THE TECHNOSPHERE OF A HIGHLY URBANIZED TERRITORY

канд. фіз.-мат. наук Ю.С. Тарасенко
Університет митної справи та фінансів (м. Дніпро)

Cand. of Phys. and Math. Sc. Y.S. Tarasenko
University of Customs and Finance (Dnipro)

Тенденція сучасного суспільства полягає в об'єднанні і проживанні у високо урбанізованих районах, про що свідчать дані ООН, що викликано значним зростанням міського населення по відношенню до сільського. Зокрема, згідно з рейтингом країн за рівнем урбанізації (Urbanization Index), Україна посідає 73 місце (з 195 країн) у світі за останніми результатами дослідження щодо частки міського населення, представленого по відношенню до загального населення країни (станом на 04.10.2023 рік) 69,5 % населення міста [1]. Як правило, техносфера таких територій, до якої входять різні інженерні споруди, в тому числі транспортна система, що поєднує в собі громадський транспорт, промисловий залізничний транспорт, відомчий транспорт, трубопровідний транспорт і громадський зв'язок (дороги, мости, дамби, водосховища і т.д.) [2], за своїм значенням в національній безпеці держави відноситься до сфери кібербезпеки, тоді як озвучені транспортні об'єкти є критичною інфраструктурою (ОКІ) [3,4].

На жаль, все більших оборотів набуває тенденція несумлінного протиборства новітніх технологій (в тому числі геоінформаційних систем - ГІС), які навіть доходять до кібершпигунства, кіберзлочинності та кібертероризму з використанням не тільки інформаційної зброї, які спрямовані на злом існуючих ОКІ. При цьому сенс їх безпеки полягає в неможливості нанесення шкоди штатному функціонуванню та властивостей цих об'єктів або їх структурним складовим [5]. На державному (і не тільки) рівні вимушені створювати системи безпеки и кібербезпеки ОКІ. Цілеспрямовані дії останніх пов'язані з кіберзахистом - сукупністю «організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем» [6]. Безсумнівно, спектр безпеки інформаційних аспектів у вигляді доступності, цілісності і

конфіденційності інформації повністю залежить від прогресу використовуваних систем і технологій (зокрема й геоінформаційних), їх соціальної складової та ймовірного характеру можливих впливів (охоплюючи й фізичні прояви різноманітних ризиків) на об’єкт дослідження [7].

Згідно [8], сучасні геоінформаційні технології (Geographic Information Technologies, ГІТ) – це сукупність методів і прийомів збору та обробки географічної (просторової) інформації у сучасній цифровій формі з виділенням трьох складових **– *технології ГІС*** ***(Geographic Information Technologies),*** що реалізує технологія введення, інтеграції, зберігання, обробки, аналізу, моделювання та візуалізації географічної інформації; - технології дистанційного зондування Землі (Retote Sensipg - RS) з метою отримання інформації про поверхню Землі та об’єктів реального світу (середовища) за допомогою авіаційного та космічного моніторінгу; - технології позиціонування *(Global Positioning System, GPS),* що реалізує технології визначення місця розташування об’єктів на Землі різними засобами глобальних навігаційних систем та сучасних оптоелектронних геодезичних вимірів.

Особливий інтерес представляє розвиток інтелектуальних транспортних систем (ІТС). Необхідною (але не достатньою) умовою успішного і безумовно довгострокової реалізації ІТС є розробка не тільки методів штучного інтелекту та їх практичної реалізації, а й надійних (безвідмовних) платформ щодо розташування руху, взаємного положення та стану рухомих об'єктів. На даний момент стало цілком зрозуміло, що без космічного моніторингу Землі, сучасних комп'ютерних засобів та їх програмного забезпечення (сервісу) неможливо розробити методи штучного інтелекту, як в транспортній системі, так і ГІС. Не виключено, що саме через швидке розширення використання ГІТ відстає єдина (насамперед європейська) стандартизація за умов представлення цифрової картографії в ГІС, сфері використання яких постійно розширюється [9].

З існуючих вітчизняних та міжнародних стандартів слід відзначити ГОСТ 28441-99 «Цифрова картографія. Терміни та визначення» з датою введення 2000-07-01 [10], яка повинна використовуватися спільно з ГОСТ 15971, ГОСТ 21667 ГОСТ 26387. Крім того, (мабуть, перш за все, через гриф «засекречено») обмежена (щодо використання) схемотехнічна реалізація первинних джерел геоінформації, наприклад від об’єктів критичної інфраструктури, здійснюється у вигляді оптико-радіолокаційних систем або пристроїв. Таким чином ГІС – це не тільки сучасні комп'ютерні технології для картографування й аналізу об'єктів реального світу, подій і явищ, що відбуваються та будуть відбуватись у прогнозованому періоді. ГІС - це інформаційна система, яка забезпечує збір, збереження, обробку, доступ, відображення та поширення геопросторових даних, першоджерела яких – це дані, які отримане кіберфізичними та радіотехнічними системами.

