Krzysztof Gawkowski*

Cyberbezpieczeństwo w inteligentnym mieście

Streszczenie

Bezpieczeństwo cyfrowych miast to jeden z najważniejszych elementów, który powinien towarzyszyć implementacji technologicznej w samorządzie terytorialnym. Celem artykułu jest przedstawienie kluczowych obszarów rozwoju inteligentnych miast oraz konieczności wdrażania wysokiej jakości cyberochrony, która pozwoli na zrównoważony wzrost przestrzeni miejskich. W pracy korzystano z obszarów badawczych obejmujących metodę monograficzną, obserwacyjną oraz indywidualnych przypadków. Autor podkreśla, że tylko symbioza wzrostu technologicznego i cyberbezpieczeństwa może na trwale zmienić tkankę miejską. Brak odpowiednich form zabezpieczenia cyfrowego dla coraz nowszych inwestycji technologicznych może zahamować rozwój miast i zniechęcić ludzi do inwestycji w smart city. Cyberbezpieczeństwo w inteligentnym mieście jest więc kluczowym punktem łączącym oczekiwania społeczne z szybkim rozwojem.

Słowa kluczowe: cyberbezpieczeństwo, miasta, technologia, cyfryzacja, smart city

* Dr Krzysztof Gawkowski, Katedra Bezpieczeństwa Wewnętrznego, Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej w Warszawie, e-mail: krzysztof.gawkowski@uth.edu.pl, ORCID: 0000-0002-4025-5927.

Wstęp

Rozwój technologiczny w XXI wieku stał się katalizatorem wielu społecznych przemian, a obszarem, który w znakomity sposób odnalazł się w zmieniającej się rzeczywistości, są miasta i duże aglomeracje. Powszechnym określeniem synergii między technologią a przestrzenią miejską stał się termin „inteligentne miasta" (smart cities). Idea ta wyrosła ze społecznych potrzeb mieszkańców, którzy z jednej strony cały czas domagają się lepszego życia w postaci odpowiedniego dostępu do ochrony zdrowia, edukacji, usług publicznych czy transportu, a z drugiej chętnie korzystają z nasilającego się trendu obecności technologicznej w życiu każdego człowieka.

Transformacja społeczna w miastach wywołana zmianą ich struktury demograficznej, urbanizacją czy niespotykanym wcześniej przepływem ludności, kapitału i informacji sprawiła, że stanęły one przed olbrzymimi wyzwaniami rozwojowymi. Ewolucja przestrzeni i kapitału społecznego na tym etapie nie może już zostać pozostawiona sama sobie i dlatego coraz mocniej przestrzenie miejskie potrzebują odpowiednich strategii działania. Dlatego idea smart cities staje się wewnętrzną tkanką do stymulacji rozwojowych i jednocześnie umożliwia dynamiczne przemiany społeczno-gospodarczo-technologiczne[1].

Nie wszystko co nazywane jest smart city w rzeczywistości nim jest. Termin ten bywa często nadużywany i wiązany jedynie z rozwojem technologiczny. To podstawowy błąd, dlatego że implementowane do rozwoju technologie informacyjno-komunikacyjne (ICT) mają wzmacniać i wiązać ze sobą inteligentną gospodarkę, mobilność czy środowisko wraz z odpowiednim wykorzystaniem inteligentnego kapitału społecznego, poprawy warunków życia oraz dobrego zarządzania. Problemy intensyfikują się również wtedy, kiedy inteligentne miasto jest bardziej zabiegiem marketingowym niż rzeczywistym rozwiązaniem wspomagającym funkcjonowanie miasta i ludzi w nich mieszkających.

Nowoczesne przestrzenie miejskie muszą odczytywać i łączyć ze sobą przede wszystkim oczekiwania mieszkańców. Szczególną rolę do odegrania mają władze, które odpowiadają za rozwój miasta, muszą dbać o to, żeby był on zrównoważony i dopasowany do społecznych oczekiwań. Podstawą takiej współpracy musi być zaufanie i zrozumieniu potrzeb, jest więc elementem bardzo delikatnym i narażonym na różnego rodzaju problemy. Jednym z nich jest bezpieczeństwo, a w nim cyberprzestrzeń.

