**Zygmunt Mazur, Hanna Mazur, Teresa Mendyk-Krajewska**

# Problemy elektronicznej realizacji usług w administracji publicznej i ochronie zdrowia

Ekonomiczne Problemy Usług nr 123, 159-168

2016

Ekonomiczne Problemy Usług nr 123

ISSN: 1896-382X | www.wnus.edu.pl/pl/epu/
DOI: 10.18276/epu.2016.123-15 | strony: 159-168

*ZYGMUNT MAZUR, HANNA MAZUR, TERESA MENDYK-KRAJEWSKA*
Politechnika Wrocławska[1]

# PROBLEMY ELEKTRONICZNEJ REALIZACJI USŁUG W ADMINISTRACJI PUBLICZNEJ I OCHRONIE ZDROWIA

**Streszczenie**

Informatyzacja gospodarki, dokonywana dynamicznie w ostatnich latach, obejmuje swoim zakresem coraz więcej obszarów. Gromadzone dane to już nie tylko dane osobowe obywateli, ale także finansowe, medyczne, biznesowe itp. Tymczasem stan bezpieczeństwa systemów informatycznych jest niezadowalający. Celem artykułu jest przedstawienie aktualnych problemów związanych z budową cyfrowych rejestrów danych oraz systemów teleinformatycznych niezbędnych do realizacji usług w administracji publicznej i ochronie zdrowia.
**Słowa kluczowe:** e-administracja, e-zdrowie, e-usługa, bezpieczeństwo.

## Wprowadzenie

Wizja sprawnie działającego państwa z rozwiniętymi usługami realizowanymi drogą elektroniczną (e-usługami) jest możliwa do zrealizowania dzięki powszechnemu wykorzystywaniu technologii teleinformatycznych. Wraz z ich rozwojem budowane są odpowiednie rejestry i systemy informatyczne oraz opracowywane są odpowiednie akty prawne. Konieczne jest doskonalenie obsługi oferowanych e-usług, których lista powinna być stale poszerzana, by w jak największym zakresie umożliwiać obywatelom kontaktowanie się z jednostkami realizującymi zadania publiczne oraz by coraz więcej procesów biznesowych można było wykonywać online. W artykule przedstawiono aktualne problemy związane z budową cyfro-

[1] Wydział Informatyki i Zarządzania, Katedra Informatyki.

wych rejestrów danych i systemów teleinformatycznych niezbędnych do realizacji usług w administracji publicznej i ochronie zdrowia.

W 2014 r. z usług polskiej e-administracji korzystało 92,4% przedsiębiorstw, przy czym tę formę kontaktu stosowały prawie wszystkie firmy duże i średnie. W 2015 roku z usług e-administracji korzystało 26,6% osób w wieku 16–74 lat (GUS 2015). W prawie 78% gospodarstw domowych jest co najmniej jeden komputer, a 76% ma dostęp do Internetu. Wiele osób korzysta z dostępu do sieci w pracy, w szkole i w miejscach użyteczności publicznej.

W celu ułatwienia obywatelom korzystania z e-usług oraz zwiększenia liczby podmiotów je oferujących opracowano system ePUAP (elektroniczna Platforma Usług Administracji Publicznej), dostarczający jednolite środowisko, z założenia łatwe i ergonomiczne w obsłudze.

Duże znaczenie dla rozwoju innowacyjności w kraju oraz rozwoju społeczeństwa informacyjnego ma udostępnianie w jednym miejscu danych pochodzących z rejestrów od różnych podmiotów. Zadanie takie spełnia Centralne Repozytorium Informacji Publicznej. W serwisie danepubliczne.gov.pl udostępniane są dane, raporty i statystyki z rejestrów publicznych różnych dostawców (m.in. GUS, ministerstw, Komendy Głównej Policji, Komendy Głównej Państwowej Straży Pożarnej), np. raporty Ministerstwa Administracji i Cyfryzacji, dane o szkołach wyższych i ich finansach czy lista rzeczoznawców majątkowych. W styczniu 2015 r. udostępnionych było 314 zbiorów. Niestety, polska gospodarka pod względem poziomu ucyfrowienia zajmuje w klasyfikacji Unii Europejskiej jedno z ostatnich miejsc (Europa 2015).

