

Administracja publiczna

Rewolucja technologiczna w zarządzaniu publicznym. E-administracja

Dr hab. Ryszard Szarfenberg

Instytut Polityki Społecznej

rszarf.ips.uw.edu.pl/apub

Rok akademicki 2018/2019

Podróż kontynuujemy przez zdolność do działania i sprawność

1. Administracja multientryczna. Poziomy zarządzania publicznego

2. Polityka publiczna i rola administracji w jej tworzeniu

I. Tworzenie polityki publicznej

3. Zarządzanie publiczne przez władztwo. Administracja władcza i jej przeobrażenia

4. Prawo do dobrej administracji - narzędzie ochrony jednostki przed nadużyciem władztwa

II. Regulowanie przez zakazy i nakazy

5. Administracja dobrobytu. Ewolucja zakresu i form wykonywania funkcji świadczących

6. Mechanizmy rynkowe jako główna metoda zapewnienia usług publicznych

III. Zapewnianie usług publicznych

7. Zarządzanie przez rezultaty. Administracja zorientowana na wyniki

8. Zarządzanie zasobami ludzkimi w administracji publicznej

9. **Rewolucja technologiczna w zarządzaniu publicznym. E-administracja**

10. Nowa formuła kontroli w administracji. Od klasycznej kontroli do audytu i zarządzania jakością

IV. Zdolność do działania i sprawność

11. Europeizacja zarządzania publicznego. Administracja krajowa w Unii Europejskiej

12. Administracja współpracująca. Zarządzanie publiczne jako kooperacja

13. Administracja i obywatele. W stronę partnerstwa

V. Współdziałanie

Administracja jako przedsiębiorstwo. E-administracja

- ***Społeczeństwo informacyjne i e-administracja***
- **Technologie informacyjne** na rzecz sprawnego zarządzania w administracji
- **Obsługa obywatela** z wykorzystaniem technologii informacyjnych
- **Cyberzagrożenia** (*cyberbezpieczeństwo*)

Pytania sprawdzające

1. Czym jest **społeczeństwo informacyjne** i jak je mierzyć?
2. Podaj definicję **rejestru publicznego** i trzy przykłady rejestrów publicznych.
3. Jakie główne funkcje spełniają **technologie informatyczne w administracji publicznej**?
4. Czym jest i jakie informacje zawiera **Biuletyn Informacji Publicznej**?
5. Czym są **cyberzagrożenia** i jakie są ich źródła? Jaka politykę cyberbezpieczeństwa ma Polska?
6. Jakie dokumenty powinien opracować **administrator danych osobowych**?
7. Jakie zagrożenia wiążą się z przetwarzaniem danych w modelu **cloud computing**?
8. Jakie dokumenty z zakresu prawa miękkiego i twardego określają politykę Polski w zakresie **cyberbezpieczeństwa**?

Motto

“

Docelowo wszystkie e-usługi resortu finansów będą zintegrowane i udostępniane na nowym portalu podatnika.

Jego nowa odsłonę planujemy już na początku 2019 r. wraz z uruchomieniem usługi Twój e-PIT. Dalsza integracja e-usług pozwoli w okresie 4-5 lat na wdrożenie koncepcji e-urzędu.

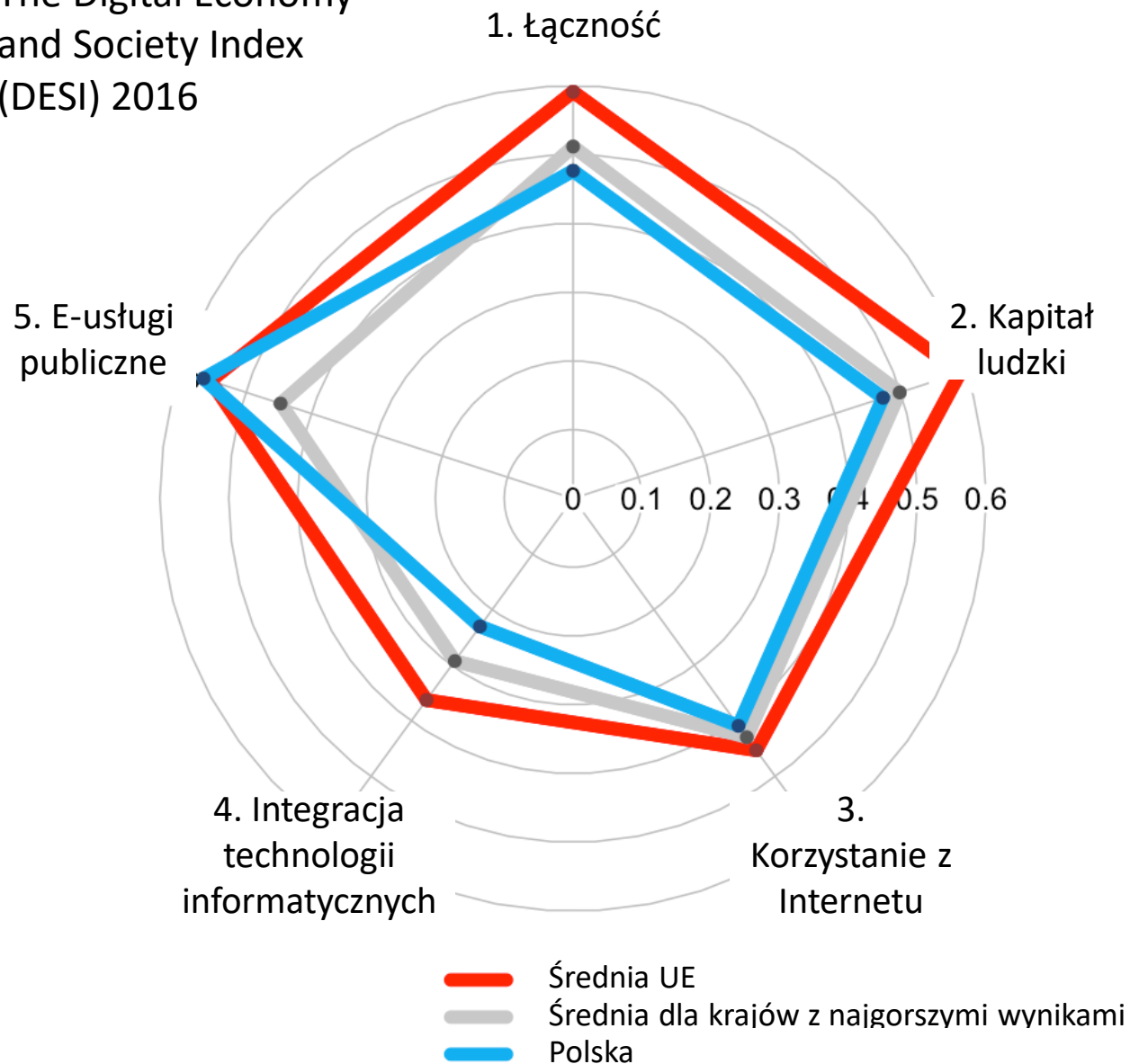
minister finansów prof. Teresa Czerwińska



