DOI: https://doi.org/10.33216/1998-7927-2023-278-2-56-60

УДК 332.1 : 911.375 : 004 :338

ІНТЕГРАЦІЯ ЦИФРОВИХ ТЕХНОЛОГІЙ В МІСЬКУ ІНФРАСТРУКТУРУ ЯК ФАКТОР РОЗБУДОВИ СОЦІАЛЬНО-ЕКОНОМІЧНОЇ БЕЗПЕКИ МІСТА

Кудріна О.Ю.

THE INTEGRATION OF DIGITAL TECHNOLOGIES INTO THE CITY INFRASTRUCTURE AS A FACTOR IN THE DEVELOPMENT OF THE SOCIAL AND ECONOMIC SECURITY OF THE CITY

Kudrina O.Y.

Безпека міста має важливе значення, тому міста впроваджують цифрові технології в свою інфраструктуру та покращують умови життя своїх громадян. Зі стрімким розвитком цифрових технологій і впровадженням концепції розумного міста життєво важливо визначити та запровадити засоби контролю соціально-економічної безпеки. Цифрові технології можуть керувати моделями транспортного руху, камерами безпеки, постачанням води тощо. Зараз майже кожна розвинена країна має доступ до певного типу таких пристроїв, які можуть мати доступ до Інтернету, тому безпека для розумних міст стала важливою вимогою, зокрема у світлі російсько-української війни. Отже, безпека міста стала одним із важливих та надзвичайно актуальних питань на арені кібербезпеки. Концепція розумних міст стала частиною нашого повсякденного життя. Концепція розумних міст означає майже повний контроль кожного аспекту функціонування повсякденного життя громадян, наприклад, контроль над передачею комунальних послуг, таких як вода, електрика тощо. Мета статті полягає у розкритті особливостей соціально-економічної безпеки міст як важливої умови забезпечення розвитку цифрової економіки України, визначенні факторів впливу на забезпечення кібербезпеки розумних міст у період повоєнного відновлення міст України. У статті розглянуто питання безпеки розумного міста. Перше з цих питань полягає в тому, що зі швидким розвитком цифрових технологій, що забезпечують концепцію розумного міста, чи розвиваються технології, які здатні підтримувати безпеку такого міста. Іншою проблемою є розгортання виправлень і оновлення безпеки. Ще одна проблема, про яку багато людей не замислюються і яка має величезний зв'язок із розумними містами, це бюджет для проєкту розумних міст. Однією з найкращих речей для вирішення проблем безпеки розумного міста є постійне тестування на проникнення. Одним із найважливіших способів захисту є наявність навчених і сертифікованих спеціалістів, які розробляють, проєктують і підтримують цифрові системи безпеки міста, а також оцінка існуючих продуктів безпеки на ринку, які можна адаптувати до потреб безпеки розумного міста. Для вирішення проблем безпеки, пов'язаних із безпекою розумного міста доцільно: розробити або налаштувати систему або продукт безпеки для посилення бездротових портів, протоколів і шифрування; розробити варіанти навчання сертифікованих фахівців з безпеки, які мають здатність захистити розумне місто від зовнішніх загроз; визначити та оцінити існуючі продукти безпеки на ринку, які можна адаптувати до потреб безпеки розумного міста.

***Ключові слова**: соціально-економічна безпека міста, міська інфраструктура, розвиток міста, розумне місто, цифрові технології.*

Вступ. Цифрові міста стають реальністю і є частиною нашого повсякденного життя. Безпека міста має важливе значення, тому міста впроваджують цифрові технології в свою інфраструктуру та покращують умови життя своїх громадян. Зі стрімким розвитком цифрових технологій і впровадженням концепції розумного міста життєво важливо визначити та запровадити засоби контролю соціально-економічної безпеки. Цифрові технології можуть керувати моделями транспортного руху,

камерами безпеки, постачанням води тощо. Зараз майже кожна розвинена країна має доступ до певного типу таких пристроїв, які можуть мати доступ до Інтернету, тому безпека для розумних міст стала важливою вимогою, зокрема у світлі російсько-української війни. Отже, безпека міста стала одним із важливих та надзвичайно актуальних питань на арені кібербезпеки.

