KATARZYNA MODZELEWSKA

E-standard bezpieczeństwa społeczności lokalnych

W poszukiwaniu akceptowalnego poziomu bezpieczeństwa e-administracji samorządowej

Wprowadzenie

Fundamentalnym zadaniem administracji samorządowej jest zapewnianie bezpieczeństwa społeczności lokalnej, które może być rozumiane jako stan wewnętrzny gminy, regulowany normami prawnymi i pozaprawnymi, których przestrzeganie umożliwia prawidłowe funkcjonowanie tej wspólnoty[1]. Zatem kwestia poczucia bezpieczeństwa mieszkańców ma kluczowe znaczenie dla rozwoju e-administracji samorządowej, do którego przyczynia się każdy jej użytkownik i adresat e-usług. Stan bezpieczeństwa lokalnego jest skorelowany z takimi zagrożeniami jak cyberprzestępczość, cyberprzemoc oraz wykluczenie cyfrowe. Należy zauważyć, że nie jest to katalog zamknięty. W związku z powstawaniem nowych cyberzagrożeń i przeniesienia działań administracji samorządowej do sieci, konieczne jest znalezienie odpowiedzi na pytanie, w jaki sposób e-administracja przyczynia się do budowania i kształtowania poczucia bezpieczeństwa społeczności lokalnych za pomocą technologii ICT. Przedmiotem niniejszego artykułu jest próba dokonania oceny poziomu bezpieczeństwa e-administracji samorządowej i wyznaczenia standardu jej e-usług kierowanych do społeczności lokalnej. W artykule zbadano zarówno e-usługi wpływające na bezpieczeństwo społeczności lokalnych, jak również dokonano analizy poziomu bezpieczeństwa e-usług oferowanych przez e-administrację samorządową.

E-usługi i narzędzia informatyczne administracji samorządowej kształtujące poczucie bezpieczeństwa mieszkańców

[1] A. Urban, *Bezpieczeństwo społeczności lokalnych*, Warszawa 2009, s. 15.

Nowelizacje istniejącego prawa zobligowały administrację samorządową do korzystania z kanału elektronicznego, szczególnie w komunikacji z klientami urzędu, np. za pomocą elektronicznej skrzynki podawczej. Warto dodać, że „doręczenie pism następuje za pomocą środków komunikacji elektronicznej, jeżeli strona złoży podanie w formie dokumentu elektronicznego przez **e-skrzynkę podawczą**, wystąpi o to lub wyrazi na to zgodę”[2]. Wciąż aktualnym wyzwaniem na poziomie lokalnym jest osiągnięcie interakcji dwukierunkowej, czyli poziomu, który umożliwia załatwienie każdej sprawy administracyjnej drogą elektroniczną. Najczęściej świadczoną e-usługą przez administrację samorządową jest udzielanie informacji publicznych[3]. W tym zakresie działalność e-administracji samorządowej reguluje szereg ustaw: o dostępie do informacji publicznej[4], ochronie danych osobowych[5] i ochronie informacji niejawnych[6]. Oczywiście kluczowym aspektem w postępowaniach prowadzonych drogą elektroniczną jest zapewnienie bezpieczeństwa przepływu informacji i danych przez ten kanał. Z tego względu w niniejszym artykule poruszono następujące zagadnienia: podpis elektroniczny, profil zaufany oraz **bezpieczeństwo elektronicznego obiegu dokumentów**. Podpis elektroniczny został powołany ustawą z 18.09.2001 r. o podpisie elektronicznym, jednak liczne obwarowania prawne zahamowały jego rozwój i popyt na niego. Zgodnie z art. 5 powyższej ustawy tylko „**bezpieczny podpis elektroniczny** weryfikowany przy pomocy kwalifikowanego certyfikatu wywołuje skutki prawne określone ustawą, jeżeli został złożony w okresie ważności tego certyfikatu”. Podpis elektroniczny jest przydatnym narzędziem z tego względu, że w chwili poświadczenia elektronicznego następuje znakowanie czasem[7], każda zmiana zostaje wychwycona i można ją poddać weryfikacji.