[TT@MF_GOV_PL](mailto:TT@MF.GOV.PL)

Czym jest społeczeństwo informacyjne i jak je mierzyć?

- W społeczeństwie informacyjnym:
 - gospodarstwa domowe, przedsiębiorstwa i **administracja publiczna wykorzystują infrastrukturę ICT** – Internet i inne sieci (intranet, extranet), komputery, telefony, smartfony, tablety, serwery, terminale, smart TV itp. [PO CO?]
 - aby sprawnie **pozyskać wiarygodną informację** przyjmującą coraz częściej postać **cyfrowego produktu lub usługi (e-produktu, e-usługi)** [PO CO?]
 - dla efektywnej **realizacji celów** w wielu obszarach swojej działalności
 - Wybranymi ogólnymi celami tej działalności mogą być:
 - lepsze zaspokajanie potrzeb, poprawa jakości życia
 - maksymalizacja zysku
 - **wzrost sprawności i efektywności administracji**
 - [GDZIE?] W praktyce znajduje to wyraz w rozwoju **e-biznesu, e-administracji, e-zdrowia, e-edukacji, e-kultury, e-turystyki**

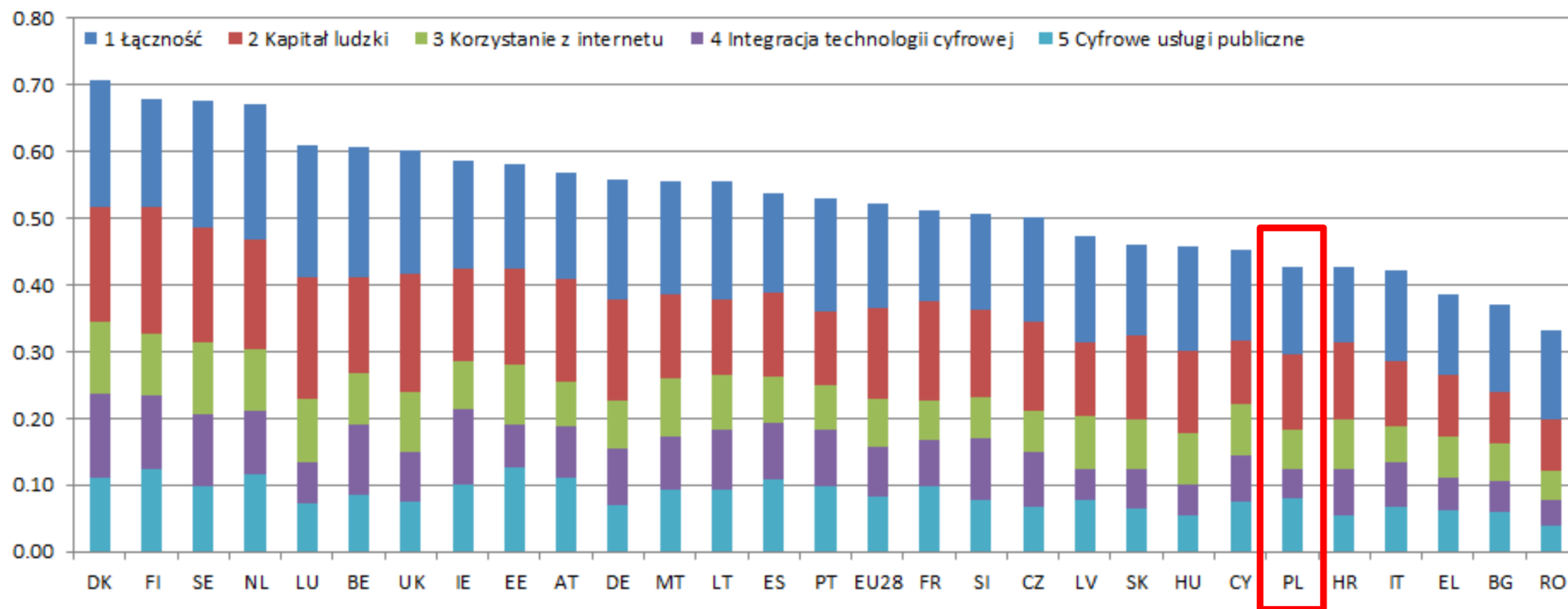


Jak mierzyć społeczeństwo informacyjne? Indeks cyfrowej gospodarki i społeczeństwa (DESI)