1 Ch. Montgomery, *Miasto szczęśliwe*, Kraków 2015, s. 116–118.

Wszystkie główne sektory miejskich aktywności w smart cities są połączone zazwyczaj w jeden system informacyjno-informatyczny. Ilość przetwarzanych w ten sposób danych jest wręcz gigantyczna, a możliwości analityczne niewyobrażalne. Powoduje to, że posiadane zasoby są bardzo cenne zarówno dla biznesu, jak i pospolitych przestępców. Powszechna informatyzacja powoduje, że w miastach są zagrożone także systemy infrastruktury krytycznej, które trzeba chronić w zorganizowany sposób. Cyberbezpieczeństwo staje się ważnym elementem działania inteligentnego miasta, dlatego że bez odpowiednich zasobów straty spowodowane ewentualnymi naruszeniami mogą być zdecydowanie większe niż korzyści z rozwoju inteligentnego miasta.

Rozwój miast przyszłości

Miasto przyszłości to koncepcja mająca uczynić życie w lokalnych społecznościach bardziej przystępnym, wydajniejszym, można powiedzieć lepszym. Inteligentne zarządzanie polega na nieustającej i przenikającej się koordynacji oraz integracji wielu systemów. Szybki rozwój jest możliwy dzięki milionom sensorów zbierających informacje o aspektach funkcjonowania miasta, automatyzowanych procedurach administracyjnych, planowaniu strategicznym czy zarządzaniu na podstawie zaawansowanej analityki[2]. Miasto otoczone inteligentną siecią zbiera dane o zużyciu energii w budynkach, obciążeniu komunikacji miejskiej i ruchu na ulicach, dostępności parkingów, zapotrzebowaniu na wodę, korkach, wykorzystaniu energii elektrycznej czy liczbie wypożyczanych rowerów o każdej godzinie w ciągu dnia. Jednakże to jedynie namiastka tego, co inteligentne miasto może i jak to wykorzystuje.

Idealnym przykładem jak głęboko wkracza technologia w tkankę miejską jest Amsterdam. Nie chodzi tu wcale o ilość włączonej do pracy technologii, a wykorzystanie agregowanych danych i społecznego zaangażowania. Stworzono inteligentne centra pracy, żeby zachęcać do rezygnowania z dojazdu do innych dzielnic, stania w korkach i straty czasu, a jednocześnie mobilizować do korzystania z przestrzeni odpowiednio przygotowanej oraz zaopatrzonej w technologie audiowizualne. Inny pomysł to program „Ring-ring", czyli nagradzanie osób, które z samochodu przesiadły się na rower. Aplikacja zlicza

2 A. Korenik, *Smart city jako forma rozwoju miasta zrównoważonego i fundament zdrowych finansów miejskich*, „Ekonomiczne Problemy Usług" 2017, nr 4, s. 170.

kilometry przejechane na rowerze i przelicza je na pieniądze, które można wymienić na różne usługi. Inny projekt to inteligentna sieć energetyczna, która umożliwia elastyczny dobór źródeł energii i dokładny pomiar jej zużycia. Wdrożenie rozwiązań pozwoliło na oszczędności w zużyciu energii o blisko 30%. Rozwiązania smart pomagają także w inteligentnym zarządzaniu ruchem na kolei, monitorowanym w czasie rzeczywistym, a przy okazji informują korzystających o aktualnym czasie podróży[3].

Rozwiązania wprowadzone w Amsterdamie dzięki rosnącym możliwościom technologicznym będą na pewno się rozwijały. Coraz częściej miasta będą korzystać z osiągnięć sztucznej inteligencji, danych i ludzkich doświadczeń. W partnerskiej współpracy łatwiej rozwiązywać problemy, ale i na pewno będzie ich więcej niż dotychczas[4]. Koncepcja smart city jest tworzeniem nowego systemu funkcjonowania miasta. Z jednej strony opartego na władzy, która określa zadania publiczne i wybiera formę ich realizacji, wyznacza standardy jakościowe, ale zarazem dba o jakość i rezultaty świadczonych usług. Z drugiej strony, na człowieku, który jest zainteresowany nie tylko ciągłością usług, innowacyjnością, lecz także ich efektywnością oraz swoim bezpieczeństwem[5].