Natomiast bezpłatną metodę potwierdzania tożsamości w elektronicznych kontaktach z administracją[8] stanowi **profil zaufany** na ePUAP, czyli elektronicznej platformie umożliwiającej wymianę dokumentów elektronicznych między urzędem a klientami z uwzględnieniem wymagań bezpieczeństwa, procedur urzędowych i neutralności technologicznej[9]. Planuje się zwiększenie poziomu bezpieczeństwa profilu zaufanego oraz

[2] Art.39[1], *Ustawa z 14.06.1960 r. Kodeks postępowania administracyjnego* [Dz. U. 1960 nr 30 poz. 168].
[3] V. Szymanek (red.), Raport: *Społeczeństwo informacyjne w liczbach*, Warszawa 2012, s. 92.
[4] *Ustawa z 6.09.2001 r. o dostępie do informacji publicznej* [Dz. U. 2001 nr 112 poz. 1198].
[5] *Ustawa z 29.08.1997 r. o ochronie danych osobowych*, [Dz. U. 1997 nr 133 poz. 883].
[6] *Ustawa z 5.08. 2010 r. o ochronie informacji niejawnych*, [Dz. U. 2010 nr 182 poz. 1228].
[7] Art. 3, ustawa z *18.09.2001 r. o podpisie elektronicznym*, [Dz. U. 2001 nr 130 poz. 1450].
[8] *Profil zaufany - bezpłatna metoda potwierdzania tożsamości w elektronicznych kontaktach z administracją*, http://epuap.gov.pl/wps/portal/!ut/p/a1/04_Sj9CPykssy0xPLMnMz0vMAfGjzOINLY1MDI2CDbwswlycDDzDQoJCvN3CjAxCDPQLsh0VAdV64x8!/ [dostęp: 20.04.2014].
[9] *Ibidem*.

wprowadzenie nowych metod udostępniania hasła[10]. Innym zadaniem sformułowanym w Programie Zintegrowanej Informatyzacji Państwa jest „dostarczenie jednolitych, ustandaryzowanych i w pełni bezpiecznych usług uwierzytelniania dla systemów administracji”[11]. Powyższe narzędzia umożliwiają załatwienie sprawy administracyjnej bez wychodzenia z domu, jednocześnie poświadczenie dokumentów z ich wykorzystaniem jest równoważne z własnoręcznym podpisem. Zatem wymogi bezpieczeństwa w odniesieniu do podpisu elektronicznego, profilu zaufanego, czy elektronicznego obiegu dokumentów ograniczają się do minimalnych wymagań dla systemów teleinformatycznych określonych w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne w art. 3 jako „zespół wymagań organizacyjnych i technicznych, których spełnienie przez system teleinformatyczny umożliwia wymianę danych z innymi systemami teleinformatycznymi oraz zapewnia dostęp do zasobów informacji udostępnianych za pomocą tych systemów”[12] oraz minimalnych wymagań dla wymiany informacji w postaci elektronicznej, tzn. „zespołu cech informacyjnych, w tym identyfikatorów oraz odpowiadającym im charakterystyk elementów strukturalnych przekazu informacji”[13]. Zgodnie z Programem Zintegrowanej Informatyzacji Państwa „w każdym przypadku obowiązywać będą wzajemnie przenikające się wymagania dla systemów teleinformatycznych w odniesieniu do interoperacyjności, bezpieczeństwa (w tym zaufania), technologii”[14].

Kolejną kwestią wymagającą omówienia są zachodzące zmiany w społeczności lokalnej, tzn. przeobrażanie się modelu społeczeństwa informacyjnego w **społeczeństwo sieciowe**[15]. Zaistniały proces jest ryzykowny ze względu na grupę osób wykluczonych cyfrowo. Przewiduje się, że „w 2020 roku 90 % zawodów będzie wymagało kompetencji cyfrowych”[16]. **Wykluczenie cyfrowe** grupy osób w społeczności lokalnej oznaczać może ich wycofanie z życia i działalności tej wspólnoty. W końcu e-administracja stwarza możliwości lepszego doinformowania mieszkańców, zwiększenia stopnia ich partycypacji i wpływu na to, co się dzieje w gminie. Zatem pozbawienie tych przywilejów grupy osób będzie

[10] *Program Zintegrowanej Informatyzacji Państwa (dalej PZIP),* Warszawa 2013, s. 65.
[11] *Ibidem*.
[12] Art. 4, pkt 9, *Ustawa z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne* [Dz. U. 2005 nr 64 poz. 565].
[13] *Ibidem*, art. 3, pkt 10.
[14] PZIP, s. 58.
[15] Społeczeństwo sieciowe zakłada wykorzystanie technologii ICT na każdej płaszczyźnie życia, dlatego działalność i integracja uczestników tej społeczności odbywa się w sieci, za pomocą elektronicznych systemów przetwarzania danych.
[16] *Cyfrowa Polska wspiera PCRS*, http://www.mwi.pl/aktualnosci/270-cyfrowa-polska-wspiera-pcrs.html [dostęp: 20.04.2014].

dyskryminacją cyfrową i poważnym zagrożeniem dla funkcjonowania tej wspólnoty, a także dla rozwoju e-administracji samorządowej. Dlatego pomysł edukacji cyfrowej w ramach projektu Polska Cyfrowa Równych Szans narodził się z oddolnej inicjatywy. Pomoc we wdrożeniu pokolenia 50+ do świata wirtualnego zaoferowali wolontariusze, liderzy społeczności lokalnych zwani **Latarnikami Polski Cyfrowej**[17].