Wymiary DESI

1. **Łączność** – rozwój i jakość **infrastruktury szerokopasmowej**
2. **Kapitał ludzki** – **kompetencje** potrzebne do korzystania z technologii cyfrowych
3. **Korzystanie z Internetu** – różnorodność **aktywności w sieci**
4. **Integracja technologii informatycznych** – zakres wykorzystywania przez biznes **sprzedaży on-line**
5. **E-usługi publiczne** – usługi **e-administracji i e-zdrowie**

Wyniki Polski w pięciu wymiarach DESI na tle innych krajów (2017)



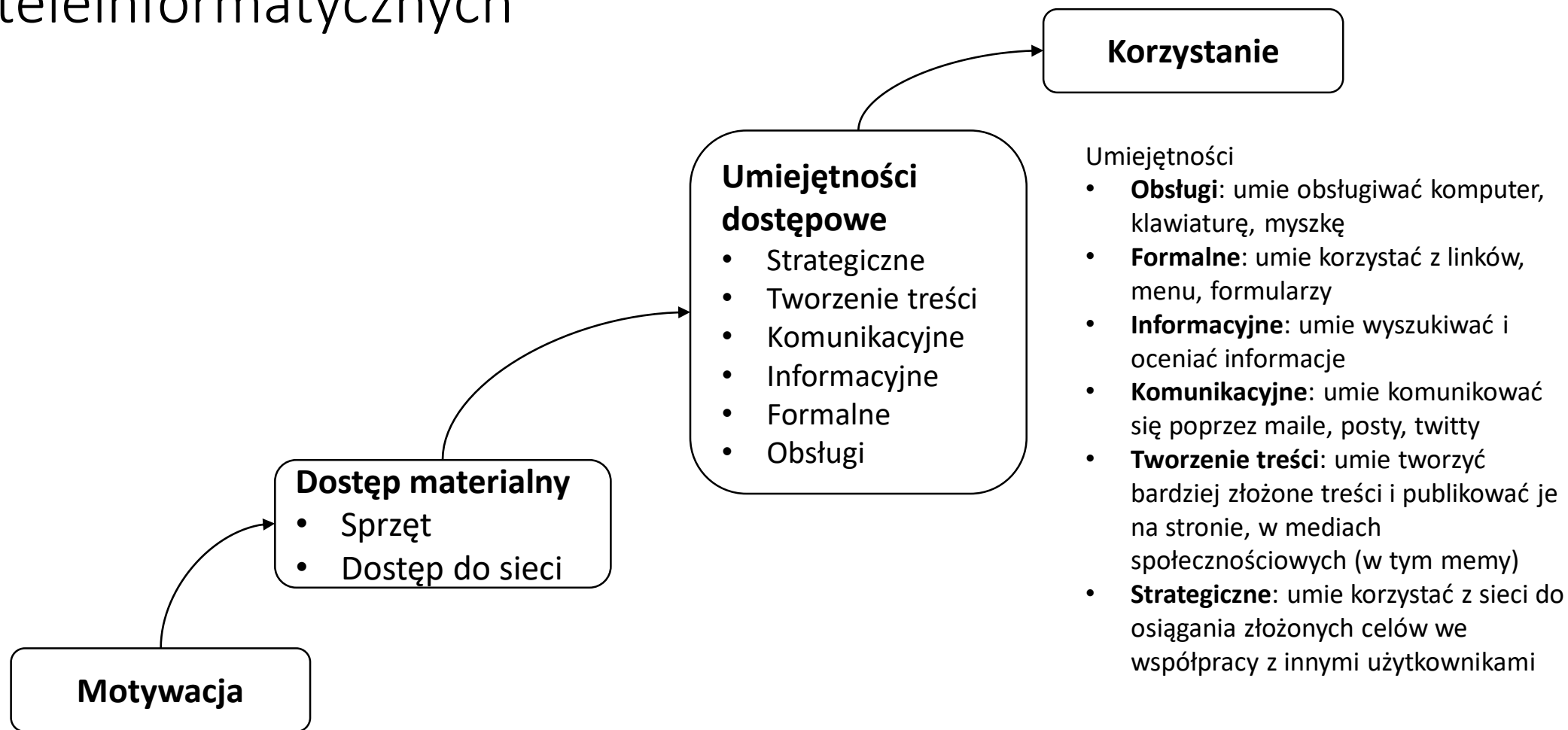
Państwo wobec rozwoju technologii informatycznych

- Upowszechnienie **narzędzi teleinformatycznych** oraz **ich konsekwencje** (np. **wykluczenie cyfrowe**) powoduje, że **konieczne jest zaangażowania państwa**
- **Państwo angażuje się w rozwój technologii informacyjnych w**
 1. obrębie samej administracji
 2. obszarze jej kontaktów z obywatelami
 3. proces inwestycji w infrastrukturę telekomunikacyjną (ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych)
- **Państwo ingeruje w społeczeństwo informacyjne**, aby rozwiązywać jego problemy:
 - **wykluczenie cyfrowe**
 - **ochrona konsumentów** w obrocie elektronicznym
 - **zwalczanie przestępczości komputerowej**
 - **rozwój systemów płatności elektronicznych**
 - **poszanowanie prywatności jednostek**
 - **ochrona praw własności intelektualnej**