Procesy globalizacji będą niewątpliwie idee smart cities napędzały i tylko takie miasta, które nadążą za postępem technologiczny, będą mogły w sposób świadomy się rozwijać. Warto przy tym pamiętać, że miasta przyszłości to nie tylko nasycona do granic możliwości elektroniką przestrzeń życiowa, lecz także określona filozofia, która dotyczy kształtowania postaw mieszkańców, ich zachowań oraz warunków życia[6]. Żeby smart cities stały się rzeczywistym drogowskazem współczesnego rozwoju, wolnym od destabilizacji i niskiego poziomu życia, musimy przewidywać wszystkie zdarzenia, które tym procesem mogą zachwiać. Biorąc pod uwagę zasoby cyfrowe miast przyszłości, można śmiało powiedzieć, że zachowanie równowagi pomiędzy rozwojem a rozstrojem jest tam, gdzie bezpieczna cyberprzetrzeń. To właśnie cyberbezpieczeństwo będzie najważniejsze w zachowaniu zrównoważonego rozwoju i jednocześnie pozwoli korzystać ze wszystkich zasobów przestrzeni miejskiej bez żadnych obaw.

3 Ibidem, s. 172–173.

4 K. Korneluk, M. Bielawska, S. Zygadło, B. Dominiak, A. Kruczek, *Human Smart City: przewodnik dla samorządów*, Warszawa 2019.

5 P. Trąpczyński, M. Gorynia, J. Nowak, R. Wolniak, *EU Countries from Central and Eastern Europe, and the Investment Development Path Model: A New Assessment*, „Argumenta Oeconomica" 2019, t. 2, nr 3, s. 402.

6 A. Korenik, op. cit., s. 173.

Cyfrowe miasto

Identyfikacja zagrożeń w cyfrowym mieście w dużej mierze zależy od jego technologicznego zaawansowania. Nie bez znaczenia jest liczba czujników, sensorów i używanych aplikacji. Jednakże najważniejsza jest świadomość administratorów i użytkowników wprowadzanych technologii, a ta różni się w zależności od zaawansowania rozwojowego. Obecnie obserwujemy cztery fazy kształtowania się przestrzeni miejskich:

– smart city 1.0 – odnosi się do miast w początkowej fazie budowy, gdy wykorzystywanie nowoczesnych technologii zostało zainicjowane przede wszystkim przez firmy teleinformatyczne. Przemiana technologiczna była realizowana niezależnie od tego, czy była potrzebna miastom czy nie. Celem nadrzędnym była sprzedaż jak największej liczby systemów bez wcześniejszego sprawdzenia zapotrzebowania na nie, a procesy bezpieczeństwa były na poziomie podstawowym[7];

– smart city 2.0 – faza inicjowana zazwyczaj przez władze lokalne, które stawiają na rozwiązania mające poprawić jakość życia mieszkańców oraz wykorzystują projekty do promocji miasta. Bezpieczeństwo jest zintegrowane z projektowanymi urządzeniami, ale bez ich specjalnego wykorzystywania[8];

– smart city 3.0 – czas aktywnego podejścia do realizowanych projektów smart. Szczególną rolę w projektowaniu zapotrzebowania technologicznego odgrywają mieszkańcy i to oni decydują o kierunkach rozwoju. W tym zakresie zadaniem władz lokalnych jest skupienie się na tworzeniu przestrzeni i możliwości wykorzystania różnorodnego potencjału mieszkańców. Bezpieczeństwo jest obszarem dobrze rozeznanym i jest wymagane w każdym procesie[9];

– smart city 4.0 – najnowsza formuła rozwoju inteligentnego miasta. Stawia na hiperpołączenie technologii, danych i zaangażowania obywateli. Obszar czwartej generacji miast przyszłości jest silnie powiązany z innymi rewolucjami przemysłowymi zdominowanymi przez roboty, sztuczną inteligencję, nanotechnologię, internet rzeczy czy pojazdy autonomiczne. Głębokie zmiany technologiczne wymuszają stosowanie najwyższych standardów

7 H.I. Hussain, M. Haseeb, F. Kamarudin, Z. Dacko-Pikiewicz, K. Szczepańska-Woszczyna, *The Role of Globalization, Economic Growth and Natural Resources on the Ecological Footprint in Thailand: Evidence from Nonlinear Causal Estimations*, „Processes" 2021, t. 9, nr 7, art. 1103, s. 9.
8 B. Dominiak, K. Gawkowski, Z. Wasielewski, *Cyfrowe miasto – bezpieczna czy niebezpieczna przyszłość?*, Warszawa 2022, s. 15.
9 Ibidem.

cyberbezpieczeństwa, ponieważ tylko w taki sposób miasto może rozwijać się w zrównoważony sposób[10].