## 1. Elektroniczna realizacja usług w administracji publicznej

Obecnie uruchomiono wiele przedsięwzięć i przeznaczono duże środki finansowe na działania zmierzające do rozwoju e-usług w administracji publicznej i do budowy odpowiednich systemów informatycznych zapewniających niezawodne funkcjonowanie urzędów.

Program Operacyjny Innowacyjna Gospodarka (POIG) podzielony jest na 9 osi priorytetowych o różnych szczegółowych działaniach. Celem 7. osi „Społeczeństwo informacyjne – budowa elektronicznej administracji", realizowanej w latach 2007–2013, była poprawa warunków prowadzenia działalności gospodarczej poprzez zwiększenie dostępności zasobów informacyjnych administracji publicznej oraz rozwój elektronicznych usług publicznych dla obywateli i przedsiębiorców. Zadania 8. osi POIG „Społeczeństwo informacyjne – zwiększanie innowacyjności gospodarki" dotyczyły stymulowania rozwoju gospodarki elektronicznej poprzez wspieranie tworzenia innowacyjnych e-usług i nowych rozwiązań elektronicznego biznesu oraz zmniejszania technologicznych, ekonomicznych i mental-

nych barier wykorzystywania e-usług. W ramach POIG w grudniu 2015 roku ukończono portal Inventorum, udostępniający dane z różnych źródeł, które dotyczą projektów i przedsiębiorstw innowacyjnych, instytucji naukowych oraz ekspertów i konferencji. W 2015 r. wdrożono także System Digitalizacji Akt i w październiku w postaci cyfrowej istniało już 12 749 tomów akt karnych (SDA 2015).

W celu ułatwienia kontaktów administracji z przedsiębiorcami opracowano Elektroniczny Punkt Kontaktowy (ePK) umożliwiający szybką realizację spraw, z którymi przedsiębiorcy zgłaszają się do urzędów. W wielojęzycznym serwisie biznes.gov.pl znajduje się wykaz e-usług oraz wzory wykorzystywanych formularzy.

W ministerstwach odpowiedzialnych za rozwój e-usług stosuje się mieszany model utrzymania systemów informatycznych – część usług jest realizowana wewnątrz odpowiednich podmiotów (ministerstw), a część jest kontraktowana na zewnątrz. W przypadku Ministerstwa Gospodarki (MG), które odpowiada za ePK i serwis biznes.gov.pl, zadania takie, jak np. bieżące monitorowanie usług i aktualności treści publikowanych w serwisie oraz współpraca z właściwymi organami w zakresie publikowanych treści – są realizowane przez MG, natomiast realizacja prac rozwojowych w zakresie funkcjonalnym i technicznym zlecana jest na zewnątrz (POIG 2015). Taki model często bywa przyczyną problemów przy tworzeniu, rozbudowie czy integracji systemów. W raporcie z 2014 r.[2] dotyczącym przebiegu wdrożenia funkcjonalności Profil Zaufany oraz Dostawca Tożsamości w ramach systemu ePUAP stwierdzono niedociągnięcia w kwestii wydajności i bezpieczeństwa rozwiązania. Stwierdzono m.in. nieuzasadnione przekazanie firmie zewnętrznej kodów źródłowych Profilu Zaufanego, chociaż powinny one być szczególnie chronione (ePUAP2 2014, s. 8). W ramach 7. osi POIG realizowano także projekt ePUAP2, którego celem była rozbudowa funkcjonalności platformy ePUAP i zwiększenie oferty usług świadczonych elektronicznie. Portal udostępniono w sierpniu 2015 r. Niestety jego jakość nadal nie jest zadowalająca – system jest nieintuicyjny i działa wolno, podczas zakładania konta często traci się połączenie z systemem, są problemy z uwierzytelnianiem, komunikaty są nieczytelne.