Wykluczenie cyfrowe jako problem społeczeństwa informacyjnego

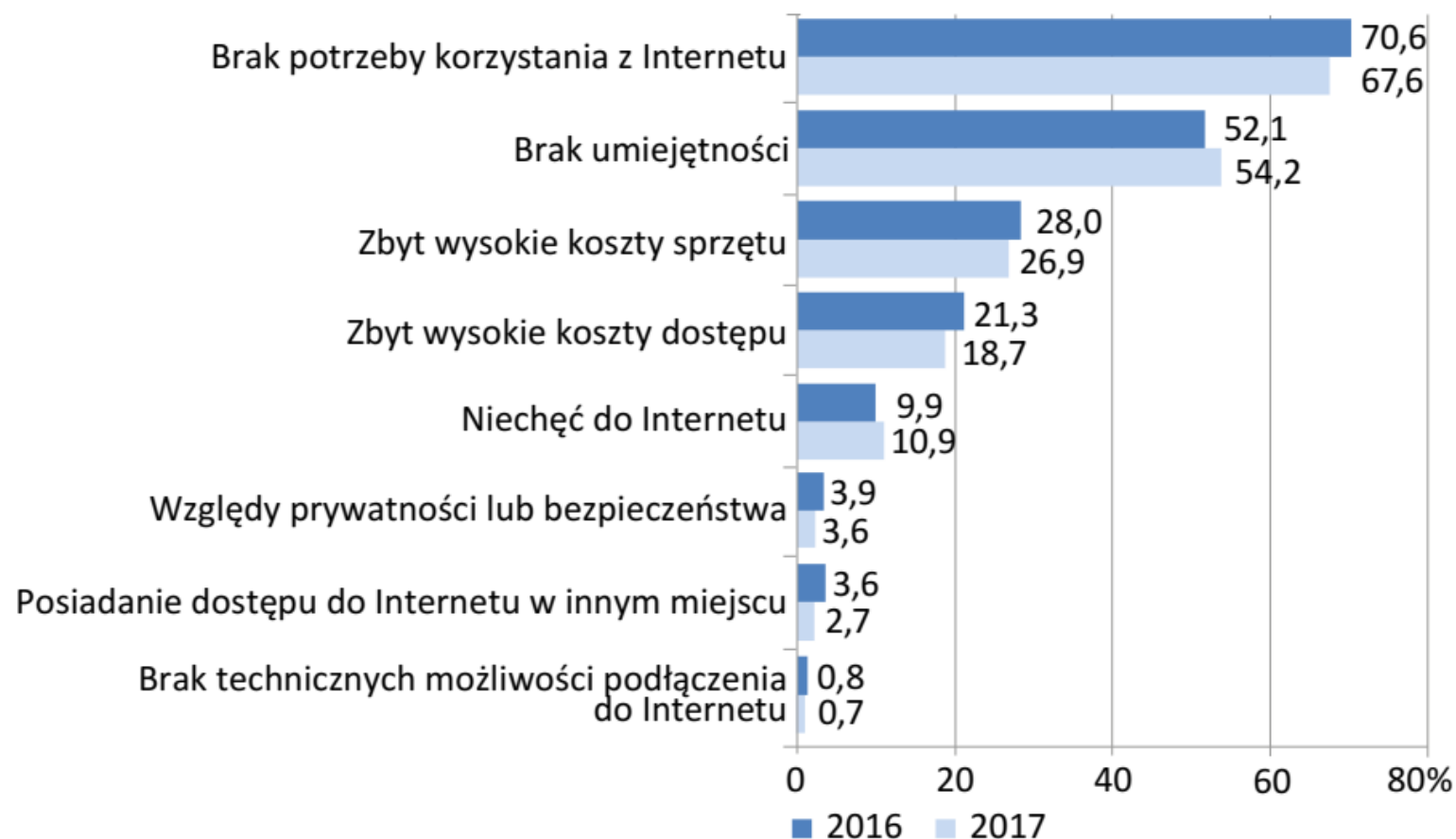
- **DEFINICJA wykluczenia cyfrowego:** pogłębianie się różnic pomiędzy obywatelami ze względu na zróżnicowany poziom dostępu do Internetu i usług elektronicznych (liUE)
 - Zróżnicowany dostęp do liUE => pogłębianie nierówności między obywatelami
- Jest to zjawisko **związane z dwoma czynnikami**
 - **BRAK DOSTĘPU** brak bądź ograniczenie fizycznego dostępu do Internetu
 - **BRAK KOMPETENCJI** nieumiejętność posługiwania się Internetem oraz nieznajomość języków
- Odpowiedź władz publicznych i administracji polega więc na:
 - **Upowszechnianiu dostępu** do szerokopasmowego Internetu
 - **Upowszechnianiu kompetencji teleinformatycznych** i językowych (wiedza, umiejętności, postawy)