Należy zauważyć, że już w 2019 roku ESI ThoughtLab przeprowadził w 167 miastach w 82 państwach badania nad inteligentnym rozwojem i efektywnym wdrażaniem technologii cyfrowych. Z zebranych danych wynika m.in, że w miastach czwartej generacji dokonano poważnych inwestycji w rozwiązania chmurowe wykorzystujące internet rzeczy oraz nieco mniej technologie mobilne, biometryczne, blockchain oraz sztuczną inteligencję. Co ważne, aż 95% miast z obszaru rozwojowego 4.0 zapewniało, że cyberbezpieczeństwo jest brane pod uwagę na wczesnym etapie procesu, w porównaniu z 51% pozostałych miast. Wyniki badań jasno pokazały, że cyfrowe miasto przyszłości musi żyć w symbiozie z cybernetyczną tarczą, ponieważ tylko wtedy jego wszystkie atutu mogą zostać odpowiednio wykorzystane[11].

Bezpieczeństwo technologii smart

Bezpieczeństwo cyfrowe, ze względu na niewidzialną powłokę, która mu towarzyszy, jest często ignorowane i niedoceniane[12]. Największe problemy rodzą się wtedy, kiedy dokonujemy niewłaściwej klasyfikacji zagrożeń w technologii smart. Podział, którego powinniśmy się trzymać, dotyczy zarówno sfery wewnętrznej, jak i zewnętrznej. W obszarze wewnętrznym może być to np. przekazanie lub sprzedaż cyfrowych danych nieuprawnionym osobom bądź instytucjom, sabotaż, brak odpowiedniej kontroli nad procesami przetwarzania informacji czy błędy techniczne. W obszarze zewnętrznym pojawiać się będą ataki hackerskie, włamania, fałszywe informacje czy naruszenia integralności sprzętowej.

Przygotowanie rozwiązań mających ochronić cyberprzestrzeń przed incydentami wewnętrznymi i zewnętrznymi musi być poprzedzone odpowiednią ich identyfikacją. Biorąc pod uwagę liczbę aplikacji i sensorów używanych

10 Z.J. Makieła, M.M. Stuss, K. Mucha-Kuś, G. Kinelski, M. Budziński, J. Michałek, *Smart city 4.0: zrównoważony rozwój miast w Górnośląsko-Zagłębiowskiej Metropolii*, „Zrównoważony Rozwój" 2022, nr 14, s. 2–3, https://doi.org/10.3390/su14063516 [dostęp: 27.02.2023].
11 *Smart City Solutions for a Riskier World, How innovation can drive urban resilience, sustainability, and citizen well-being*, Filadelfia 2019, https://econsultsolutions.com/wp-content/uploads/2021/03/ESITL-Smart-City-Solutions-eBook-Final.pdf [dostęp: 22.03.2023].
12 R. Kitchin, M. Dodge, *The (In) Security of Smart Cities: Vulnerabilities, Risks, Mitigation and Prevention*, „Journal of Urban Technology" 2019, t. 26, nr 2, s. 47.

w miastach, złożoność systemów, ilość przetwarzanych danych oraz procesy podejmowania decyzji, ważne jest, żeby obraz zarządzanego pola był czytelny i umożliwiał odpowiednie wdrożenie procesów cyberbezpieczeństwa.