W celu obniżenia ryzyka wystąpienia nieprawidłowości w projektach informatycznych prowadzi się kontrole prewencyjne *ex ante* (przed ogłoszeniem postępowania) oraz *ex post* (po zakończeniu podpisania umowy o zamówieniach publicznych). Ponadto organizowane są seminaria i konferencje dotyczące zarządzania projektami i interoperacyjności. Dokonane kontrole potwierdzały na ogół prowadzenie projektów zgodnie ze zgłoszonymi metodykami, konieczne jest jednak dalsze upraszczanie dostępności zrealizowanych e-usług, szersze rozpowszechnianie informacji o zaletach korzystania z nich oraz o udanych projektach elektronicznej administracji.

---

[2] Obejmującym okres od opracowania założeń systemu do dnia kontroli, tj. 8.09.2014 r.

Ze względów bezpieczeństwa, w myśl nowelizacji ustawy o działach administracji rządowej, od 2016 roku nadzór na rejestrami państwowymi (PESEL, Rejestr Dowodów Osobistych, Rejestr Stanu Cywilnego, Centralna Ewidencja Wydanych i Unieważnionych Dokumentów Paszportowych oraz ewidencja pojazdów, ewidencja kierowców oraz ewidencja posiadaczy kart parkingowych), sprawowany dotychczas przez Ministerstwo Spraw Wewnętrznych i Administracji, został powierzony nowo utworzonemu Ministerstwu Cyfryzacji (Ustawa 2015).

W projektach dopuszczających wydzielanie podprojektów częściowych i podpisywanie umów z różnymi wykonawcami konieczne jest podejmowanie działań integrujących poszczególne rozwiązania w całość, co wymaga dodatkowych środków finansowych, ludzi i czasu. Dobra jakość poszczególnych modułów (systemów) otrzymanych z różnych zadań częściowych, przy braku koordynacji i wcześniejszych uzgodnień oraz braku standaryzacji i nadzoru nad całością – może doprowadzić do negatywnego efektu końcowego, co miało miejsce w przypadku projektu P1, stanowiącego kluczowy element dla obsługi systemu informacji w ochronie zdrowia.

## 2. Usługi elektroniczne w sektorze ochrony zdrowia

Od kilku lat trwają prace nad jednym z największych przedsięwzięć informatycznych w publicznym systemie ochrony zdrowia w Polsce, czyli projektem P1 – *Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania Zasobów Cyfrowych o Zdarzeniach Medycznych*, w ramach którego ma powstać platforma do udostępniania usług elektronicznych, takich jak Internetowe Konto Pacjenta, Elektroniczna Recepta, e-Skierowanie, e-Zlecenie oraz Portal informacyjny e-Zdrowie. Na temat problemów z realizacją systemu, rosnących kosztów (ok. 90 mln zł) i niedotrzymanych terminów napisano już wiele artykułów. Centrum Systemów Informacyjnych w Ochronie Zdrowia (CSIOZ), odpowiedzialne za realizację systemu, zapewnia, że w roku 2016 zostaną uruchomione usługi: e-recepta i e-skierowanie (Janczura 2015). Na stronie CSIOZ (csioz.gov.pl) są udostępniane różne rejestry medyczne, np. aptek, produktów leczniczych, farmaceutów. Z biuletynu CSIOZ wynika, że w 2015 roku nastąpiło pogorszenie jakości danych zawartych w Rejestrze Podmiotów Wykonujących Działalność Leczniczą (RPWDL) (CSIOZ 2015, s. 2), a platforma ePUAP nie jest w zasadzie w ogóle wykorzystywana przez podmioty lecznicze (CSIOZ 2015, s. 3). W ramach RPWDL dostępne są wyszukiwarki: Praktyk Zawodowych Lekarzy i Lekarzy Dentystów, Podmiotów Leczniczych oraz Praktyk Zawodowych Pielęgniarek i Położnych. W styczniu 2016 roku wydano pierwsze zwolnienia elektroniczne (e-ZLA). Do końca 2017 r. zwolnienia nadal będą mogły mieć także formę papierową (ZUS ZLA), ale od 1 stycznia 2018 roku mają już obowiązywać wyłącznie zwolnienia elektroniczne.