W celu skonkretyzowania wpływu e-usług administracji samorządowej na bezpieczeństwo społeczności lokalnych, warto przytoczyć dobre praktyki i projekty wzmacniające poczucie bezpieczeństwa mieszkańców i ich zaufanie do e-administracji. Podstawowa kategoria e-usług w badanym obszarze to bezpieczeństwo i powiadamianie ratunkowe. W trakcie realizacji jest projekt z obszaru e-bezpieczeństwa w województwie podlaskim, który polega na budowie informatycznego systemu wspomagania zarządzania bezpieczeństwem i funkcjonowania zarządzania kryzysowego w województwie podlaskim.[18] „Zostanie on zrealizowany przez utworzenie wspólnego, kompleksowego systemu integrującego, standaryzującego i porządkującego informacje organów i służb województwa podlaskiego odpowiadających za bezpieczeństwo, funkcjonujących w ramach Zarządzania Kryzysowego Wojewody Podlaskiego (**e-Bezpieczeństwo**)"[19]. Do planowanych działań zalicza się powiadamianie obywateli o zagrożeniach lokalnych z wykorzystaniem technologii ICT, rozbudowę systemu numeru 112 o dodatkowe usługi np. SMS do zgłaszającego, z zapytaniem: co się dzieje oraz usługę wspomagającą zarządzanie ryzykiem powodziowym[20]. Serwis internetowy **ujawnij.pl** również przyczynia się do poprawy bezpieczeństwa i porządku publicznego, umożliwia sprawne i anonimowe zawiadomienie o zaistniałych zagrożeniach. Inna e-usługa wzmacniająca bezpieczeństwo w Gdańsku to **Mapa porządku**, czyli aplikacja służąca mieszkańcom do zgłaszania wszelkich sygnałów związanych z czystością w miejscach publicznych i porządkiem[21]. Kolejnym wdrożonym projektem, bazującym na mapie porządku, jest interaktywne narzędzie do zgłaszania i obserwowania usterek miejskich, niepokojących zdarzeń w tym mieście, zwane **Systemem zgłaszania miejskich usterek**. Zaś w Warszawie jako dobrą praktykę wyróżnia się

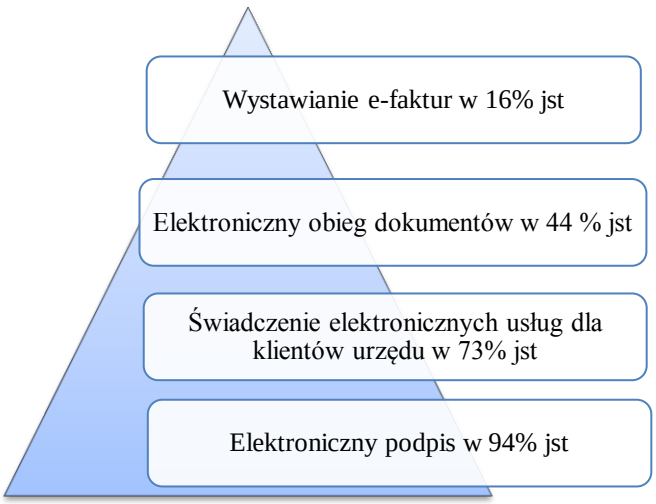
[17] Ministerstwo Administracji i Cyfryzacji, *Pierwszy krok w cyfrowym świecie - Latarnicy przeszkolili z obsługi internetu już ponad 100 tysięcy "Starszaków"*, https://mac.gov.pl/aktualnosci/pierwszy-krok-w-cyfrowym-swiecie-latarnicy-przeszkolili-z-obslugi-internetu-juz-ponad [dostęp: 20.04.2014].
[18] Cyfrowy Urząd, *Ogólny opis projektu administracji rządowej województwa podlaskiego "Wdrażanie elektronicznych usług dla ludności województwa podlaskiego - część II, administracja rządowa"*, http://cu2.bialystok.uw.gov.pl/Default.aspx [dostęp: 20.04.2014].
[19] *Ibidem*.
[20] Ministerstwo Administracji i Cyfryzacji, *E-usługi*, https://mac.gov.pl/e-uslugi/bezpieczenstwo-i-powiadamianie-ratunkowe [dostęp: 20.04.2014].
[21] *Otwarte dane*, http://www.gdansk.pl/otwartygdansk,1844.html [dostęp: 20.04.2014].