Cztery poziomy dostępu do pełnego korzystania z technologii teleinformatycznych

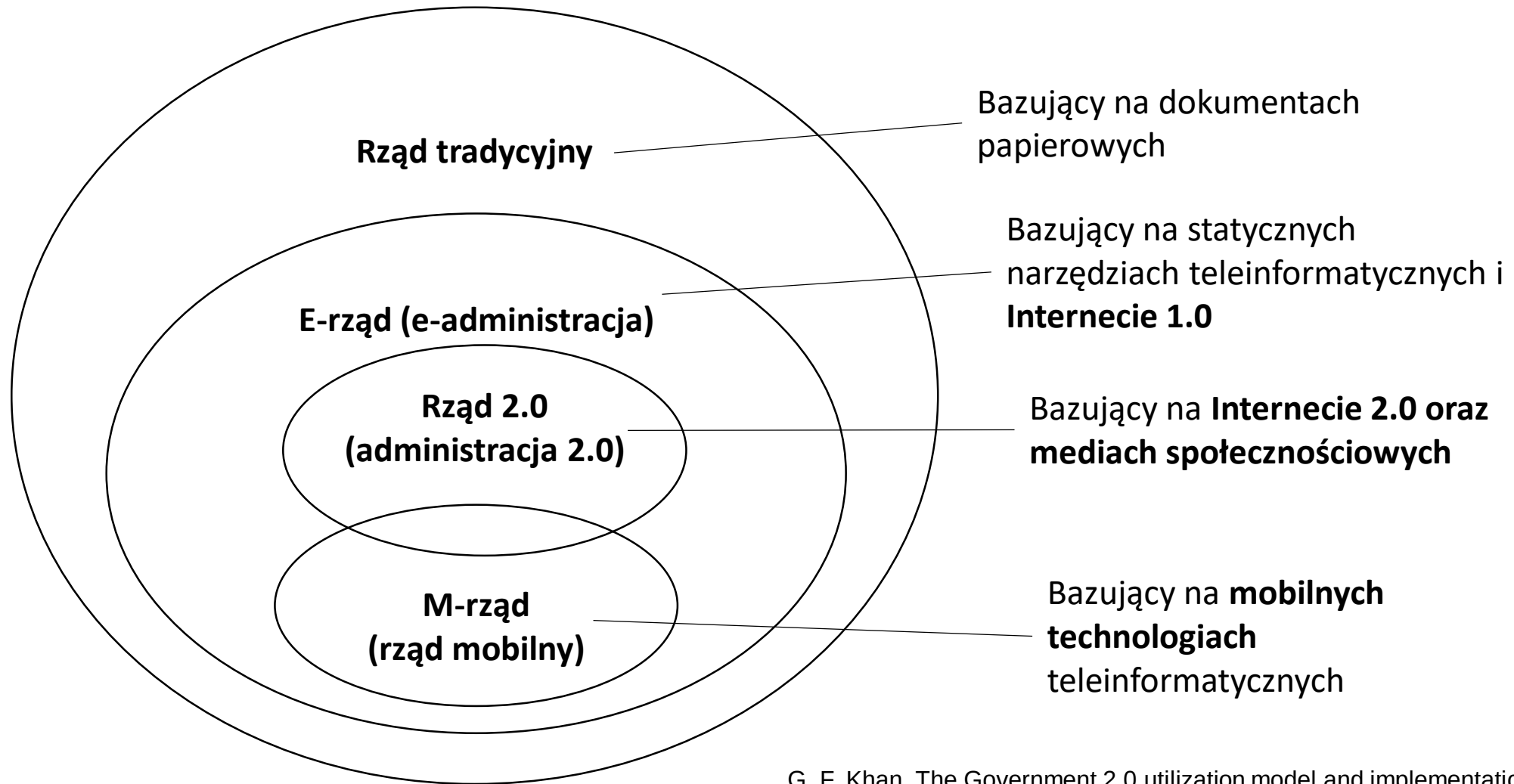


Brak dostępu do Internetu: powody podawane przez respondentów

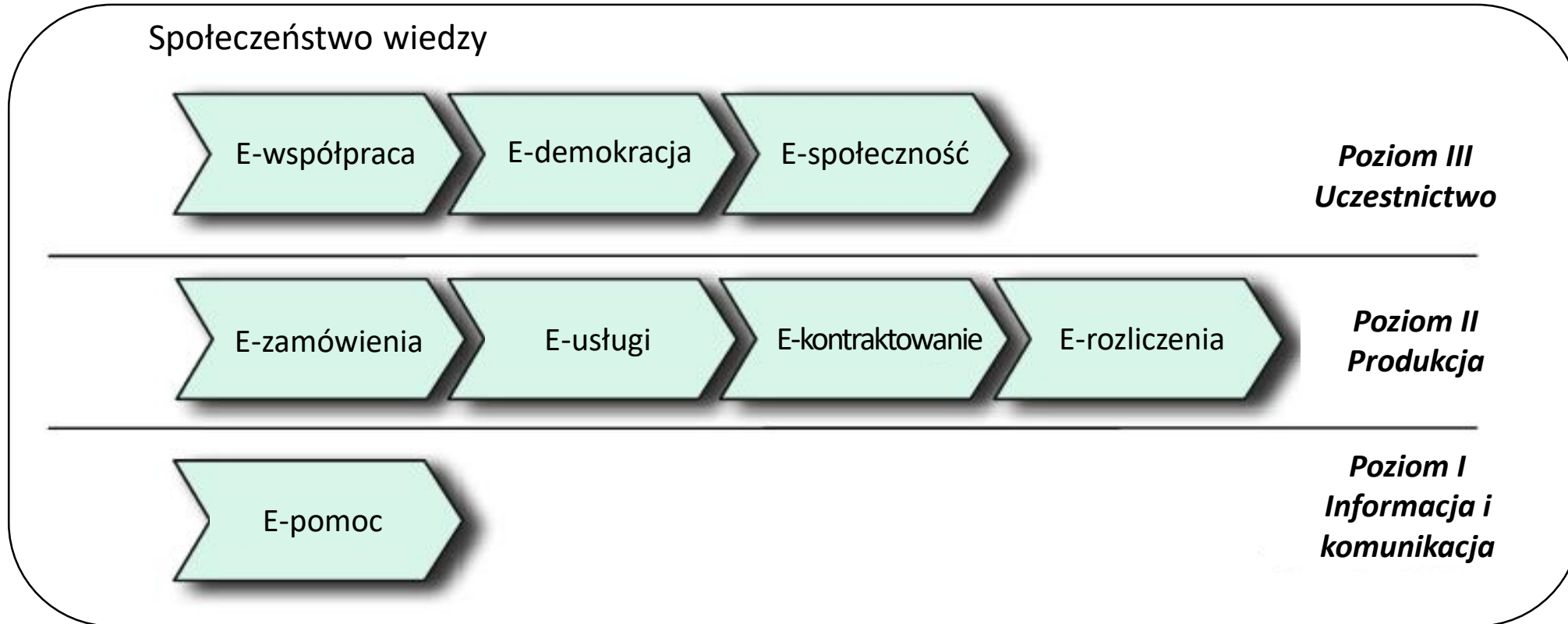
Wykres 9. Powody braku dostępu do Internetu w domu (w % gospodarstw bez dostępu do tej sieci)