CSIOZ w ramach projektu P4: „Dziedzinowe systemy teleinformatyczne systemu informacji w ochronie zdrowia"[3] ma zbudować i wdrożyć:

- System Statystyki w Ochronie Zdrowia,
- System Monitorowania Zagrożeń,
- Zintegrowany System Monitorowania Obrotu Produktami Leczniczymi,
- System Monitorowania Kształcenia Pracowników Medycznych,
- System Ewidencji Zasobów Ochrony Zdrowia.

W obszernym, liczącym 540 stron raporcie opracowanym dla CSIOZ przez Infovide Matrix, dotyczącym stanu 30 medycznych rejestrów podmiotowych, w podsumowaniu stwierdzono, że w zasadzie rejestry są prowadzone zgodnie z przepisami prawnymi, ale poza Rejestrem Produktów Leczniczych wszystkie są wykorzystywane tylko w kraju (InfoVide 2014). Użytkownikami rejestrów są internauci i gestorzy. Każdy z rejestrów zaprojektowany jest zgodnie z wymaganiami danej instytucji, a nie ogólnego systemu informacji w ochronie zdrowia. Poważnym utrudnieniem w dalszej modernizacji i rozbudowie rejestrów jest brak pełnej dokumentacji poszczególnych systemów, i w wielu przypadkach jest ona w posiadaniu wykonawców zewnętrznych. Rejestry mają charakter zdecentralizowany i niejednorodny. W celu przebudowy i integracji rejestrów należałoby najpierw opracować spójną i kompleksową architekturę korporacyjną.

Wiele rejestrów zawiera bardzo ogólne dane, inne natomiast są opracowane bardzo rzetelnie i zawierają wszystkie niezbędne dane o chorym, jego wizytach, przebiegu choroby itp. Przykładem poprawnie prowadzonego rejestru jest Krajowy Rejestr Operacji Kardiochirurgicznych. Zgromadzone w nim dane mogą być wykorzystywane do przeprowadzania wielowymiarowych analiz kosztów, istotnych czynników ryzyka wczesnych powikłań i niepowodzeń po leczeniu kardiochirurgicznym, oceny jakości podjętego leczenia i generowania raportów. Dane mogą być wymieniane z bazą Europejskiego Towarzystwa Kardio-Torakochirurgów (EACTS). Profesjonalne prowadzenie rejestrów medycznych jest kosztowne, czasochłonne i wymaga od prowadzących (lekarzy, pielęgniarek itd.) niezwykłej staranności i systematyczności. Coraz więcej szpitali ubiega się o certyfikaty jakości nadzorowane przez Centrum Monitorowania Jakości w Ochronie Zdrowia.

Od kilku lat trwają prace nad utworzeniem Elektronicznego Rekordu Pacjenta i, według założeń, od 1 sierpnia 2014 r. dokumentacja medyczna miała być tworzona wyłącznie w wersji elektronicznej. Termin ten jednak nie został utrzymany. Zgodnie z Rozporządzeniem Ministra Zdrowia od 1 sierpnia 2017 r. prowadzenie EDM (Elektronicznej Dokumentacji Medycznej) będzie obowiązywało wszystkie placówki medyczne, przychodnie, kliniki, gabinety prywatne, NZOZ oraz wszystkie pozostałe podmioty medyczne (także indywidualne praktyki lekarskie).

---

[3] POIG, oś 7. „Społeczeństwo informacyjne – budowa elektronicznej administracji".

## 3. Bezpieczeństwo IT w podmiotach publicznych

Poziom bezpieczeństwa teleinformatycznego w administracji publicznej zależy od wiedzy i świadomości pracowników, szkoleń w tym zakresie, nakładów finansowych, od opracowania i przestrzegania polityki bezpieczeństwa oraz wielu innych czynników.