Identyfikacja zagrożeń w cyfrowym mieście musi uwzględniać wspominane wcześniej technologie informacyjne i komunikacyjne (ICT), które obejmują techniki przetwarzania, gromadzenia i przesyłania informacji. Dają one poczucie bezpieczeństwa m.in w procesach zarządzania sytuacjami kryzysowymi i pozwalają na lepszą koordynację w działaniach smart city. Drugi obszar to System Informacji Geograficznej (Geographic Information System – GIS), który służy do gromadzenia i przetwarzania danych geograficznych ułatwiających dostęp do danych statystycznych czy wykorzystywanie infrastruktury technicznej. Postęp tworzy się tam, gdzie jest mocno wykorzystywany internet rzeczy (Internet of Things – IoT), który ułatwia procesy komunikowania, wymiany informacji i automatyzuje wiele procesów bez bezpośredniego zaangażowania człowieka[13].

Kolejny element, który musi mocno brać pod uwagę infrastruktura cyfrowego bezpieczeństwa, to internet usług (Internet of Services – IoS). Wykorzystuje on zbiory danych i ich analizę w wypracowywaniu ostatecznych decyzji i ingeruje w wykonywanie usług końcowych, z których korzysta społeczność lokalna. Ostatni, ale nie mniej ważny element to duże zbiory danych (Big Data). Pozwalają one agregować potężne zbiory informacji i jednocześnie wyciągać z nich szybko wnioski. Systemy ich zabezpieczenia mają istotne znaczenie dla podejmowanie decyzji politycznych, czyli w konsekwencje zarządzania miastem[14].

Tak skonstruowana mapa zagrożeń pozwala na odpowiednią skalowalność zagrożeń w cyberprzestrzeni i jednoczesne planowanie odpowiednich środków przeciwdziałania. Różnorodność podnoszonych zagadnień utwierdza jedynie w przekonaniu, że systemy cyfrowego bezpieczeństwa na poziomie smart nie mogą być zaniedbywane już od początku procesów projektowania. Większy nacisk położony na odpowiednie przygotowanie procesów prewencyjnych w cyberprzestrzeni zwiększa tylko szanse na to, że incydentów będzie mniej, a jeżeli się zdarzą, to będą odpowiednio zarządzane.

13 K. Sienkiewicz-Małyjurek, *Smart City w budowaniu odporności miast na zagrożenia*, „Bezpieczeństwo. Teoria i Praktyka" 2020, nr 4, s. 82.
14 Ibidem.

Planowanie cyberbezpieczeństwa w smart cities

Bezpieczeństwo cyfrowe w inteligentnych miastach w dużej mierze zależy od procedur i zasad, które organizacja stosuje w celu ochrony swoich zasobów. Wyznaczone standard określają typy i sposoby reagowania w sytuacjach kryzysowych oraz określają postępowania w razie zaistnienia komplikacji w systemie. Niezmiennie istotne jest odpowiednie planowanie reakcji na zagrożenia w cyberdomenie oraz umiejętne ich eliminowanie. Celem cyberbezpieczeństwa w smart city jest odpowiednie zaplanowanie działań związanych podatnościami i ryzykami oraz zarządzanie bezpieczeństwem systemów informatycznych, które z jednej strony będzie zautomatyzowane, z drugiej, zapewni odpowiedni i czytelny podział ról dla pracowników odpowiadających za obszar bezpieczeństwa cyfrowego.

Mechanizmy odpowiedzialne za cyberbezpieczeństwo w smart city powinny zapewniać skuteczną ochronę zasobów informatyczno-informacyjnych organizacji i dlatego muszą spełniać wiele funkcji. Do zadań obszaru mapowania cyberprzestrzeni w mieście należy wykrywanie zagrożeń, odstraszanie potencjalnych atakujących, zapobieganie i minimalizowanie intensywności zagrożeń oraz odtwarzanie prawidłowej pracy wszystkich systemów tworzących tkankę smart w mieście. Bardzo ważne jest również udoskonalanie zabezpieczeń w celu podnoszenia poziomu ochrony, umiejętne wykorzystywanie doświadczeń i dzięki temu skuteczne monitorowanie zagrożeń zewnętrznych i wewnętrznych, a także uświadamianie użytkowników systemów informatyczno-informacyjnych o pojawiających się nowych zagrożeniach[15]. Taka organizacja bezpiecznej cyberprzestrzeni to pierwszy krok w kierunku dobrze zorganizowanej ochrony cyfrowego miasta. Pierwszy nie oznacza, że ostatni.

