

УДК 621.376; 534::621.382

Ігнатоля П.М.¹, Різак М.В.²

¹ асп. ДВНЗ «Ужгородський національний університет»

² доц. ДУ «Київський авіаційний інститут»

АНАЛІЗ РИЗИКІВ І ЗАГРОЗ КОНФІДЕНЦІЙНОСТІ В РОЗУМНИХ МІСТАХ, КЕРОВАНИХ ДАНИМИ

Процеси урбанізації та друга промислова революція, відома також як технологічна революція, починаючи з 1990-х років, стали каталізатором виникнення концепції «розумних міст» – урбанізованих територій, що використовують передові інформаційні технології та аналіз даних для підвищення якості життя населення, забезпечення громадської безпеки та покращення взаємодії між громадянами та органами державної влади і місцевого самоврядування.

Недостатній захист приватності в розумних містах може викликати серйозні занепокоєння серед громадян, призводячи до юридичних та етичних проблем, крадіжок особистих даних і навіть до проявів дискримінації.

У контексті розумних міст та громад питання конфіденційності зазвичай фокусуються на трьох основних напрямках: безпеці даних, їх

комерційному використанні та рівні довіри до урядових структур. Далі в роботі буде здійснено детальний аналіз кожного з цих аспектів.

Безпека даних

Забезпечення безпеки та конфіденційності персональної інформації є основою для ефективного функціонування будь-якої системи збору та обробки даних, зокрема в контексті розумних міст. Оскільки ці міста значною мірою залежать від пристроїв Інтернету речей (IoT), то вони стають вразливими до кібератак на рівні інфраструктури через недостатньо захищені технології, що лежать в основі таких пристроїв.

Державні структури та організації, які можуть виступати у ролі зберігачів великих обсягів чутливої інформації про громадян і працівників, стають особливо привабливими для кіберзлочинців.

Відсутність належного рівня захисту даних може не лише спричинити економічні та репутаційні втрати, а й викликати серйозні соціальні наслідки, включаючи порушення прав громадян на приватність.

Крім того, обмін даними з приватними підрядниками чи організаціями підвищує ризики, адже кібератака на будь-який із таких суб'єктів може поставити під загрозу спільну інформаційну мережу.

Розв'язання зазначених проблем вимагає комплексного підходу, спрямованого на вдосконалення практик кібербезпеки та впровадження ефективних стратегій захисту чутливих даних у контексті функціонування розумних міст.

Комерційне використання даних у розумних містах і громадах викликає значне занепокоєння щодо конфіденційності.

Розглянемо основні аспекти проблем конфіденційності, пов'язаних із комерційним використанням даних:

Таргетована реклама

Зібрані дані використовуються для формування детальних профілів індивідів, що забезпечує можливість подальшої реалізації цільової реклами. Така практика може спричинити відчуття порушення приватності у мешканців, оскільки персоналізовані рекламні повідомлення базуються на їхній поведінці, вподобаннях та інших аспектах особистого життя.

Монетизація даних

Компанії можуть отримувати прибуток від монетизації зібраних даних шляхом їх продажу третім сторонам. Така практика порушує важливі питання щодо отримання згоди громадян та їхньої поінформованості про способи використання і передачі їхньої особистої інформації.

Профілювання та прийняття рішень

Комерційні суб'єкти можуть використовувати алгоритми для аналізу даних із метою профілювання, що може впливати на рішення, пов'язані з

працевлаштуванням, житлом чи фінансовими послугами. Це викликає занепокоєння щодо справедливості та потенційної дискримінації.

Довіра до уряду

Остання група проблем, що стосується впровадження розумних міст та громад, зосереджується на занепокоєнні громадськості щодо потенційного використання цих ініціатив для здійснення урядового спостереження за громадянами.

Знаковим прикладом таких побоювань стали події 2013 року, коли колишній співробітник Агентства національної безпеки США (АНБ) Едвард Сноуден оприлюднив дані про існування глобальних програм масового спостереження. Серед них — програма PRISM, яка передбачала збір даних користувачів великих технологічних корпорацій, а також масовий збір метаданих телефонних розмов АНБ. Це викликало широку суспільну дискусію щодо балансу між національною безпекою та правами на приватність.

Для забезпечення захисту конфіденційності та зміцнення довіри громадян у контексті ініціатив розумних міст пропонуються такі стратегії:

Впровадження надійних політик конфіденційності

Розробка та впровадження чітких і суворих законодавчих норм, які регулюють процеси збору, зберігання та використання даних. Такі норми повинні надавати пріоритет захисту приватності громадян через чітко визначені правила та процедури.

Прозорість і підзвітність

Важливим фактором зміцнення довіри громадян є створення механізмів громадської підзвітності, що включають регулярне інформування про мету та масштаби збору їх приватної інформації.

Юридичні гарантії

Удосконалення правових механізмів для забезпечення відповідності заходів по збору даних громадян чинним законам і нормативним актам. Необхідно проводити регулярні аудити практик збору даних для контролю за їхньою відповідністю встановленим правовим стандартам і недопущення порушень прав громадян.

Висновок

Таким чином, ефективне вирішення проблем конфіденційності в розумних містах вимагає впровадження багаторівневого підходу, що включає технічні, правові та організаційні заходи, спрямовані на забезпечення етичного використання технологій у міському управлінні.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ali, J., et al. "Trust-Based Secure Parking Allocation for IoT-Enabled Smart Cities." Sustainability, 2023.

2. Kitchin, R. (2014). The real-time city? Big Data and smart urbanism. *GeoJournal*, 79, 1–14. DOI: 10.1007/s10708-013-9516-8