Аналіз досліджень та публікацій. Перший справжній приклад розумного міста з'явився на початку 1970-х років, коли у Лос-Анджелесі були використані комп'ютерні бази даних, кластерний аналіз і аерофотознімки для збору даних [4]. Це був справді початок революції розумних міст і безпеки, яка прийде з нею. До середини 1980-х суспільство почало спостерігати поширення локальних мереж, клієнтських робочих столів і серверів для освітніх, медичних і військових цілей. Мережа агентства передових дослідницьких проєктів (ARPANET) була першою такою мережею. Спочатку ARPANET фінансувався Міністерством оборони Сполучених Штатів і використовувався у військових дослідженнях. Однак ця технологія породила початок мереж для загального користування. Крім того, у 1980-х роках ми почали спостерігати, як Інтернет у його перших формах почав використовуватися мережами. Академічні установи, такі як школи та інші заклади, почали створювати базові мережі для обміну інформацією між дослідницькими групами. ARPANET є одним із важливих факторів, які привели до створення розумних міст у їхньому нинішньому. На даний момент розумні міста розуміються як міста, де все базується на ідеї збору даних за допомогою технологій.

Відтоді розумні міста в тій чи іншій формі почали з'являтися по всьому світу [9]. Будь-яке сучасне місто керується певною кіберінфраструктурою розумного міста. Тобто місто та його ресурси, такі як постачання води, рух транспорту та використання електроенергії, контролюються кіберінфраструктурою.

Поряд з цим зросла не лише сфера розумних міст, але й занепокоєння муніципалітетів щодо їх безпеки [7]. Індустрія кібербезпеки в області безпеки розумних міст має намір стати однією з найбільших областей, що приносять прибуток, у наступні кілька років. Технологія BusinessInsider повідомляє, що протягом наступних років відбудеться зростання економічної цінності індустрії безпеки розумних міст [5].

Враховуючи очікуване розширення ініціатив розумного міста та проблеми безпеки розумного міста, дуже важливо серйозно ставитися до питань безпеки, досліджувати та впроваджувати ініціативи для захисту міст від загроз безпеці.

Таким чином, **мета статті** полягає у розкритті особливостей розбудови соціально-економічної безпеки міст за умов інтеграції цифрових технологій в їх інфраструктуру у період повоєнного відновлення міст України.

Результати дослідження. Концепція розумних міст стала частиною нашого повсякденного життя. Концепція розумних міст означає майже повний контроль кожного аспекту функціонування повсякденного життя громадян, наприклад контроль над передачею комунальних послуг, таких як вода, електрика тощо.

В результаті, якщо людина живе в розумному місті, вона стає неймовірно залежною від нього. Наприклад, розумні міста надають своїм жителям безкоштовний доступ до Wi-Fi. Це стало можливим завдяки встановленню бездротових маршрутизаторів на вулицях міст і дозволу жителям доступу до них. Як наслідок, важливою проблемою є загрози безпеці, які стоять за цим, і те, як громадяни міста можуть захистити себе, коли місто надає всім доступ до Інтернету безкоштовно [6].

Давайте розглянемо кілька сценаріїв, якими керує кіберінфраструктура розумного міста. Наприклад, розумний житель міста прокидається вранці і включає воду, щоб почистити зуби і ввімкнути світло у своїй ванній кімнаті. Обидва ці елементи, ймовірно, контролюються системою розумного міста. Місто надає ці об'єкти громадянам, і вони контролюються кіберінфраструктурою. Далі громадянин виходить на вулицю до пішохідного переходу, де має зупинитися рух транспорту та засвітитися світлофор на пішохідному переході. Схемами дорожнього руху, системами та пішохідними сигналами керує розумне місто. Необхідно зазначити, що розумне місто контролює більше аспектів, ніж можна подумати. Розумне місто також публікує відкриті дані, наприклад інформацію для громадян про своє місто. Наприклад, надається інформація про споживання води та електроенергії, кількість автомобілів, які проїхали на дорозі, кількість злочинних дій, скоєних у місті. Ця інформація використовується, щоб мати більш поінформованих і освічених жителів цього міста. Проте, зловмисники розумного міста можуть отримати інформацію про всіх мешканців за лічені хвилини, створюючи потенційну загрозу їх добробуту.

