ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ «SMART CITY» (РОЗУМНОГО МІСТА) В КОНТЕКСТІ РЕФОРМУВАННЯ БЕЗПЕКОВОГО СЕГМЕНТУ ДЕРЖАВИ

Діордіца Ігор Володимирович,

д.ю.н., професор,

професор кафедри приватного та публічного права,

Київський національний університет технологій та дизайну

м. Київ, Україна

На наше переконання основною передумовою невироблення чітких критеріїв концепції «Smart City» при формуванні стратегій розвитку регіонів чи територіальних громад в Україні є некоректне усвідомлення її сутності.

Архітектоніка розумного міста може включати такі елементи:

1. Розумне/електронне урядування: «розумна рада громади» створює цінність для сталого суспільного продукту, використовуючи інтеграцію ІКТ для планування, управління та операцій на одному рівні або між ними.

2. Розумна охорона здоров'я: розумна охорона здоров'я – це служба охорони здоров'я, яка використовує такі технології, як Інтернет речей (переносні сучасні медичні засоби) і мобільний Інтернет, для динамічного доступу до інформації, з'єднуючи людей, медичні заклади та установи [1].

3. Розумна енергетика: традиційна інфраструктура енергетичної мережі не відповідає зростаючим потребам громад. Розумна енергетична мережа, оснащена технологіями ІС, може підтримувати двосторонній зв'язок і електричні струми між різними об'єктами в мережі. Розумна мережа забезпечує миттєвий моніторинг, забезпечуючи оптимальні потоки електроенергії між енергосистемою та клієнтами [2].

4. Розумний транспорт: у сучасних системах управління дорожнім рухом оптимальне використання наявних об'єктів і сучасних технологій є метою планувальників. Найважливішими перевагами використання розумних транспортних систем є зменшення заторів, підвищення рівня безпеки,

економія часу, зменшення споживання палива та покращення рівня обслуговування.

5. Розумна будівля: розумні будівлі використовують датчики та мережеві технології для обміну даними між обладнанням будівель, повідомляють інтелектуальний лічильник про зареєстроване споживання енергії в розумну мережу та дозволяють передавати дані від розумної мережі до будівлі.

6. Розумне водопостачання: за даними Всесвітньої організації охорони здоров'я, до 2025 року половина населення світу проживатиме в районах, що зазнають нестачі води, а до 2050 року глобальна урбанізація призведе до зростання споживання ресурсу на 55%. Тому в містах США, Канади, Німеччини, Японії вже сьогодні ухвалюють рішення щодо розумного використання водних ресурсів.

«Smart City» по-українськи лише подекуди має зазначені вище ознаки. Так, у столиці України, місті Києві, натепер запроваджено цифровий квиток на транспорт, на низці вулиць та метро працює розумна система відеоспостереження, функціонують е-петиції, електронний документообіг, є можливість записатися на прийом до лікаря і т. ін. Однак, якщо порівнювати розумні можливості міст Києва та, наприклад, Сінгапуру, значну перевагу матиме останнє.

Висновуючи зазначене вище, вважаємо за необхідне сконцентрувати увагу на блоках проблем, які ускладнюють впровадження концепції «Smart City» в українських містах, а саме:

1. У зв'язку з некоректним розумінням сутності концепту «Smart City» відсутнє стратегічне бачення щодо вибудування архітектоніки та практичного впровадження програм «Smart City» для конкретного міста чи територіальної громади.

2. Джерела фінансування конкретної програми «Smart City». Такі програми мають реалізовуватись переважно за бюджетування інвесторів,

меценатів, грантових проєктів та територіальної громади, оскільки коштів, які інколи виділяються з державного бюджету, завжди буде недостатньо.

3. Недостатні кваліметричні спроможності працівників територіальних громад, які б могли розробляти та супроводжувати реалізацію програми «Smart City» на належному рівні.

4. В Україні відсутній централізований орган, на який би покладалися повноваження щодо централізованого урядування питань, пов'язаних із концептом «Smart City». З поміж таких можемо назвати Міністерство розвитку громад та територій України, Міністерство цифрової трансформації України, громадські організації метою діяльності яких є забезпечення нормального функціонування територіальних громад і т. ін.

Наступним питанням, яке має систематично та ефективно вирішуватися розумним містом, є його кібербезпека.

Територіальні громади в Україні, нажаль, не вважають за необхідне належним чином фінансувати заходи із забезпечення кібербезпеки конфіденційної інформації, що перебуває у їх віданні.

Зокрема, у 2017 році (вже після масованих атак вірусу Petya) Київська міська рада спромоглася на Рішення «Про вжиття заходів кібербезпеки» від 22.06.2017 № 614/2776, яким виконавчому органу КМДА доручалося вжити протягом 2017 року заходів щодо впровадження вітчизняного програмного забезпечення для потреб місцевих органів виконавчої влади та органів місцевого самоврядування, підприємств, установ та організацій, що належать до комунальної власності територіальної громади міста Києва, *без додаткових витрат з бюджету міста Києва* [3].

У листопаді 2018 року в Дніпрі було створено перший регіональний центр СБУ, основними завданнями якого є реагування на кібератаки, націлені на державні електронні інформресурси та об'єкти критичної інфраструктури Дніпропетровщини [4].