„**inwestmapę**", czyli „wiarygodne źródło informacji o sytuacji w mieście"[22]. Ta e-usługa polega na „wspomaganiu procesu koordynacji, poprzez przedstawienie lokalizacji planowanych i realizowanych inwestycji, w oparciu o miejskie zasoby informacji przestrzennej, cyfrową bazę i serwis internetowy „**e-Inwestycje**"[23]. Inną dobrą praktyką wzmacniającą poczucie bezpieczeństwa i zaufanie mieszkańców okazuje się rybnicka elektroniczna karta miejska, czyli **e-bilet**, za pomocą którego można dokonać opłat miejskich i skarbowych, załatwić sprawę w urzędzie przy pomocy Internetu.[24] Projekt ten zapewnia późniejszą informację zwrotną i warunkuje analizy o potrzebach, preferencjach i oczekiwaniach mieszkańców Rybnika oraz przyczynia się do poprawy komunikacji i warunków dostępu do informacji publicznej i e-usług[25].

Narzędzia informatyczne warunkujące efektywne funkcjonowanie e-administracji samorządowej są stosowane w 99% jednostek samorządu terytorialnego[26]. E-usługi udostępniane przez samorządy są rozproszone, powoduje to dezorientację i chaos informacyjny wśród obywateli. P. Laskowski zwraca uwagę na to, że „brak standardów podnosi poziom skomplikowania i wprowadza zamęt"[27]. Z racji tego, ze samorządy świadczą większość usług publicznych (około 70%), konieczne jest stworzenie ustandaryzowanych e-usług, ich jednorodnego katalogu, banku dobrych praktyk i wzorców oraz zintegrowanie platform regionalnych z ePUAP.

[22] Baza dobrych praktyk, *Internetowy serwis "eInwestycje" - skuteczne narzędzie wspomagające proces koordynacji inwestycji i remontów stołecznych dróg*, http://www.dobrepraktyki.pl/index.php?p1=2&p2=4&art=149 [dostęp: 20.04.2014].
[23] Baza dobrych praktyk, *Internetowy serwis …*
[24] Baza dobrych praktyk, *Elektroniczna karta miejska i publiczne punkty dostępu do Internetu w Mieście Rybnik*, http://www.dobrepraktyki.pl/index.php?p1=3&p2=11&art=80 [dostęp: 20.04.2014].
[25] Baza dobrych praktyk, *E-bilet w ramach Elektronicznej Karty Miejskiej*, http://www.dobrepraktyki.pl/index.php?p1=2&p2=4&art=41 [dostęp: 20.04.2014].
[26] K. Piróg (red.), *Raport Barometr rozwoju instytucjonalnego jednostek samorządu terytorialnego*, Warszawa 2013, s. 42.
[27] P. Laskowski, *Samorządowa e-administracja*, s. 6.

Rys 1: Przykładowe narzędzia informatyczne stosowane w jst z uwzględnieniem powszechności ich występowania w skali procentowanej

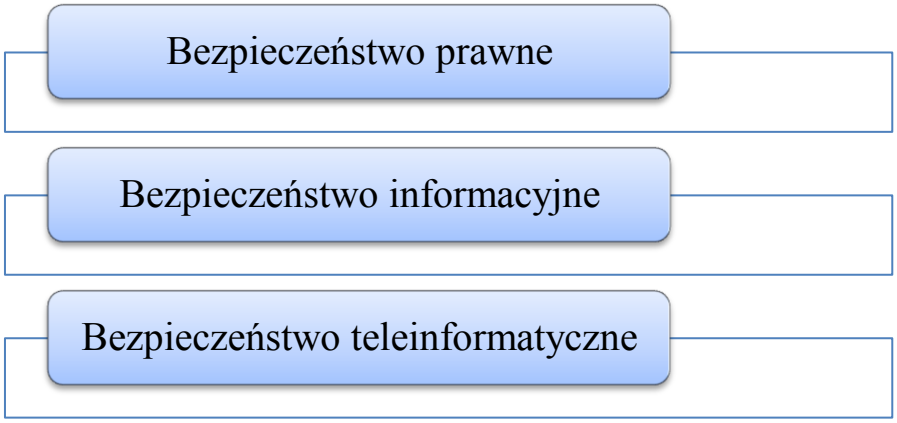


Źródło: K. Piróg, Raport (red.), *Barometr rozwoju instytucjonalnego jednostek samorządu terytorialnego*, Warszawa 2013, s. 43.