Bezpieczeństwo danych w serwisach internetowych i e-usługach instytucji publicznych nie jest na odpowiednim poziomie. Potwierdzają to wyniki badań zawarte w różnych raportach, m.in. NIK (Stefczyk 2015), „Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny" (EY 2015), „Zarządzanie ryzykiem w cyberprzestrzeni" (PWC 2014) i „Globalny stan bezpieczeństwa informacji 2015" (PwC 2015). Największym problemem administracji publicznej są źle zabezpieczone serwisy webowe urzędów w małych ośrodkach. Jednak do włamań dochodzi także na innych serwisach, np. Państwowej Komisji Wyborczej. Wiele serwisów w domenie gov.pl jest podatnych na ataki (Kasicki 2015). Uchybienia dotyczą także zarządzania uprawnieniami użytkowników w zakresie dostępu do systemów informatycznych, możliwości instalowania na komputerach urzędów dowolnego oprogramowania, nieuzasadnionego posiadania uprawnień administratora systemu, nieprzestrzegania procedur w zakresie odbierania uprawnień byłym pracownikom. W wielu urzędach brakuje opracowanych i wdrożonych regulacji związanych z zarządzaniem bezpieczeństwem informacji, czyli polityką bezpieczeństwa informacji (Muliński 2015).

W 2014 roku odnotowano w Polsce 7,5 tys. incydentów (Kasicki 2015), co oznacza 41% wzrost w porównaniu do roku 2013 (Jadczak 2014). Całkowity koszt systemów zabezpieczeń cybernetycznych na świecie w 2014 roku szacuje się na 2,4 mld USD (Stolarz 2015).

Zarządzanie bezpieczeństwem to nie tylko zadanie dla działu IT, tymczasem w Polsce nadal niewiele organizacji ma opracowaną strategię bezpieczeństwa, zidentyfikowane zasoby, które powinny podlegać ochronie, oraz wyznaczone osoby odpowiedzialne za ich ochronę. Opublikowany w 2013 roku dokument „Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej" (zatwierdzony przez Radę Ministrów) okazał się nieczytelny i trudny do praktycznego stosowania. Rada Bezpieczeństwa Narodowego opublikowała nowy dokument pt. „Doktryna cyberbezpieczeństwa RP 2015", zawierający opisy zagrożeń, ryzyk i szans oraz rekomendacje przeznaczone do odpowiedniego wykorzystywania „przez wszystkie podmioty publiczne i prywatne odpowiedzialne za planowanie, organizowanie i realizowanie zadań w dziedzinie cyberbezpieczeństwa" (BBN 2015).

Z badania Orange Insights przeprowadzonego przez firmę ICAN Research wynika, że 81% prezesów firm jest przekonanych, że bezpieczeństwo IT w ich firmach jest na odpowiednim poziomie, podczas gdy sytuację tę uważa za dobrą tylko 60% kierowników IT. Jako największy problem widzą oni utratę ciągłości

pracy systemów informatycznych i nieodpowiednie podejście pracowników do zagadnień bezpieczeństwa, a dopiero na trzecim miejscu wymieniane są ataki cybernetyczne. Widocznym trendem w firmach jest zwiększanie nakładów finansowych na zapewnienie bezpieczeństwa teleinformatycznego (Świrkula 2015). Zdaniem CERT w instytucjach państwowych przy wyborze systemów bezpieczeństwa głównym kryterium jest często jednak cena, a nie ich jakość (CERT 2015).

Instytucje administracji państwowej w coraz większym stopniu ufają rozwiązaniom w chmurze (cloud computing) i decydują się na przekazanie realizacji przynajmniej części usług i procesów na zewnątrz, m.in. w chmurze są przechowywane kopie zapasowe danych. Coraz większe zaufanie do cloud computing wykazują także małe i średnie przedsiębiorstwa (PS 2015).