Розглянемо детальніше саме питання безпеки розумного міста.

Перше з цих питань полягає в тому, що зі швидким розвитком цифрових технологій, що забезпечують концепцію розумного міста, чи розвиваються технології, які здатні підтримувати безпеку такого міста. Нові пристрої, такі як планшети, ноутбуки, смартфони тощо, полегшили потенційним зловмисникам пошук безпекових прогалин у кіберінфраструктурі. Також із запровадженням загальноміського Wi-Fi у деяких містах є постійний доступ до Інтернету в будь-який час, тому рівень загрози для атаки лише зріс.

Ще одна пов'язана проблема – навчання працівників, які справді знають, як захистити мережу розумного міста. З таким швидким зростанням і розширенням розумних міст існує небагато фахівців з безпеки, які мають кваліфікацію для фактичного обслуговування та підтримки системи безпеки розумного міста. Сфера безпеки розумних міст наразі неукомплектована кадрами, очікується, що найближчим часом вона стане однією з п'яти найбільш затребуваних і бажаних вакансій на ринку технологій. Підготовлені спеціалісти в цій галузі користуються великим попитом. Без сертифікованих осіб було б важко вирішити проблеми безпеки. Нестача фахівців із безпеки дозволяє зловмисникам легко виявляти більше «дірок» у мережі та націлюватися на них, щоб загроза перетворилася на атаку [1; 2].

Іншою проблемою є розгортання виправлень і оновлення безпеки [10; 11]. Наприклад, з кожним новим оновленням, яке відбувається, у кіберінфраструктурі з'являтиметься якась нова прогалина в безпеці. Якщо програмне забезпечення не повністю протестоване, то воно може мати дуже реальні загрози для себе, що може спричинити великі проблеми для сторони безпеки [12].

Ще одна проблема, про яку багато людей не замислюються і яка має величезний зв'язок із розумними містами, – це бюджет для проєкту розумних міст. Бюджет міста має безпосереднє відношення до проєкту розумного міста, оскільки він визначає, скільки грошей місту доведеться витратити на заходи безпеки розумного міста. Як уже обговорювалося в цій статті, розумне місто може живити майже все, що забезпечує щоденні потреби міста. Наприклад, розумне місто керує такими речами, як камери руху, водопровідні та каналізаційні лінії, електростанції тощо. Якщо відповідний бюджет не буде надано особам, які керують розумними містами, вони не зможуть належним чином захистити ці міста. Бюджет може стати «тихим вбивцею» ініціативи безпеки розумного міста. Без належного бюджету це може призвести до таких ситуацій, як відсутність навчених і сертифікованих спеціалістів із безпеки, а також відсутність належних ресурсів для належного захисту розумного міста. Без встановленого бюджету, який обговорюється та планується, розумне місто може стати відкритим для більшої кількості загроз і атак, ніж багато хто вважає можливим.

Хоча може здатися, що з розумними містами існує нескінченна кількість проблем, існують рішення та способи їх покращення.

Однією з найкращих речей для вирішення проблем безпеки розумного міста є постійне тестування на проникнення. Розумні міста постійно розвиваються та в тій чи іншій формі оновлюються. Тому важливо переконатися, що ви постійно перевіряєте мережу на наявність нових безпекових «дірок», а шляхи доступу до неї мають бути першою лінією захисту для запобігання загрозам і атакам.

Іншим питанням, яке слід розглянути, є захист портів. Деякі міста пропонують безкоштовний Wi-Fi, це призводить до великого обсягу трафіку, що надходить і виходить через порти в мережі щодня. Завдяки цьому безпека порту також може бути важливою частиною зміцнення та захисту мережі.

Крім того, одним із найважливіших кроків у захисті розумного міста шляхом підвищення безпеки є апаратні та програмні брандмауери. Визначення типу трафіку, якому дозволено проходити через брандмауер, є одним із найважливіших способів захисту мережі від потенційної атаки, яка може мати місце. Брандмауер є ключовим для будь-якої мережі, але з точки зору розумного міста та безпеки брандмауер є життєво важливим для щоденних функцій.