Polityka bezpieczeństwa w odniesieniu do e-administracji samorządowej

Gwarantem i determinantą korzystania z e-usług przez społeczności lokalne i sprawnego funkcjonowania e-administracji samorządowej jest jej bezpieczeństwo. Polityka ochrony bezpieczeństwa cyberprzestrzeni RP (dalej zwana polityką) z dnia 25.06.2013 r. stanowi wskazówkę oraz wyznacznik działań dla e-administracji samorządowej. Osiągnięcie przez nią akceptowalnego poziomu bezpieczeństwa, czyli celu strategicznego polityki, stwarza warunki do rozwoju i ewolucji w pełni z osiągniętego w 2011 poziomu interakcji jednokierunkowej do poziomu interakcji dwukierunkowej umożliwiającej załatwienie sprawy administracyjnej drogą elektroniczną. Bezpieczeństwo e-administracji samorządowej można zobrazować następująco:

Rys. 2 Komponenty bezpieczeństwa e-administracji samorządowej



Źródło: Opracowanie własne.

Części składowe bezpieczeństwa e-administracji samorządowej są wobec siebie współzależne, zahamowanie rozwoju bezpieczeństwa teleinformatycznego blokuje pozostałe. Zaprezentowana powyżej klasyfikacja umożliwia kompleksowe zrozumienie całego procesu zapewniania i wprowadzania e-standardu bezpieczeństwa w kontekście e-usług administracji samorządowej. W polityce **bezpieczeństwo cyberprzestrzeni** zdefiniowano jako „zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych, mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni”[28]. Kwestia bezpieczeństwa cyberprzestrzeni jest o tyle problematyczna, że trudno stwierdzić, czy minimalne wymagania wobec systemów teleinformatycznych okażą się dostateczne. Z drugiej strony szczegółowe określenie tych wymogów w prawie może doprowadzić do stagnacji i ograniczenia elastyczności w dostosowaniu się do zmieniającego się otoczenia. Ta dychotomia skutkuje tworzeniem i wdrażaniem ustandaryzowanych i podstawowych mechanizmów zabezpieczeń, które nie stanowią barier dla hakerów, a ryzyko cyberataku redukują w sposób niewspółmierny do wielkości i częstotliwości występowania zagrożeń. Według raportu „Risk Index 2013” firmy Lloyd’s, strach przedsiębiorców przed cyberprzestępczością uplasował się na miejscu trzecim zaraz po wysokich podatkach i utracie klientów[29]. Obawy firm, które brały udział w badaniu, są uzasadnione wzrostem cyberataków w 2013 r. Wyniki badań z 2011 r. pokazują, że amerykańscy przedsiębiorcy boją się

[28] *Uchwała RM z 25.06.2013 r. w sprawie Polityki Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej* (dalej polityka), s. 6.
[29] *Lloyd’s Risk Index 2013*, http://www.lloyds.com/~/media/Files/News%20and%20Insight/Risk%20Insight/Risk%20Index%202013/Report/Lloyds%20Risk%20Index%202013report100713.pdf [dostęp: 20.04.2014].

cyberataków bardziej niż terroryzmu[30]. W Polsce „rok 2013 pod względem liczby otrzymanych zgłoszeń (8817) i obsłużonych incydentów (5670) okazał się rekordowy w stosunku do lat poprzednich"[31].

Obecnie bezpieczeństwo cyberprzestrzeni stanowi jeden z priorytetów w obszarze bezpieczeństwa państwa[32]. Nie można wyeliminować zagrożeń z cyberprzestrzeni albo się od nich odizolować, dlatego prowadzone analizy mają na celu jedynie obniżenie wpływu ataków na system teleinformatyczny oraz wskazanie potencjalnych zagrożeń. Następnie na podstawie przeprowadzonej analizy wypracowuje się minimalne standardy bezpieczeństwa[33]. Ustalony **e-standard bezpieczeństwa** stanowi wypadkową mechanizmów: ochronnych, niwelujących podatność infrastruktury teleinformatycznej na cyberataki, zapobiegających i zwalczających zagrożenia. Według M. Ganczar „serwisy internetowe urzędów administracji publicznej nie spełniają żadnych standardów, zdecydowana większość urzędów administracyjnych traktuje obowiązek udzielenia informacji publicznej jako zło konieczne, do którego realizacji zostały przymuszone"[34].

Polityka zakłada funkcjonowanie w każdej jednostce organizacyjnej administracji rządowej pełnomocnika ds. bezpieczeństwa cyberprzestrzeni, natomiast w administracji samorządowej zgodnie z raportem Społeczeństwo informacyjne w liczbach z 2012 r. „w 64% gmin obsługą informatyczną urzędu zajmuje się jedna osoba. W kolejnych 12% – dwie osoby, co razem daje ¾ urzędów gminnych z jedno- lub dwuosobowym zespołem informatyków"[35]. Wobec braków kadrowych można zastosować takie rozwiązania. jak zlecanie ochrony portali i stron internetowych urzędów firmom zewnętrznym na podstawie porozumienia, które należałoby szczegółowo określić w prawie albo dostosowanie zarobków ekspertów IT do ich kompetencji i zakresu pracy. W jednostkach samorządu terytorialnego wojewoda kontroluje działanie systemów teleinformatycznych „pod względem zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych lub minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej"[36] na podstawie art. 25