## Podsumowanie

Komisja Europejska, zgodnie ze strategią Jednolitego Rynku Cyfrowego w UE, umożliwiła wszystkim zainteresowanym organizacjom i osobom prywatnym przekazanie swoich spostrzeżeń w sprawie e-administracji do 22 stycznia 2016 r. Na ich podstawie zostanie opracowany plan działania na rzecz e-administracji (eGovernment Action Plan 2016–2020) w zakresie zintegrowania europejskich i krajowych portali w celu utworzenia jednego portalu cyfrowego przyjaznego dla obywateli i przedsiębiorstw, wprowadzenia w 2016 r. zasady jednorazowości (ang. *once only*)[4], wzajemnego połączenia rejestrów handlowych do 2017 r., przyspieszenia przejścia państw członkowskich do w pełni elektronicznych zamówień publicznych oraz interoperacyjnych podpisów elektronicznych (MAC 2015).

Aktualne tematy dyskutowane w UE to jakość platform internetowych udostępnianych przez podmioty publiczne, problem cyberprzemocy i nielegalnych treści w Internecie oraz odpowiedzialności pośredników internetowych, przetwarzanie danych i wykorzystanie chmury obliczeniowej oraz model tzw. współdzielonej konsumpcji (*collaborative economy*), czyli ekonomii dzielenia się.

Jako rozwiązania najbliższej przyszłości wskazywane są usługi cloud computing i wszelkiego rodzaju usługi oparte na analizie danych. W przypadku urzędów administracji publicznej i ochrony zdrowia istotna jest taka budowa systemów centralnych, by możliwe było jednorazowe wprowadzanie danych i wielokrotne ich wykorzystywanie w określonym zakresie przez upoważnione podmioty. Bezpieczna realizacja zadań jest uzależniona od wdrożenia Systemu Zarządzania Bezpieczeń-

[4] Urzędy administracji państwowej powinny wykorzystywać dane zgromadzone o obywatelu, a nie pytać o nie ponownie. Obecnie ta zasada jest wykorzystywana tylko w 48% przypadków (KE 2015).

stwem Informacji, ze szczególnym uwzględnieniem ochrony danych poufnych, zapewnieniem ciągłości pracy oraz zarządzaniem incydentami i zmianami.

Podstawą sprawnej działalności administracji publicznej i ochrony zdrowia jest wykorzystywanie nowych technologii i systemów informatycznych, które muszą łączyć wygodę korzystania z nich z bezpieczeństwem użytkowania.

## Literatura


1. BBN (2015), *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, bbn.gov.pl/.html [dostęp 22.01.2015].
2. CERT (2015), *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014*, cert.gov.pl [dostęp 5.01.2016].
3. CSIOZ (2015), *Biuletyn informacyjny CSIOZ – wydanie dwudzieste*, csioz.gov.pl [dostęp 5.01.2016].
4. ePUAP2 (2014), Raport: *Analiza stanu realizacji projektu ePUAP2 w zakresie zadania „Rozbudowa lub poprawa ergonomii ePUAP2 ze szczególnym uwzględnieniem wydzielenia funkcjonalności Profilu Zaufanego"* przygotowany dla Władza Wdrażająca Programy Europejskie, Warszawa 2014, http://7poig.wwpe.gov.pl/index.php/dla-osi/17-analizy [dostęp 5.01.2016].
5. Europa (2015), *Jaki stopień cyfryzacji osiągnął twój kraj?*, KE – Komunikat prasowy, europa.eu/rapid/press-release_IP-15-4475_pl.htm [dostęp 24.2.2015].
6. EY (2015), Raport: *Bezpieczeństwo infrastruktury krytycznej, wymiar teleinformatyczny*, itsecurity24.info [dostęp 10.03.2015].
7. GUS (2015), *Społeczeństwo informacyjne w Polsce w 2015 r.*, raport GUS, Warszawa 2015, spoleczenstwo_informacyjne_w_polsce_2015_-_notatka.pdf [dostęp 6.01.2016].
8. Infovide (2014), *Raport z przeglądu stanu 30 Medycznych Rejestrów Podmiotowych*, Infovide-Matrix 2014, csioz.gov.pl [dostęp 10.07.2014].
9. Jadczak A. (2014), Raport PwC: *Polskie firmy zwiększają nakłady na bezpieczeństwo IT*, itwiz.pl [dostęp 11.12.2014].
10. Janczura M. (2015), *Największy system informatyczny w Polsce ruszy bez testów, z opóźnieniem i po zastrzyku 74 mln zł od resortu finansów. Przez ciąg błędów urzędników*, tokfm.pl [dostęp 24.07.2015].
11. Kasicki W. (2015), *Bezpieczeństwo serwisów i usług administracji publicznej*, computerworld.pl [dostęp 16.04.2015].
12. KE (2015), Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Strategia jednolitego rynku cyfrowego dla Europy. Bruksela, 2015. mac.gov.pl/files/komunikat_komisji_europejskiej_-_strategia_jednolitego_rynku _cyfrowego.pdf [dostęp 6.05.2015].