Однак, навіть якщо є все апаратне та програмне забезпечення для захисту кіберінфраструктури розумного міста, воно не принесе користі, якщо немає добре навчених і сертифікованих осіб для захисту розумного міста [8]. Тому ми вважаємо, що одним із найважливіших способів захисту є наявність навчених і сертифікованих спеціалістів, які розробляють, проєктують і підтримують цифрові системи безпеки міста.

Останнім варіантом, який ми хотіли б дослідити, є оцінка існуючих продуктів безпеки на ринку, які можна адаптувати до потреб безпеки розумного міста. Бажано, щоб продукт був заздалегідь розроблений з урахуванням вимог безпеки розумного міста [3], тобто допомогти

захистити від злочинності, тероризму та громадянських заворушень. Це повинно допомогти правоохоронним органам і персоналу екстреної медичної служби, забезпечуючи швидке реагування на виклики та екстрену допомогу. Іншим важливим питанням є захист цього продукту або системи безпеки, щоб переконатися, що вони не потрапили в чужі руки, щоб продукт був повним охопленням і повністю виконував цілі безпеки.

Таке захищене розумне місто може зменшити рівень злочинності, підвищити привабливість для бізнесу, а також покращити розподіл ресурсів.

Отже, для вирішення проблем безпеки, пов'язаних із безпекою розумного міста доцільно: розробити або налаштувати систему або продукт безпеки для посилення бездротових портів, протоколів і шифрування; розробити варіанти навчання сертифікованих фахівців з безпеки, які мають здатність захистити розумне місто від зовнішніх загроз; визначити та оцінити існуючі продукти безпеки на ринку, які можна адаптувати до потреб безпеки розумного міста.

Висновок. Концепція розумних міст змінює світ. Хоча ми не усвідомлюємо, що так багато складних технологій уже інтегровано в міську інфраструктуру, і існує багато переваг, пов'язаних з цією концепцією, безпека є головною проблемою як фактор розбудови соціально-економічної безпеки міста. Незважаючи на значний інтерес до безпеки розумних міст, потрібні додаткові дослідження, щоб громадяни могли повністю усвідомити переваги таких міст. У цій статті ми обговорили питання інтеграції цифрових технологій в міську інфраструктуру та деякі потенційні рішення та рекомендації щодо роботи з захисту розумного міста з точки зору кібербезпеки.

Література

1. Бойко А. В. Стійкість національної економіки: теорія, методологія, практика. Київ : Ін-т екон. та прогнозув. НАН України, 2014. 288 с.
2. Павловський М.А. Стратегія розвитку суспільства: Україна і світ (економіка, політологія, соціологія) Київ: "Техніка", 2001. 312 с.
3. AGT. URL : http://www.cisco.com/c/dam/en_us/solutions/industries/docs/agt-cisco-city_safetyaag.pdf
4. Brasuell J. PlanetizenI. URL : http://www.planetizen.com/node/78847
5. Cerrudo C. Hacking Smart Cities. RSA Conference Cyber Security Guidelines for Smart. 2015.Pp. 2 – 18.
6. Edwards L. Privacy, Security and Data Protection in Smart Cities: a critical EU Law Perspective. CREATe Working paper,2015. 39 p.
7. Elmaghraby S., Losavio M. Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research*. 2014. Volume 5, Issue 4. Pp. 491–497.
8. Ji Y.B., Dou Y.D. Coordinated development of new urbanization and transportation infrastructure.*Acad. Exch.*2016. № *7*. Pp. 127–132.
9. Naphade M., Banavar G., Harrison C., Paraszczak J., Morris R. Smarter cities and their innovation challenges.*Computer (Long. Beach. Calif)*.2011. Vol. 44, no. 6.Pp. 32-39.
10. Sen M., Dutt A., Agarwal S., Nath A. Issues of privacy and security in the role of software in smart cities. International Conference on Communication Systems and Network Technologies, 2013. Pp. 518-523.
11. Zhao R.D., Fang C.L., Liu H.M. Progress and prospect of urban resilience research.*Prog. Geogr.*2020. № *39*. Pp. 1717–1731.
12. Xie C.Y., Wang M.H. A Study on the Impact of Transportation Infrastructure on the Spatial Distribution of Industrial Activities.*Manag. World*. 2020. № *36*. Pp. 52–64.