Rząd (administracja) tradycyjny, e-rząd, rząd 2.0, rząd mobilny (m-rząd)



Trzy poziomy e-rządu



Technologie teleinformatyczne w administracji - zagadnienia

- Technologie informacyjne **w administracji** wspomagają
 - **procesy wewnętrzne** (np. intranet)
 - **procesy zewnętrzne** (np. komunikacja z obywatelami)
- Najistotniejsze zagadnienia z tym związane
 - **standaryzacja dokumentów i procedur** elektronicznych
 - regulacja technik identyfikacji oraz **podpisu elektronicznego**
 - **ochrona poprawności i integralności informacji** przetwarzanych i wykorzystywanych przez administrację
 - **ochrona prywatności jednostek i innych praw** podmiotów administrowanych

Główne funkcje technologii informatycznej w administracji publicznej

- „Jednym z najważniejszych celów informatyzacji administracji publicznej w Polsce jest przezwycięzenie tzw. asymetrii informacyjnej pomiędzy państwem a obywatelem”
- Technologie informacyjne w komunikacji z obywatelem, służą realizacji trzech funkcji
 1. **informacyjnej**, czyli uzyskiwania informacji o podmiotach, osobach lub rzeczach (rejstry publiczne i inne)
 2. **świadczenia usług e-administracji**
 3. **jawności działania administracji** (czyli uzyskiwania informacji o organach władzy publicznej i administracji, np. Biuletyn Informacji Publicznej)
- Docelowym modelem świadczenia usług e-administracji będzie **pełna automatyzacja procesów**

Definicja rejestru publicznego i trzy przykłady rejestrów publicznych

- **DEFINICJA rejestru publicznego – zbiór informacji o osobach, rzeczach lub prawach, który ma następujące cechy:**
 - **jest utworzony na podstawie przepisów prawa** (przepisy przynajmniej przewidują jego utworzenie)
 - **jest prowadzony przez organ rejestrowy** o charakterze publicznym
 - przyjęcie, utrwalenie a następnie ujawnienie określonych w nim informacji co do zasady **następuje w drodze decyzji**
 - prowadzenie rejestru i ujawnianie zawartych w nim danych rodzi skutki prawne zarówno dla osoby, której wpis dotyczy, jak i dla organu
 - **jest jawny**
- Przykłady: KRS, KRK, NKW, POLTAX, PESEL, CEPIK, REGON

Świadczenie e-usług publicznych: profil zaufany i lista dostępnych usług

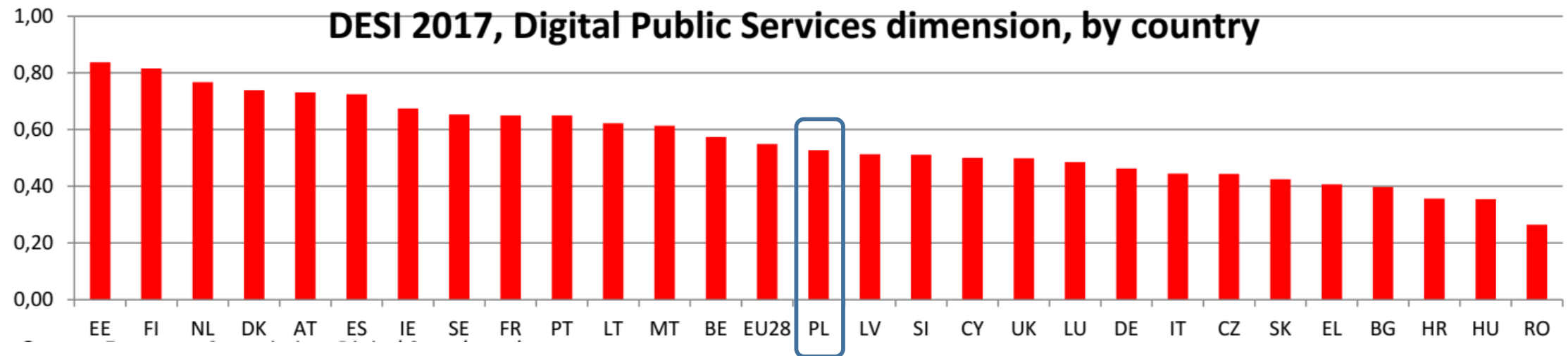
- **Definicja profilu zaufanego:** bezpłatna metoda potwierdzania tożsamości obywatela w systemach elektronicznych administracji publicznej

- Lista e-usług:

- Sprawdzić i złożyć **dokumenty rozliczeniowe** w Urzędzie Skarbowym
- Złożyć i sprawdzić **dokumenty w ZUS** np. sprawdzić wysokość składki odprowadzanej przez ZUS do OFE, obliczyć prognozowaną wysokość emerytury
- Sprawdzić swoje **punkty karne**
- Złożyć **wniosek o rejestrację działalności** gospodarczej
- Zgłosić utratę lub uszkodzenie **dowodu osobistego**
- Złożyć **wniosek o dowód osobisty dla siebie lub dziecka**
- Wystąpić o **Europejską Kartę Ubezpieczenia Zdrowotnego**
- Załatwić **sprawy urzędowe** dla swojej **rodziny**: świadczenia rodzicielskie, Świadczenie z Funduszu Alimentacyjnego
- Złożyć **wniosek o przyznanie Karty Dużej Rodziny** lub wydanie duplikatu Karty Dużej Rodziny
- Uzyskać **odpis aktu stanu cywilnego**
- Złożyć **deklarację na podatek od nieruchomości**
- Złożyć **wniosek o udostępnienie dokumentacji medycznej**
- Zgłosić **sprzedaż samochodu**

[Pełna lista 44 usług online na portalu Obywatel.gov.pl](https://www.gov.pl)

Wyniki Polski w wymiarze cyfrowych usług publicznych na tle innych krajów (2017)



Digital Public Services. Europe's Digital Progress Report 2017

Korzystanie z usług e-administracji w Polsce

Tablica 4. Osoby korzystające z usług administracji publicznej za pomocą Internetu w ciągu ostatnich 12 miesięcy według celu

Wyszczególnienie	2014	2015	2016	2017
	w %			
Osoby korzystające z usług administracji publicznej za pomocą Internetu	26,9	26,6	30,2	30,8
w celu:				
wyszukiwania informacji na stronach administracji publicznej	20,4	19,1	22,8	20,6
pobierania formularzy urzędowych	16,8	16,8	19,0	20,2
wysyłania wypełnionych formularzy	14,8	15,7	18,8	21,0

Przykłady potrzeb w zakresie e-usług: e-rynek pracy

- Scentralizowanie usług dla osób bezrobotnych, poszukujących pracy, pracodawców i przedsiębiorców oraz publicznych służb zatrudnienia poprzez **e-PUP** (e-Powiatowy Urząd Pracy)
- Zapewnienie **jednego punktu dostępu do wszystkich ofert pracy** pochodzących z sektora publicznego
- Umożliwienie **aplikowania o pracę w sektorze publicznym w formie elektronicznej**: obecnie wszystkie oferty pracy zamieszczane w BIP KPRM (który nie obejmuje całego sektora publicznego, a tylko administrację rządową) zawierają wymóg dostarczania dokumentów papierowych
- **Przeniesienie kolejnych usług rynku pracy do Internetu** (dostępne są już rejestracja osób bezrobotnych i przeszukiwanie ofert)

Przykłady potrzeb w zakresie e-usług: e-świadczenia

- **Internetowe konto ubezpieczonego**, zintegrowane z innymi usługami e-administracji
- Usługi Zakładu Ubezpieczeń Społecznych (ZUS):
 - dalsza **elektronizacja zwolnień lekarskich** i ich przesyłania od lekarzy wystawiających do ZUS (wymaga komunikacji między systemami teleinformatycznymi podmiotów leczniczych, platformą P1 oraz systemem ZUS)
 - budowa **platformy analityczno-statystycznej** możliwej do udostępnienia innym systemom i instytucjom
- Utworzenie na poziomie centralnym **skonsolidowanego systemu informatycznego**, wspomagającego gminy, powiaty i województwa w realizacji zadań z zakresu zabezpieczenia społecznego (racjonalizacja w skali całego kraju wydatków na infrastrukturę techniczną, standaryzacja sposobu pracy jednostek, ograniczenie problemów kadrowych dot. IT w gminach oraz poprawa efektywności mechanizmów sprawozdawczych)

Przykłady pełnej automatyzacji procesów (hipotetyczne)

- **Kończy się ważność dowodu osobistego**, system to wykrywa, podejmuje działania mające na celu wystawienie nowego, powiadamia zainteresowanego o możliwościach odbioru
- **Decyzja w sprawie zasiłku rodzinnego** będzie polegała na:
 - skierowaniu przez system obsługujący przyznawanie świadczeń rodzinnych zapytania do systemu PESEL
 - zapytaniu o dochody (obecnie system POLTAX)
 - zapytaniu o ew. niepełnosprawność (NFZ)
 - zapytaniu do Systemu Informacji Oświatowej (SIO)
 - po uzupełnieniu o inne dokumenty automatyczna decyzja o przyznaniu świadczenia

Definicja Biuletynu Informacji Publicznej (BIP) i jego treści

- **DEFINICJA BIP:** „urzędowy publikator teleinformatyczny w postaci ujednoliconego systemu stron w sieci teleinformatycznej”
- **Organy publiczne umieszczają w BIP informacje o**
 - **polityce** wewnętrznej i zagranicznej
 - **swoim statusie** prawnym, organizacji, przedmiocie działalności i kompetencjach, organach i osobach sprawujących w nich funkcje i ich kompetencjach, swojej strukturze własnościowej oraz majątku, którym dysponują
 - **zasadach ich funkcjonowania** (tryb działania, sposoby załatwiania spraw, stan załatwiania spraw itp.)
 - **danych publicznych** (treść i postać dokumentów urzędowych, treść innych wystąpień i ocen dokonywanych przez organy władzy publicznej, informacja o stanie państwa, samorządów i ich jednostek organizacyjnych)
 - **majątku publicznym**

