Олександр ТИТАРЕНКО
старший викладач кафедри інформаційних технологій
та інформаційних систем ДРІДУ НАДУ

КІБЕРБЕЗПЕКА «РОЗУМНОГО» МІСТА

В останні десять років у багатьох країнах реалізуються проекти з розвитку сучасної міської інфраструктури на базі широкого використання досягнень сучасних технологій, особливо засобів інформаційно-комунікаційних технологій (ІКТ). Ця концепція, яка отримала назву «розумне» місто (Smart City), згуртовує навколо себе міську владу, громадських діячів та бізнес. Концепцію Smart City можна визначити як використання цифрових і комунікаційних технологій з метою підвищення якості та ефективності міських послуг, скорочення витрат і споживання ресурсів, розширення співробітництва з громадянами Концепція розумного міста більше не футуристична ідея, а реальна ініціатива, яку розпочинають застосовувати уряди по всьому світу. Багато організацій в світі працюють над цими технологіями. За прогнозами світовий ринок «розумних» міст виросте з 411,31 млрд. дол. у 2014 році до 1,13484 трлн.дол. у 2019 році.

«Розумні» міста визначаються також як «місто знань», «цифрове місто», «кібермісто», «екомісто» – в залежності від цілей міського планування. Вони ведуть постійний моніторинг найважливіших об'єктів інфраструктури – автомобільних доріг, мостів, тунелів, залізниць, метро, аеропортів, морських портів, систем зв'язку, водопостачання, енергопостачання, найважливіших будівель з метою оптимального розподілу ресурсів і забезпечення безпеки. Вони постійно нарощують число надаваних населенню послуг, забезпечуючи стійке середовище, яке сприяє благополуччю і збереженню здоров'я городян. «Розумними» можуть бути як нові міста, які відразу будуються як «розумні», або, що частіше, звичайні міста, які крок за кроком стають «розумними».

Подібні проекти відносяться до інфраструктурних і їхній бюджет становить десятки мільярдів доларів, як при будівництві нових «розумних» міст з нуля, так і при модернізації існуючих міських систем. Реалізуються вони завжди з ініціативи урядів або місцевої влади із залученням бізнес-партнерів.

Багато найбільших міст світу розпочали здійснення проектів створення «розумного» міста, серед них Нью-Йорк, Сеул, Токіо, Шанхай, Сінгапур, Каїр, Дубай, Барселона, Амстердам, Лондон, Ніцца, Париж, Копенгаген, Відень. Існуючі проекти «розумного» міста ставлять різні пріоритетні цілі і завдання, але всі «розумні» міста мають три спільні найважливіші риси – наявність інфраструктури ІКТ, чітко вибудувана і інтегрована система управління, «розумні» користувачі

В Україні такі проекти розгортаються в Києві, Львові, Дніпропетровську, Вінниці. Так, «Стратегія реалізації концепції Київ Смарт Сіті 2020» [1], передбачає активну співпрацю політичних лідерів, депутатів Київської міської ради, керівників та працівників департаментів і служб міста; державних та приватних операторів житлово-комунальних послуг, операторів зв'язку,

освітніх та наукових закладів; кінцевих користувачів; інвесторів; постачальників рішень – технологічних, фінансових та інвестиційних.

З огляду на сучасні темпи інновацій вже найближчим часом моделі «розумних» міст стануть поширеними реальними і популярними стратегіями міського розвитку. Для того щоб формування «розумних» міст стало наступним етапом процесу урбанізації потрібні і нові стандарти. З огляду на велике значення стандартизації для створення «розумних» міст, різноманітні заходи здійснюються Міжнародною організацією по стандартизації та Міжнародним союзом електрозв'язку.

Проблеми безпеки смарт-міст мають за своєю природою міжнародний рівень і притаманні містам по всьому світу. Громадська інфраструктура, як і раніше, являє собою особливо привабливу мішень для злочинців і терористів. У міру того, як світ стає все більш урбанізованим, міські високотехнологічні центри із цифровими технологіями збільшують вразливість суспільства. Міста є критично важливими інфраструктурами у всіх можливих сенсах, і якщо їх комп'ютеризація проводиться без урахування кібербезпеки з самого початку, проблеми, що можуть виникнути, сягнуть куди більш драматичного розмаху ніж знайомі і часто обговорювані питання кібербезпеки сьогоднішньої критичної інфраструктури. Це завдання треба вирішувати на ранній стадії, інакше вартість і складність створення «розумного» міста може надзвичайно ускладнити вирішення проблем безпеки на наступних етапах реалізації.

З Інтернетом речей (IoT), який продовжує стимулювати розвиток розумних міст, міські інфраструктури стають все більш комплексними, але залишаються легкими для проникнення. Кілька років тому, під час реалізацій першої хвилі Інтернету речей, комунікації та зв'язок були основними цілями. Факт підключення до мережі телевізорів, електричних лампочок і термостатів був значним технічним прогресом і аспекти управління доступом та ідентичністю часто нехтувалися. Такими підключеннями стара інфраструктура модернізувалася, але в мережах, коли вони створювалися, ніякої кібербезпеки за проектом не передбачалося.

З досягненням зрілості і стабільності IoT краще стали розумітися потенційні уразливості і ризики пов'язані з втратою даних. Значна кількість пристроїв Інтернету речей надає можливості атаки на дані мережі. У масштабах міста, в якому тисячі пристроїв спілкуються одночасно як з користувачами, так і між собою, наслідки для безпеки стають значними.

Мережа може бути порушена певними хакерами, зловмисниками або й одиночними гравцями. Вразлива кібератака може бути здійснена з одного смартфона або робочого місця. Кожна з функціональних систем розумного міста може викликати інтерес з боку внутрішніх і зовнішніх зловмисників. Вони можуть поставити під загрозу надання послуг, спровокувати серйозні інциденти в наданні критично важливих послуг, створити мережі типу ботнет, які складаються із скомпрометованих пристроїв, і використовувати їх для виконання завдань, відмінних від тих, для яких вони були спочатку призначені [4].