References

1. Boyko, A. V. (2014).Stiykist′ natsional′noyiekonomiky: teoriya, metodolohiya, praktyka[Stabilityofthenationaleconomy: theory, methodology, practice]. Kyiv: InstituteofEconomics. andpredicted NAS ofUkraine.
2. Pavlovskiy, M.A. (2001).Strategiarozvitkusyspilstva: Ukrainaisvit [The strategy of social development: Ukraine and the world], Kyiv, Ukraine
3. AGT (2016). URL : http://www.cisco.com/c/dam/en_us/solutions/industries/docs/agt-cisco-city_safetyaag.pdf
4. Brasuell, J. (2015). PlanetizenI. URL : http://www.planetizen.com/node/78847
5. Cerrudo, C. (2015). Hacking Smart Cities. RSA Conference Cyber Security Guidelines for Smart, 2-18.
6. Edwards, L. (2015). Privacy, Security and Data Protection in Smart Cities: a critical EU Law Perspective. CREATeWorkingpaper.
7. Elmaghraby, S.,&Losavio, M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. Journal of Advanced Research, 5, 4, 491–497.
8. Ji, Y.B.; Dou, Y.D. (2016). Coordinated development of new urbanization and transportation infrastructure.Acad. Exch.,7, 127–132.
9. Naphade, M., Banavar, G., Harrison, C., Paraszczak, J., &Morris, R. (2011). Smarter cities and their innovation challenges. Computer (Long. Beach. Calif), 44, 6, 32-39.
10. Sen, M., Dutt, A., Agarwal, S., &Nath, A. (2013).Issuesofprivacyandsecurityintheroleofsoftwareinsmartcities. InternationalConferenceonCommunicationSystemsandNetwork Technologies.
11. Zhao, R.D.; Fang, C.L.; Liu, H.M. (2020). Progress and prospect of urban resilience research.Prog. Geogr.,39, 1717–1731.
12. Xie, C.Y.; Wang, M.H. A (2020). Study on the Impact of Transportation Infrastructure on the Spatial Distribution of Industrial Activities.Manag. World,36, 52–64.

Kudrina O.Yu. The integration of digital technologies into the city infrastructure as a factor in the development of the social and economic security of the city.

The article is devoted to the disclosure of features of socio-economic security of cities as an important condition for ensuring the developmen to the digital economy of Ukraine, determination of influencing factors on ensuring the cyber security of smart cities during the post-warre construction of Ukrainian cities. Theso-called "digitalage" has brough to neprofound key change to the global economy: digital infrastructure has become a key element of critical infrastructure. The growing dependence of almost every sector of the economy on the digital capabilities of one or another country dramatically affects the economic security as a whole and the socio-economic security of the city inparticular. The current state and prospects for the developmen to ffixed and mobile broad band networks in Ukraine, the growing capacities of post-war urban development create the necessary conditions for more intensive development, conceptualization and development of smart cities. It is very important to develop digital services to ensure the most efficientuse of the city's digital infrastructure. Governments can do this by requiring well-designed and well-planned environments and platforms that are based on internationally recognized systems and rules, ensuring interoperability, trust and cyber security in the initial design of information systems. The impact of digital transformation on city security is critical in the coming years, increasing the need for public support to develop digital skills, social and public services driven by the needs of the smart city security market. Directly, the smart city is a complex technological system in which the digital mind, with the help of a person, helps with the organization of transport, management of city utility services, and also manages security. Cyber security experts are convinced that solutions to ensure the security of smart cities can not be point-based. Rather, they should be part of a unified cybersecurity strategy that complements and support seach other. Of course, such planning includes the development of detailed regulations and instructions for Smart City services on what and how to do in the event of a cyberattack. There fore, to address the security challenges as sociated with smart city security, it is advisable to: design or configure a security system or product to streng then wire less ports, protocols, and encryption; develop training options for certified security specialists who have the ability to protect the smar tcity from external threats; identify and evaluate existing security products on the market that can be adapted to the security needs of a smart city.

***Keywords**: socio-economic security of the city, city infrastructure, city development, smart city, digital technologies.*

Кудріна Ольга Юріївна – доктор економічних наук, професор, професор кафедри бізнес-економіки та адмініструванняСумського державного педагогічного університету імені А.С. Макаренка

Стаття подана 15.04.2023.