Наприкінці 2018 року Дніпровська міська рада уклала меморандум про співпрацю із Службою безпеки України. Його мета – розширення взаємодії у

сфері кібернетичної безпеки та підвищення рівня захищеності інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем міської ради [5]. За допомогою цієї платформи Дніпровська міська рада та Ситуаційний центр СБУ в режимі реального часу можуть обмінюватися технологічною інформацією про кіберзагрози, що забезпечить підвищення рівня безпеки та мінімізує час реакції на інциденти.

У лютому 2023 року на позачерговій сесії Мукачівської міської ради депутати розглянули проєкт Меморандуму про організацію взаємодії у сфері кібербезпеки та кіберзахисту між Державним центром кіберзахисту Державної служби спеціального зв'язку та захисту інформації України та Мукачівською міською радою. З метою організації співпраці та координації дій Сторін у сфері кібербезпеки та кіберзахисту, оперативного реагування на кіберінциденти (SOC) в межах функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, затвердили текст меморандуму та уповноважили Мукачівського міського голову на його підписання [6].

Зауважимо, що зазначені вище заходи щодо забезпечення кібербезпеки з боку територіальних громад не є системними. Так, залучаються до співпраці спеціальні державні органи (СБУ, ДССЗЗІУ і т. ін.), до повноважень яких належить реалізація державної політики щодо кіберзахисту державних підприємств, установ та організацій і об'єктів критичної інфраструктури. Проте безпосередніх повноважень щодо кіберзахисту інформаційних ресурсів, які перебувають у віданні підприємств, установ та організацій територіальних громад, дані органи не мають.

Звертаємо увагу, що у розрізі паралельного реформування місцевого самоврядування та інформаційної безпекової сфери, зокрема прийняття Стратегії кібербезпеки України (2021 р.), Доктрини інформаційної безпеки України (2017 р.), Стратегії інформаційної безпеки України (2021 р.), будь-які згадки про кібербезпеку інформаційних ресурсів, що створюються

територіальними громадами та перебувають у їх віданні, у даних нормативно-правових актах взагалі відсутні.

Однак у п. 1 ч. 2 ст. 4 Закону України «Про основні засади забезпечення кібербезпеки України» (2017 р.) зазначено, що об'єктами кіберзахисту є комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону. Ч. 4 ст. 5 цього Закону визначено, що з-поміж інших, суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є органи місцевого самоврядування.

У статті 13 цього ж Закону, яка має назву «Фінансове забезпечення заходів кібербезпеки», зазначено, що джерелами фінансування робіт і заходів із забезпечення кібербезпеки, крім іншого, є кошти і місцевих бюджетів.

Однак, у ЗУ «Про місцеве самоврядування в Україні» (1997р.) *про повноваження органу місцевого самоврядування як суб'єкта забезпечення кібербезпеки не згадується жодним чином*. Як наслідок, у бюджетах територіальних громад не закладаються видатки на забезпечення кібербезпеки інформаційних ресурсів, які перебувають у їх віданні. Тобто такі видатки територіальні громади не вважають обов'язковими.

Отже, з метою вирішення даної проблематики, Закон України «Про місцеве самоврядування в Україні» (1997 р.) необхідно доповнити положеннями, які б розширили повноваження сільських, селищних, міських рад, зокрема щодо «затвердження обов'язкових вимог із кібербезпеки об'єктів, що перебувають у власності територіальних громад» та «здійснення заходів щодо підготовки обов'язкових вимог із кібербезпеки об'єктів, що перебувають у власності територіальних громад».

Список використаних джерел:

1. Singh, A., Chatterjee, K. Securing smart healthcare system with edge computing. *Computers & Security*. Vol. 108, September 2021. URL: https://doi.org/10.1016/j.cose.2021.102353

2. Behzad, r., Mehrpooya, M., Marefati, M. Parametric design and performance evaluation of a novel solar assisted thermionic generator and thermoelectric device hybrid system. *Renewable Energy*. Vol. 164, 2021. pp. 194–210.

3. Рішення Київської міської ради «Про вжиття заходів кібербезпеки» від 22.06.2017 № 614/2776. URL: https://kyivcity.gov.ua/npa/pro__vzhittya_zakhodiv_z_kiberbezpeki/eiloxqlprq_614-2776.pdf

4. У Дніпрі створили перший регіональний центр кібербезпеки СБУ (2018). *Укрінформ.* URL: https://www.ukrinform.ua/rubric-regions/2585234-u-dnipri-stvorili-persij-regionalnij-centr-kiberbezpeki-sbu.html

5. Дніпровська міська рада підписала меморандум про співпрацю з СБУ у сфері кібернетичної безпеки. URL: https://dniprorada.gov.ua/uk/articles/item/28689/dniprovska-miska-rada-pidpisala-memorandum-pro-spivpracyu-z-sbu-u-sferi-kibernetichnoi-bezpeki

6. У Мукачеві погодили меморандум у сфері кібербезпеки та кіберзахисту. URL: https://cybersec.net.ua/novyny/496-u-mukachevi-pohodyly-memorandum-u-sferi-kiberbezpeky-ta-kiberzakhystu.html