[30] *State of security survey 2011*, http://www.symantec.com/content/en/us/about/media/pdfs/symc_state_of_security_2011.pdf?om_ext_cid=biz_socmed_web_2011Aug_worldwide_securitysurvey [dostęp: 20.04.2014].
[31] *Raport o stanie bezpieczeństwa cyberprzestrzeni w roku 2013*, cert.gov.pl, s. 5.
[32] *Polityka*, s. 5.
[33] *Ibidem*, s. 13.
[34] M. Ganczar, *Nowa jakość usług publicznych dla obywateli i przedsiębiorców*, Warszawa 2009, s. 158.
[35] V. Szymanek, *op. cit.*, s. 88.
[36] Art. 15, *ustawa z dnia 17.02.2005 r. o informatyzacji działalności ...*

ustawy z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

Kooperacja jednostek samorządu terytorialnego z organizacjami pozarządowymi w zakresie e-bezpieczeństwa

Administracja samorządowa z racji tego, że jest najbliżej obywatela, ma możliwość bezpośredniego kontaktu, zbadania poczucia bezpieczeństwa i poznania problemów mieszkańców. Dzięki temu tworzone e-usługi są zorientowane na użytkowników i ich potrzeby. Obecnie technologie ICT mają znaczący wpływ na budowanie relacji między jednostkami samorządu terytorialnego a obywatelami, czyli adresatami e-usług. W związku z postępem technologicznym, coraz młodsze pokolenia korzystają z Internetu, natomiast pokolenie 55+ postrzega się z reguły jako osoby wykluczone cyfrowo. W powyższych obszarach sformułowanych jako zagrożenia - **bezpieczeństwo dzieci w sieci** oraz **wykluczenie cyfrowe**, administracja samorządowa współpracuje z organizacjami pozarządowymi.

Inicjatywy organizacji pozarządowych koncentrują się głównie na działalności edukacyjnej i uświadamiającej w formie szkoleń stacjonarnych, jak również e-learningu. Przykładowy projekt z zakresu bezpieczeństwa w sieci to cykl 13 warsztatów pod hasłem „Bezpieczni w sieci" przeprowadzonych w pięciu warszawskich gimnazjach. Projekt fundacji „La Strada" został dofinansowany przez m. st. Warszawa. Do tej inicjatywy przyłączyli się uczniowie, rodzice i nauczyciele, w sumie 300 osób, które zostały poinformowane o zagrożeniach internetowych[37]. Na uwagę zasługuje także Cyfrowa Wyprawka dofinansowana z funduszy UE stworzona przez fundację „Panoptykon". Adresatami projektu są osoby prowadzące zajęcia z dziećmi. Na platformie zamieszczono materiały uświadamiające np. jak unikać zagrożeń i chronić swoją prywatność[38]. Forma materiałów jest przystosowana do 45-minutowych lekcji, które umożliwiają przekaz wiedzy w pigułce, rozwiązanie ćwiczeń sprawdzających. Podział na tematy został ustalony w oparciu o kryterium wiekowe odbiorców. „Panoptykon" sformułował również podstawowe zasady ochrony przed cyberzagrożeniami:

- Aktualizuj oprogramowanie antywirusowe, które ochroni Cię przed złośliwym

[37] La Strada, *Realizowane projekty*, http://www.strada.org.pl/index.php/pl/la-strada-w-dzialaniu/realizowane-projekty [dostęp: 20.04.2014].
[38] *O cyfrowej wyprawce*, http://cyfrowa-wyprawka.org/projekt [dostęp: 20.04.2014].

oprogramowaniem i utratą danych,

- Ostrożnie korzystaj z niezabezpieczonych sieci Wi-Fi, a przynajmniej upewnij się, że w pasku adresu widnieje „https://", które oznacza, że strona korzysta z szyfrowanego połączenia,

- Chroń swoje hasło, używaj różnych haseł do różnych usług, sprawdzaj czy witryna, na której się logujesz ma certyfikat bezpieczeństwa (symbol kłódki),

- Zadbaj o swoją politykę prywatności, czytaj uważnie regulaminy w trosce o swój wizerunek,

- Pamiętaj, że z sieci nic nie znika[39].