Cyberbezpieczeństwo w mieście powinno być zawsze uwzględniane w procesie projektowania i wdrażania systemów, które mają ułatwiać życie obywatelom. Cyfrowa ochrona nie może być traktowana jako rozwiązanie jedynie sieciowe czy aplikacyjne, bo często uszkodzenia mają charakter techniczny i tylko taka forma wsparcia może szybko pomóc w usunięciu problemów. W złożonej strukturze informatycznej miasta trzeba mieć odpowiednie rozeznanie, a to najlepiej zaplanować w symbiozie ze społeczeństwem korzystającym z technologii smart.

15 P. Górny, J. Krawiec, *Cyberbezpieczeństwa – podejście systemowe*, „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej" 2016, nr 2, s. 8.

W związku z tym w procesie projektowania cyberochrony należy uwzględnić liczbę eksploatowanych systemów informatycznych i ich złożoność, rodzaj i ilość przetwarzanej informacji oraz liczbę użytkowników i platform technologicznych. Konieczny jest przegląd systemów zabezpieczających infrastrukturę krytyczną w mieście. Ważną rolę będą odgrywały także wielkość, liczba i typ sieci: stacjonarne, mobilne, bezprzewodowe, zewnętrzne i wewnętrzne; zbierane dane wrażliwe, ich typy i sposoby fizycznego przechowywania; liczba i typ transakcji elektronicznych oraz złożoność realizowanych projektów. Dodatkowym atutem sprawnego zarządzania cyberbezpieczeństwem będzie posiadanie wiedzy o zakresie stosowania pracy zdalnej i rodzajach prowadzonej działalności biznesowej czy liczbie organizacji pozarządowych znających specyficzne wymagania branżowe smart city[16].

Cyberbezpieczeństwo w smart city musi być cały czas uzupełniane i rozwijane. Tak jak cały czas powiększa się udział technologii w życiu społeczeństwa, tak zmieniają się one same i człowiek bądź instytucja musi się do nich dopasowywać. Bezpieczeństwo w cyfrowym mieście będzie nadążało za rewolucją technologiczną tylko wówczas, gdy poświęcimy również czas na tworzenie strategii miejskiego bezpieczeństwa cyfrowego oraz programów operacyjnych do podtrzymania bezpieczeństwa cyfrowego w różnych jego aspektach. Ważnym obszarem jest także stworzenie miejskiego zespołu bezpieczeństwa cyfrowego i ratownictwa cyfrowego. Do tego niezbędne są również regulaminy bezpieczeństwa cyfrowego dla pracowników instytucji miejskich oraz szkolenia z ich stosowania.

Zakończenie

Koncepcja smart cities w ostatnich latach stała się domeną nie tylko wielkich aglomeracji, lecz także miast średniej wielkości. Oznacza to, że w coraz większym środowisku samorządowych wspólnot symbioza człowieka i technologii nabiera tempa. Społeczność lokalna, żeby mogła w pełni korzystać z dóbr, które przynoszą inteligentne miasta, musi się czuć bezpiecznie i być odpowiednio chroniona. Cyberbezpieczeństwo staje się podstawowym oczekiwaniem, od którego w największej mierze zależy czy rewolucja technologiczna w miastach zdobędzie przychylność społeczności czy nie.

16 Ibidem, s. 11.

Technologia informacyjna i komunikacyjna jest tak mocno obecna w nowoczesnych przestrzeniach miejskich, że często nie jesteśmy w stanie wyobrazić sobie, że mogłoby jej nie być. Można śmiało powiedzieć, że wzrastała wraz z jego rozwojem i jest już nie do oddzielenia. Telefony, systemy czy sensory są współzależne od siebie i zaburzenie jednego składnika może mieć negatywny wpływ na inne urządzenia. Uszkodzenia czy to software czy hardware mogą mieć bardzo istotny wpływ na bezpieczeństwo, logistykę, transport, gospodarkę oraz warunki życia każdego obywatela. Tylko odpowiednia forma działań prewencyjnych i edukacyjnych w cyfrowym świecie może uwolnić zarówno instytucje miejskie, jak i indywidualnego odbiorcę od obaw, że technologia wcale nie ułatwia życia, a rodzi masę problemów.