13. MAC (2015), *eGovernment Action Plan 2016–2020 – plan działania w obszarze e-administracji – konsultacje KE*, mac.gov.pl [dostęp 22.01.2015].
14. Muliński T. (2015), *Zagrożenia bezpieczeństwa dla systemów informatycznych e-administracji*, CeDeWu.pl, Warszawa.
15. POIG (2015), *Planowane źródła finansowania i modele utrzymania systemów teleinformatycznych 7 osi POIG – na przykładzie CEIDG i ePK*, http://7poig.wwpe.gov.pl [dostęp 31.07.2015].
16. PS (2015), *Administracja publiczna przekonuje się do chmury*, portalsamorzadowy.pl/spoleczenstwo-informacyjne/administracja-publiczna-przekonuje-sie-do-chmury,76225.html [dostęp 31.12.2015].
17. PwC (2014), *Polskie firmy zwiększają nakłady na zarządzanie bezpieczeństwem w cyberprzestrzeni*, pwc.pl [dostęp 10.12.2014].
18. PwC (2015), *Globalny stan bezpieczeństwa informacji 2015*, pwc.pl/pl/ publikacje/2014/zarzadzanie-ryzykiem-w-cyberprzestrzeni.html [dostęp 10.12.2015].
19. SDA (2015), *System Dygitalizacji Akt (SDA) – konferencja Prokuratury Generalnej podsumowująca projekt*, pg.gov.pl/aktualnosci-prokuratury-generalnej [dostęp 10.12.2015].
20. Stefczyk (2015), *System e-administracji lokalnej nie działa*, stefczyk.info/wiadomosci/raporty-stefczyk-info/system-e-administracji-lokalnej-nie-dziala,13327655129 [dostęp 23.03.2015].
21. Stolarz M. (2015), *W 2015 roku więcej cyberataków i większe wydatki na bezpieczeństwo*. Bellini Capital, biznes.newseria.pl/komunikaty/it_i_technologie/w_2015_roku_wiecej,b1506786236 [dostęp 13.01.2015].
22. Świrkula K. (2015), *Orange Insights: Bezpieczeństwo IT okiem dużych firm i korporacji*, http://itfocus.pl/raporty/orange-insights-bezpieczenstwo-it-okiem-duzych-firm-korporacji-0#.Vo1F7FLbm2l [dostęp 26.11.2015].
23. Ustawa z dnia 19 listopada 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw, DzU 2015 nr 0 poz. 2281, dziennik ustaw.gov.pl/du/2015/1960/1 [dostęp 26.11.2015].

## PROBLEMS OF ELECTRONIC EXECUTION OF SERVICES IN PUBLIC ADMINISTRATION AND HEALTH CARE

**Summary**

IT development in the area of economy, which has been proceeding dynamically in recent years, includes more and more sectors. The data gathered is not only citizens' personal data but also financial and medical data as well as data concerning one's lifestyle, tastes, etc. The condition of IT system security, however, is unsatisfactory. The aim of the study is to present current problems connected with making digital data registers and ICT systems indispensable for the execution of services in public administration and health care sectors.

**Keywords:** e-government, e-health, e-service, security.

*Translated by Zygmunt Mazur*