Ризик також полягає в тому, що установи або приватні компанії, які встановлюють міські служби, надають більшого значення належному функціонуванню їх інфраструктури, ніж захисту даних які вони обробляють. Одним з основних завдань в містах стає поєднання збору і аналізу персональних даних громадян, забезпечуючи при цьому захист інформації. Експерти Cloud Security Alliance [3] вказують, що міста, як правило, занадто довіряють продавцям технологій які вони використовують. Міська влада не повинна сліпо довіряти компаніям-розробникам − міста повинні виконувати свої власні тести, щоб визначати які продукти є найбільш ефективними не тільки з точки зору функціональності, але й з точки зору кібербезпеки.

«Розумні» міста можуть безпечно розвиватися і процвітати, якщо кібербезпека і захист інформації є фундаментальними компонентами послуг, що надаються учасникам. Коли проектуються і впроваджуються послуги, архітектура та додатки для інформаційної платформи «розумного» міста, це повинно бути зроблено з високим рівнем безпеки проти кібератак щоб гарантувати доступність послуг, їх безперервність, управління, захист даних, а також стійкість мережі в разі серйозних інцидентів. Важливо, щоб міська влада розробляла рішення з плануванням і надійним запровадженням стратегії кібербезпеки і пом'якшенням наслідків у разі нападу або втрати даних. Нереально очікувати, що міські мережі можуть бути повністю вільними від шкідливої поведінки. Навіть якщо будуть прийняті найкращі заходи безпеки, хтось або щось в кінцевому підсумку може вивести її з ладу з огляду на велику кількість існуючих векторів атак і загроз. Контроль за станом мереж і, що більш важливо, плани їх відновлення, також повинні бути розроблені не тільки для зниження ступеня ризику, а й для активного реагування, коли виявлена проблема.

Основними проблемами інформаційних систем «розумних» міст з точки зору кібербезпеки є велика кількість технологій і практичних рішень, які повинні взаємодіяти і зв'язуватися один з одним, нерівна якість різних вбудованих технологій, дистанційна і безпосередня експлуатація інформаційних систем Smart City, величезні обсяги даних для аналізу і зберігання. І всі ці проблеми поряд з багатьма іншими слід розглядати завчасно, до «порозумнішання» кожного міста. Модернізація і «доповнена кібербезпека» не варіант для концепції «розумних» міст. Ризики занадто великі і українські міста повинні використовувати шанс розглядати кібербезпеку з самої ранньої стадії на всіх можливих рівнях. Кібербезпека з нуля − єдиний варіант для концепції «розумне» місто. Міська стратегія кібербезпеки повинна передбачати розвиток системи забезпечення захисту кіберпростору; своєчасне виявлення і нейтралізацію кіберзагроз, а також їх запобігання; забезпечення координації, взаємодії і розподілу повноважень в питаннях кібербезпеки, кіберзахисту і протидії кібертероризму та кіберзлочинності; створення координаційного центру кібербезпеки як робочого органу міського управління.

З метою забезпечення кіберстійкості «розумних» міст з'явилася міжнародна ініціатива Securing Smart Cities, активно підтримувана рядом організацій в усьому світі. Заявленою місією ініціативи є визначення викликів

кібербезпеки, що стоять перед «розумними» містами, і вироблення ефективних рішень протидії. Це включає просування кращих практик в галузі кібербезпеки і кіберрішень для всіх технологій, що використовуються в «розумних» містах. Ініціатива націлена на вирішення кіберпроблем на кожному етапі розвитку Smart City – від планування до фактичної реалізації інтелектуальних міст.

У кінці листопада 2015 року ініціатори Securing Smart Cities випустили розроблені спільно з Cloud Security Alliance керівні принципи для прийняття за основу технологій «розумного» міста [2]. Це огляд ключових елементів які організації повинні враховувати з метою реалізації кращих технологічних рішень з найменшим ризиком впливу кіберзагроз. Мета ініціативи – забезпечення безпеки «розумних» міст серією заходів, таких як сприяння розумінню місцевою владою, розробниками і постачальниками необхідності і фінансових переваг передової практики кібербезпеки; співпраця з партнерами для обміну ідеями та методологіями; сприяння розумінню важливості і переваг розгляду загроз безпеці на ранній стадії розробки плану або проекту; встановлення співпраці між містами, постачальниками і спільнотою кібербезпеки; встановлення стандартів, керівних принципів і джерел, які можуть допомогти поліпшити кібербезпеку в усіх областях, пов'язаних з «розумним» містом.

Появи і розвитку «розумних» міст в Україні не уникнути, тому проблеми кібербезпеки треба вирішувати. Але кількість питань різко скоротилося б при правильному підході до «безпеки з нуля».

Список використаних джерел

1. Концепція Київ Смарт Сіті 2020. – Режим доступу : http://kscf.in.ua/Smart_City_UKR_Print_final.pdf
2. Cyber Security Guidelines for Smart City Technology Adoption. − Access mode : http://securingsmartcities.org/wp-content/uploads/2015/11/
3. Les données numériques : le cœur des villes intelligentes et leur plus grande menace. − Mode d'accès : http://www.lebigdata.fr/les-donnees-numeriques-le-coeur-des-villes-intelligentes-et-leur-plus-grande-menace1911
4. Sécuriser les smart cities. − Mode d'accès : http://www.lesechos.fr/idees-debats/cercle/cercle-145555-la-securite-des-smart-cities-nouvel-enjeu-pour-les-gouvernements-1183369.php