Саме останнім (передусім радіолокаційним) належать, добре схемотехнічно та законодавчо (з позицій єдиних стандартів), реалізовані достовірні методи та способи отримання так званої радіолокаційної інформації у вигляді здійснення етапів виявлення, дозволу, вимірювання та розпізнавання [11,12]. За аналогією з такими прототипами отримання інформації багатомільйонна індустрія ГІТ, що

використовується практично у всіх сферах людської діяльності, здатна також бути реалізованою у вигляді технологічного ланцюжка сукупності оптико-радіолокаційних методів та програмно-апаратних засобів, що забезпечують отримання, обробку, розповсюдження та архівування просторової інформації. З метою її безпеки, підвищення надійності та оперативності слід до геоінформаційних об'єктів, у тому числі і з техносфери високоурбанізованих територій, відноситись як до об'єктів критичної інфраструктури. У такому ракурсі, з одного боку, доцільно використовувати методологію побудови пізнавальної моделі безпеки ОКІ [13], включаючи як підвищення їхнього рівня безпеки [14], так і зниження супутніх ризиків [7]. З іншого боку, нескладно експериментально оцінити рівень достовірності технології та похибок (невизначеності) проведених (супутніх) вимірювань [15-17], виходячи з парадигми їх істинності відповідно до сучасних рекомендацій ISO/IEC Guide 98-1:2009, реалізуючи методики вимірювань ефективної поверхні простих, але каліброваних об'єктів, наприклад у вигляді сфери або сукупності кутових відбивачів [11].

[1] Рейтинг стран мира по уровню урбанизации /Гуманитарный портал: Исследования [Электронный ресурс] // Центр гуманитарных технологий, 2006–2023 (последняя редакция: 04.10.2023). URL: https://gtmarket.ru/ratings/urbanization-index.
[2] Крячко К.В., Кулешов В.В., Берестова Т.Т. Взаимодействие видов транспорта Конспект лекций. – Харьков: УкрДАЗТ, 2010. – Ч. 1. – 100 с.
[3] Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"».
[4] Закона Украины Про критичну інфраструктуру № 1882-IX від 16.11.2021р. *Голос України.* 2021. 14 груд. (№ 236).
[5] Тарасенко Ю.С., Соляніков В.Г., Бруй І.І. Кібербезпека: інформаційні аспекти захисту від технологій впливу. Матеріали міжнародної науково-практичної інтернет-конференції «Інноваційні рішення в економіці, бізнесі, суспільних комунікаціях та міжнародних відносинах» Секц. «Спрямування розвитку сучасних інноваційних технологій у сфері комп'ютерних наук та кібербезпеки» Дніпро 16 квітня 2021 р. С. 424-426.].
[6] Закон України «Про основні засади забезпечення кібербезпеки України». Документ 2163-VIII (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403), чинний, редакція від 15.12.2021.
[7] Тарасенко Ю. С., Савченко Ю.В. Ризик-орієнтовані процеси забезпечення безпеки об'єктів критичної інфраструктури. Системи та технології, 65 (1). С. 66-76.
[8] В.І.Зацерковний, В.Г.Бурачек, О.О.Железняк, А.О.Терещенко Геоінформаційні системи і бази даних: монографія. – Ніжин: НДУ ім. М.Гоголя, 2014. – 492 с.
[9] В.П.Савиных. Геоинформатика в системе наук. - Образовательные ресурсы и технологии. •2016'3 (15) с.106-113.
[10] Межгосударственный стандарт Digital cartography. Terms and definitions ГОСТ 28441-99 «Картография цифровая. Термины и определения». МКС 01.040.35. ОКСТУ 0090. Дата введения 2000-07-01.
[11] Тарасенко. Ю.С. Фізічні основи радіолокації [Текст]: навч. Посіб. Т 19. – Д.: «Пороги», 2011. – 487с.
[12] Теоретические и физические основы радиолокации и специального мониторинга : учебник / А. Н. Фомин, В. Н. Тяпкин, Д. Д. Дмитриев [и др.] ; под общ. ред. И. Н. Ищука. – Красноярск : Сиб. федер. ун-т, 2016. – 292 с.
[13] В.Ю.Клим. Ю.С.Тарасенко, The methodology of building the cognitive model of critical infrastructure's security. Pp. 38-51. Prospektive globale wissenschaftliche trends. Monographic series «European Science». Book 11. Part 1. Published by: *ScientificWorld-NetAkhatAV*. Karlsruhe, Germany 2022.
[14] Safety of critical infrastructure objects from the positions of risk effectiveness reduction Yu.S. Tarasenko, V.Iu. Klym. Vol. 4 No. 141 (2022): System technologies, Published: 2023-03-04, p.158-168.
[15] ISO/IEC Guide 98-1:2009, Uncertainty of measurement - Part 1: Introduction to the expression of uncertainty in measurement, IDT. Неопределенность измерения. Часть 1. Введение в руководства по выражению неопределенности измерения. Стандартинформ. 2017.
[16] ISO/IEC 98-3, Uncertainty of measurement — Guide to the expression of uncertainty in measurement (GUM:1995) Руководство ISO/МЕК 98-3 Неопределенность измерений — Часть 3: Руководство по выражению неопределенности измерений (GUM:1995).