Zgodnie z Diagnozą Społeczną z 2011 r. „najważniejsze bariery upowszechnienia wykorzystania komputerów i Internetu to przede wszystkim brak motywacji do korzystania, wynikający po części również z braku wiedzy i umiejętności"[40]. Przykładowym projektem zwalczającymi wykluczenie cyfrowe w ramach działań administracji samorządowej i organizacji pozarządowych jest „**Przeciwdziałanie wykluczeniu cyfrowemu – e-inclusion**", który polega na „wsparciu edukacji cyfrowej osób zagrożonych wykluczeniem cyfrowym oraz umożliwienie im dostępu do Internetu"[41]. Identyfikację wykluczonych cyfrowo mieszkańców gminy przeprowadzały jednostki samorządu terytorialnego przy wsparciu organizacji pozarządowych[42].

Podsumowanie

Wprowadzenie **e-standardu** rozumianego jako jednolity standard świadczenia usług w podobny sposób ułatwi komunikację administracji samorządowej z obywatelami, przyspieszy postępowanie administracyjne i poprawi jakość e-usług. Wyznaczony e-standard powinien uwzględniać aspekt konsultacyjny, ponieważ e-administracja samorządowa to „technologiczny współpartner społeczności lokalnych"[43]. Dlatego komplementarnym

[39] A. Obem, *Jak zadbać o bezpieczeństwo i prywatność w cyfrowym świecie?*, [w:] Przewodnik internetowy – poznaj, korzystaj, twórz, Centrum Cyfrowe, s. 48.
[40] J. Czapiński, T. Panek, *Diagnoza społeczna 2011 warunki i jakość życia Polaków raport*, Warszawa 2012, s. 327.
[41] Ministerstwo Administracji i Cyfryzacji, *Państwo 2.0 Nowy start dla e-administracji*, Ministerstwo administracji i Cyfryzacji, Warszawa 2011, s. 67-69.
[42] *Ibidem*.
[43] P. Laskowski, *op. cit.*, s. 6.

uzupełnieniem e-usług administracji samorządowej są „elektroniczne mechanizmy demokratycznej kontroli”[44], to znaczy takie narzędzia jak fora internetowe ułatwiające nawiązanie dialogu społecznego, ankiety online umożliwiające badanie jakości e-usług i obsługi w urzędzie, zamieszczane komentarze na stronach internetowych, nadsyłane uwagi do projektów e-usług drogą elektroniczną, a także informacje zwrotne wychwytywane za pomocą e-usług np. powyżej omówionego e-biletu.

Według P. Laskowskiego „zelektronizowana administracja samorządowa powinna stanowić źródło pierwotnych danych dla administracji rządowej”[45]. Z tego względu osiągnięcie interoperacyjności możliwe jest dzięki współpracy e-administracji rządowej z samorządową, korzystaniu z takich e-usług jak np. ePUAP przez wszystkie jednostki administracyjne w celu minimalizacji kosztów i ujednolicenia standardów jakości świadczonych e-usług oraz poziomu e-bezpieczeństwa. Zatem politykę bezpieczeństwa e-administracji samorządowej należy postrzegać jako „zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania”[46], których celem jest osiągnięcie akceptowalnego poziomu, dzięki realizacji minimalnych wymogów z zakresu bezpieczeństwa e-usług.

Obecnie główne wyzwanie dla e-administracji samorządowej stanowi ograniczenie takich zagrożeń jak wykluczenie cyfrowe oraz cyberprzestępczość. Podjęte w tym zakresie profilaktyczne działania to przede wszystkim edukowanie i uświadamianie. Przytoczone powyżej projekty realizowane we współpracy z organizacjami pozarządowymi przyczyniają się do zwiększania zaufania społeczności lokalnych do e-administracji samorządowej i jej e-usług oraz do poprawy bezpieczeństwa w sieci użytkowników. Jednak powyższe działania to zaledwie pierwszy krok w kształtowaniu akceptowalnego poziomu e-bezpieczeństwa przez administrację samorządową, społeczności lokalne oraz organizacje pozarządowe.

[44] J. Janowski, *Administracja elektroniczna,* Wyd. MUNICIPIUM, Warszawa 2009, s. 14.
[45] P. Laskowski, *op. cit.*, s. 7.
[46] § 1. pkt 15, *rozporządzenie RM z 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.*

Wykaz źródeł:

Akty normatywne

Uchwała RM z 25.06.2013 r. w sprawie Polityki Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej.

Ustawa z 14.06.1960r. Kodeks postępowania administracyjnego, Dz.U. 1960 nr 30 poz. 168.

Ustawa z 29.08. 1997 r. o ochronie danych osobowych, Dz.U. 1997 nr 133 poz. 883.

Ustawa z 18.09.2001 r. o podpisie elektronicznym, Dz.U. 2001 nr 130 poz. 1450.

Ustawa z 6.09.2001 r. o dostępie do informacji publicznej, Dz.U. 2001 nr 112 poz. 1198.

Ustawa z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2005 nr 64 poz. 565.

Ustawa z 5.08. 2010 r. o ochronie informacji niejawnych, Dz.U. 2010 nr 182 poz. 1228.