Zagrożenia związane z ICT – cyberzagrożenia

- **Definicja cyberzagrożenia:** „możliwość wystąpienia złośliwego działania mającego na celu zniszczenia lub zakłócenia działania sieci lub systemu komputerowego, uzyskanie nieuprawnionego dostępu do plików, szpiegowanie i wykradanie danych”
- Główne źródła cyberzagrożeń
 - Państwa i rządy
 - Terroryści
 - Szpiegzy przemysłowi
 - Zorganizowane grupy przestępcze
 - Hakywiści, hakerzy (hakywizm: użycie komputerów i sieci do promowania celów społecznych i politycznych)
 - Konkurencja biznesowa
 - Niezadowoleni pracownicy

Programy wykorzystywane do działalności szkodliwej

- **Wirusy, robaki** (zarażają i replikują się)
- **Konie trojańskie** (program szpiegujący, wykradający dane, ukryty w innej aplikacji)
- **Spyware** (szpiegowanie poczynąń użytkownika, wykradanie danych)
- **Malware** (szkodliwe działania i kradzież danych)
- **Exploity, rootkity** (przejęcie kontroli nad systemem z prawami administratora)
- **Phishing** (podstawione strony do złudzenia podobne do prawdziwych)
- **Dialery** (przekierowujące połączenia modemowe na płatne numery)
- **Keyloggery** (rejestrujące znaki z klawiatury)
- **Scareware, rogueware, false antivirus** (wyskakujące okienka z ostrzeżeniami o wirusie, fałszywe programy antywirusowe, skłaniają do zakupu lub instalacji)
- **Ransomware** (blokują komputer lub szyfrują dane żądając opłaty za odblokowanie)
- **Porywacze przeglądarek**

Zagrożenia związane z przetwarzaniem danych w modelu *cloud computing*

- Co to jest *cloud computing* (CC, **przetwarzanie w chmurze**)?
 - „*Cloud Computing* jest nowym modelem wykorzystania (IT) i stylem przetwarzania, w którym procesy biznesowe, aplikacje, dane i zasoby IT są dostarczane do użytkowników w formie usług”*
- Kupowanie usług typu CC nie jest zakazane, a więc podmiot administracji publicznej zamiast kupować np. aplikację, może korzystać z gotowych rozwiązań oferowanych przez dostawców rozwiązań w „chmurze”
- Główny problem polega na tym, że **nie ma kontroli nad miejscem przetwarzania danych, które mogą mieć charakter wrażliwy** (dane osobowe obywateli)

[*J. Łagowski, *Cloud Computing – Co to jest*. XVI Konferencja PLOUG, Kościelisko, październik 2010](#)

Ochrona danych osobowych (podręcznik zawiera nieaktualne informacje)

- Główny akt prawny obecnie to RODO (rozporządzenie ogólne o ochronie danych osobowych) - [Rozporządzenie Parlamentu Europejskiego i Rady \(UE\) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE](#) wszedł w życie w 2018 r.
- Polski akt wdrażający RODO [to ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych](#) (nowa ustawa zastępująca tą z 1997 r., o której mowa w podręczniku)
- Niektóre definicje z RODO (art. 4)
 - „**dane osobowe**” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
 - „**przetwarzanie**” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
 - „**naruszenie ochrony danych osobowych**” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
- Na gruncie RODO i nowej ustawy nie ma obowiązku posiadania dokumentu „polityka bezpieczeństwa”, z RODO wynika jednak konieczność prowadzenia „rejestrów czynności przetwarzania danych osobowych”. Ustanowienie inspektora danych osobowych jest obowiązkowe tylko w określonych przypadkach

Najważniejsze inicjatywy podejmowane w Polsce na rzecz zapewnienia cyberbezpieczeństwa (dokumenty strategiczne, ustawy)

Pierwszy dokument rządowy w tym zakresie: **Polityka Ochrony Cyberprzestrzeni RP** (2013)
„Celem strategicznym *Polityki* jest osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni Państwa”

Drugi dokument rządowy w tym zakresie:

Krajowe Ramy Polityki

Cyberbezpieczeństwa Rzeczypospolitej

Polskiej na lata 2017-2022 (2017) – „zbiór deklaracji i założeń, jakimi kierował się będzie rząd przy tworzeniu zapowiadanej ustawy o krajowym systemie cyberbezpieczeństwa”

Rada Bezpieczeństwa Narodowego publikuje **Doktrynę Cyberbezpieczeństwa RP**, dokument niewiążący, który postulował m.in. „wprowadzenie... rozwiązań formalno-prawnych oraz mechanizmów współpracy... sektora publicznego i prywatnego, inwestycje w narodowe rozwiązania w dziedzinie cyberbezpieczeństwa...”

Uchwalenie **ustawy o krajowym systemie cyberbezpieczeństwa** m.in. **prawna definicja cyberbezpieczeństwa**: „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”

2013

2015

2017

2018



Cyberbezpieczeństwo w polskim prawie

Ustawa o krajowym systemie cyberbezpieczeństwa (2018)

Art. 1. 1. Ustawa określa:

- 1) organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu;
- 2) sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy;
- 3) zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Cel krajowego systemu cyberbezpieczeństwa

Art. 3. Krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów.

Definicja cyberbezpieczeństwa

- 4) cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;

Lektura obowiązkowa

- Rewolucja technologiczna w zarządzaniu publicznym. E-administracja, w: Dawid Sześciło (red.), *Administracja i zarządzanie publiczne. Nauka o współczesnej administracji*, Stowarzyszenie Absolwentów Wydziału Prawa i Administracji UW, 2014.
- Na przyszłe zajęcia: **Nowa formuła kontroli w administracji. Od klasycznej kontroli do audytu i zarządzania jakością**, w: Dawid Sześciło (red.), *Administracja i zarządzanie publiczne. Nauka o współczesnej administracji*, Stowarzyszenie Absolwentów Wydziału Prawa i Administracji UW, 2014.