W ostatniej dekadzie wiele miast znacznie zwiększyło inwestycje w swoją cyfrową infrastrukturę, niekoniecznie wzmacniając systemowe działania na rzecz cyberbezpieczeństwa. To zła wiadomość, dlatego że potencjalne zagrożenia rosną wraz ze wzrostem społecznego uzależnienia od wdrażanych rozwiązań i nowej infrastruktury technologicznej. Cyberzagrożenia w ostatnich latach stały się coraz bardziej poważne i dlatego obecnie jest ostatni moment, żeby odpowiednio zarządzić systemami bezpieczeństwa cyfrowego.

W DNA działań samorządowych musi wejść, że każda nowa inwestycja cyfrowa ma zagwarantowany odpowiedni poziom cyberochrony. Często jest tak, że miasta wprowadzają technologie cyfrowe szybciej niż ludzka zdolność jest w stanie zrozumieć ich skutki, dlatego bardzo ważna jest edukacja w dziedzinie cyberzagrożeń i cyberbezpieczeństwa. W instytucjach publicznych muszą działać specjalne centra wsparcia kryzysowego i opieki cybernetycznej, ponieważ liczba urządzeń i sensorów tworzących cyfrowy świat obok człowieka będzie tylko rosła. Dopiero tak przygotowana warstwa ochronna może stanowić o odpowiedzialnym inwestowaniu w technologię smart i uczynienie miast przyjaznych obywatelom.

Bibliografia

Hussain H.I., Haseeb M., Kamarudin F., Dacko-Pikiewicz Z., Szczepańska-Woszczyna K., *The Role of Globalization, Economic Growth and Natural Resources on the Ecological Footprint in Thailand: Evidence from Nonlinear Causal Estimations*, „Processes" 2021, t. 9, nr 7.

Górny P., Krawiec J., *Cyberbezpieczeństwa – podejście systemowe*, „Obronność – *Zeszyty Naukowe* Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej" 2016, nr 2.

Kitchin R., Dodge M., *The (In) Security of Smart Cities: Vulnerabilities, Risks, Mitigation and Prevention*, „Journal of Urban Technology" 2019, t. 26, nr 2.

Korenik A., *Smart city jako forma rozwoju miasta zrównoważonego i fundament zdrowych finansów miejskich*, „Ekonomiczne Problemy Usług" 2017, nr 4.

Korneluk K., Bielawska M., Zygadło S., Dominiak B., Kruczek A., *Human Smart City: przewodnik dla samorządów*, Warszawa 2019.
Makieła Z.J., Stuss M.M., Mucha-Kuś K., Kinelski G., Budziński M., Michałek J., *Smart city 4.0: zrównoważony rozwój miast w Górnośląsko-Zagłębiowskiej Metropolii*, „Zrównoważony Rozwój" 2022, nr 14, https://doi.org/10.3390/su14063516 [dostęp: 27.02.2023].
Montgomery Ch., *Miasto szczęśliwe*, Kraków 2015.
Sienkiewicz-Małyjurek K., *Smart City w budowaniu odporności miast na zagrożenia*, „Bezpieczeństwo. Teoria i Praktyka" 2020, nr, 4.
Smart City Solutions for a Riskier World, How innovation can drive urban resilience, sustainability, and citizen well-being, Filadelfia 2019, https://econsultsolutions.com/wp-content/uploads/2021/03/ESITL-Smart-City-Solutions-eBook-Final.pdf [dostęp: 22.03.2023].
Trąpczyński P., Gorynia M., Nowak J., Wolniak R., *EU Countries from Central and Eastern Europe, and the Investment Development Path Model: A New Assessment*, „Argumenta Oeconomica" 2019, t. 2, nr 3.

Cybersecurity in a smart city

Abstract

Digital city security is one of the most important elements that should accompany technological implementation in local government. The purpose of the article is to present the key areas of smart city development and the need to implement high-quality cyber security that slowly for sustainable growth of urban spaces. The paper uses research areas including monographic, observational and individual case method. The author emphasizes that only the symbiosis of technological growth and cyber security can permanently change the urban fabric. Lack of adequate forms of digital security for the ever-newer technological investments, can hinder the development of cities and discourage people from investing in smart cities. Cyber security in a smart city is therefore a key point connecting public expectations with rapid development.

Key words: cybersecurity, cities, technology, digitization, smart city