Rozporządzenie RM z 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2012
nr 0 poz. 526.

Publikacje zwarte i artykuły naukowe

Ganczar M., *Nowa jakość usług publicznych dla obywateli i przedsiębiorców*, Warszawa 2009.

Urban A., *Bezpieczeństwo społeczności lokalnych*, Warszawa 2009.

Janowski J., *Administracja elektroniczna*, Warszawa 2009.

Artykuły internetowe

Baza dobrych praktyk, Elektroniczna karta miejska i publiczne punkty dostępu do Internetu w Mieście Rybnik,
http://www.dobrepraktyki.pl/index.php?p1=3&p2=11&art=80 [dostęp: 20.04.2014].

Baza dobrych praktyk, E-bilet w ramach Elektronicznej Karty Miejskiej, http://www.dobrepraktyki.pl/index.php?p1=2&p2=4&art=41 [dostęp: 20.04.2014].
Baza dobrych praktyk, Internetowy serwis "eInwestycje" - skuteczne narzędzie wspomagające proces koordynacji inwestycji i remontów stołecznych dróg, http://www.dobrepraktyki.pl/index.php?p1=2&p2=4&art=149 [dostęp: 20.04.2014].

Czapiński J., Panek T., *Diagnoza społeczna 2011 warunki i jakość życia Polaków raport*, Warszawa 2011.

Cyfrowa Polska wspiera PCRS, http://www.mwi.pl/aktualnosci/270-cyfrowa-polska-wspiera-pcrs.html [dostęp: 20.04.2014].

Cyfrowy Urząd, Ogólny opis projektu administracji rządowej województwa podlaskiego "Wdrażanie elektronicznych usług dla ludności województwa podlaskiego - część II, administracja rządowa", http://cu2.bialystok.uw.gov.pl/Default.aspx [dostęp: 20.04.2014].

Laskowski P., *Samorządowa e-administracja*.

La Strada, Realizowane projekty, http://www.strada.org.pl/index.php/pl/la-strada-w-dzialaniu/realizowane-projekty [dostęp: 20.04.2014].

Lloyd's Risk Index 2013, http://www.lloyds.com/~/media/Files/News%20and%20Insight/Risk%20Insight/Risk%20Index%202013/Report/Lloyds%20Risk%20Index%202013report100713.pdf [dostęp: 20.04.2014]. 30 State of security survey 2011, http://www.symantec.com/content/en/us/about/media/pdfs/symc_state_of_security_2011.pdf?om_ext_cid=biz_socmed_web_2011Aug_worldwide_securitysurvey [dostęp: 20.04.2014].

Ministerstwo Administracji i Cyfryzacji, E-usługi, https://mac.gov.pl/e-uslugi/bezpieczenstwo-i-powiadamianie-ratunkowe [dostęp: 20.04.2014].

Ministerstwo Administracji i Cyfryzacji, Państwo 2.0 Nowy start dla e-administracji, Ministerstwo administracji i Cyfryzacji, Warszawa 2011.

Ministerstwo Administracji i Cyfryzacji, Pierwszy krok w cyfrowym świecie - Latarnicy przeszkolili z obsługi internetu już ponad 100 tysięcy "Starszaków", https://mac.gov.pl/aktualnosci/pierwszy-krok-w-cyfrowym-swiecie-latarnicy-przeszkolili-z-obslugi-internetu-juz-ponad [dostęp: 20.04.2014].

Obem A., Fundacja Panoptykon, *Jak zadbać o bezpieczeństwo i prywatność w cyfrowym świecie?*, [w:] *Przewodnik internetowy – poznaj, korzystaj, twórz, Centrum Cyfrowe*.

Piróg K. (red.), *Raport Barometr rozwoju instytucjonalnego jednostek samorządu terytorialnego*, Warszawa 2013.

Program Zintegrowanej Informatyzacji Państwa, Ministerstwo Administracji i Cyfryzacji, Warszawa, listopad 2013.

Profil zaufany - bezpłatna metoda potwierdzania tożsamości w elektronicznych kontaktach z administracją, http://epuap.gov.pl/wps/portal/!ut/p/a1/04_Sj9CPykssy0xPLMnMz0vMAfGjzOINLY1MDI2CDbwswlycDDzDQoJCvN3CjAxCDPQLsh0VAdV64x8!/ [dostęp: 20.04.2014].

Otwarte dane, http://www.gdansk.pl/otwartygdansk,1844.html [dostęp: 20.04.2014].

Raport o stanie bezpieczeństwa cyberprzestrzeni w roku 2013, cert.gov.pl.

V. Szymanek (red.), *Raport Społeczeństwo informacyjne w liczbach,* Warszawa 2012.