Jerzy Krawiec

Normalizacyjne aspekty w budowaniu społeczeństwa cyfrowego

Edukacja - Technika - Informatyka nr 1(15), 80-89

2016

© Wydawnictwo UR 2016 „Edukacja – Technika – Informatyka" nr 1/15/2016
ISSN 2080-9069 www.eti.rzeszow.pl
ISSN 2450-9221 online DOI: 10.15584/eti.2016.1.12

JERZY KRAWIEC

Normalizacyjne aspekty w budowaniu społeczeństwa cyfrowego

Standardization aspects in building the digital society

Doktor inżynier, Politechnika Warszawska, Instytut Organizacji Systemów Produkcyjnych, Zakład Systemów Informatycznych, Polska

Streszczenie

Przedstawiono znaczenie procesu normalizacji w ramach budowy społeczeństwa cyfrowego. Wskazano na rolę norm w ramach agendy cyfrowej mających szczególne znaczenie w obszarach interoperacyjności, cyberbezpieczeństwa oraz umiejętności informatycznych.

Słowa kluczowe: społeczeństwo cyfrowe, normalizacja, interoperacyjność, cyberbezpieczeństwo.

Abstract

The article discusses some aspects of the standardization process in building the digital society. Indicates the role of standards in the areas of interoperability, cyber security and computer skills in the framework of the Digital Agenda.

Key words: digital society, standardization, interoperability, cyber security.

Wstęp

Społeczeństwo w fazie rozwoju organizacyjnego i technicznego, w którym poziom techniki informatycznej umożliwia powszechne stosowania informacji w celu wytwarzania produktów i świadczenia usług, jest określane mianem społeczeństwa informacyjnego lub inaczej nazywane społeczeństwem cyfrowym. W epoce społeczeństwa cyfrowego internet stał się kluczowym elementem. Jest on dziś bardzo ważnym środkiem do prowadzenia działalności biznesowej i społecznej. Natomiast podstawą rozwoju takiego społeczeństwa jest infrastruktura szerokopasmowego dostępu do internetu oraz powszechne stosowanie technik informatycznych w pracy. Pracownicy, ze swoją wiedzą i doświadczeniem, stanowią intelektualne zaplecze dla gospodarki opartej na wiedzy.

Agenda cyfrowa

Wartość rynkowa sektora technologii informacyjnych jest szacowana na poziomie 660 mld euro rocznie, co stanowi około 5% PKB Unii Europejskiej.

Przekłada się to bezpośrednio na wzrost produktywności o 20% i wzrost o 30% wynikający z inwestycji [ICT 2009]. Taki wzrost jest możliwy dzięki dynamice i innowacyjności przedsiębiorstw oraz ich wpływowi na działania w innych obszarach. Wzrosło również społeczne znaczenie technologii informacyjnych.

Przedstawiona przez Komisję Europejską „Strategia Europa 2020" zakłada wysoki poziom zatrudnienia, gospodarkę niskoemisyjną, wydajność i spójność społeczną. Zasadniczym celem agendy cyfrowej jest uzyskanie trwałych korzyści społeczno-ekonomicznych wynikających z jednolitego rynku cyfrowego przy wykorzystaniu szybkich i bardzo szybkich sieci szerokopasmowych oraz aplikacji interoperacyjnych. W ramach agendy cyfrowej zidentyfikowano następujące obszary:

- dynamiczny jednolity rynek cyfrowy – otwarcie dostępu do treści w internecie, zbiorowe zarządzanie prawami autorskimi i ich przejrzystość, system licencjonowania, ułatwienie transakcji internetowych i transgranicznych (Jednolity Europejski Obszar Płatniczy – SEPA),
- interoperacyjność i normy – doskonalenie procesu opracowywania norm z zakresu IT, promocja szerszego stosowania norm, zwiększenie interoperacyjności,
- zaufanie i bezpieczeństwo – ochrona infrastruktury informatycznej, ukierunkowane działania dotyczące bezpieczeństwa informacji,
- szybki i bardzo szybki dostęp do internetu – zapewnienie powszechnego dostępu do szerokopasmowego internetu nowej generacji – otwarty i neutralny internet,
- badania i innowacje – zwiększenie efektywności, stymulowanie innowacji,
- zwiększenie wykorzystania narzędzi informatycznych i przeciwdziałanie wykluczeniu społecznemu – umiejętność wykorzystywania narzędzi informatycznych, usługi cyfrowe.

Pobudzenie gospodarki może być uzyskane poprzez wykorzystanie potencjału intelektualnego i informatyzacji. Koherencja wiedzy, kreatywności i innowacyjności jest kluczowym elementem budowania przewagi konkurencyjnej przedsiębiorstw. Poziom umiejętności internetowych w Europie ocena się na podstawie sześciu umiejętności, których posiadanie świadczy o kompetencjach:

- stosowanie wyszukiwarki internetowej,
- wysyłanie e-maila z załącznikami,
- umieszczanie postów na czacie lub forum dyskusyjnym.
- stosowanie programów do wymiany plików P2P (ang. *peer to peer*),
- telefonowanie przez internet,
- budowanie stron internetowych.

Zgodnie z Europejską Agendą Cyfrową do 2020 roku powinien być zapewniony dostęp do szybkich (co najmniej 30 Mb/s) i bardzo szybkich (co najmniej 100 Mb/s) sieci szerokopasmowych. Zakłada się, że w przypadku dostępu do szybkich sieci szerokopasmowych wskaźnik pokrycia powinien wynosić 100%,

a dla dostępu do bardzo szybkich sieci szerokopasmowych – 50%. W przypadku wskaźnika gospodarki cyfrowej i społeczeństwa cyfrowego w 2015 roku Polska z indeksem DESI[1] wynoszącym 0,38 (w skali 0–1) zajmuje 23. miejsce wśród krajów członkowskich Unii Europejskiej (średnia unijna to 0,47). W zakresie korzystania z mobilnych usług szerokopasmowych Polska jest na 5. miejscu w tym rankingu. Zaledwie 60% gospodarstw domowych w Polsce posiada stacjonarne połączenie z internetem (23. miejsce). 63% Polaków korzysta z internetu, a podstawowe umiejętności informatyczne ma 46% obywateli, co oznacza, że jest to nadal poniżej średniej Unii Europejskiej (59%) [Europejska Agenda Cyfrowa 2015]. Zatem postęp w tym obszarze nie jest wystarczający, choć w porównaniu z poprzednim rokiem Polska awansowała w tym rankingu o jedną pozycję.

Aspekty normalizacyjne odgrywają szczególną rolę w dwóch obszarach agendy cyfrowej: interoperacyjność oraz zaufanie i bezpieczeństwo. Z punktu widzenia edukacji ważny jest także obszar dotyczący przeciwdziałaniu wykluczeniu społecznemu.

Interoperacyjność

Budowa społeczeństwa informacyjnego powinna bazować przede wszystkim na zapewnieniu interoperacyjności produktów i usług IT. Droga do uzyskania interoperacyjności wiedzie przez normy. Kontynuowany przegląd europejskiej polityki normalizacyjnej może stworzyć takie podstawy prawne w zakresie opracowywania norm, które umożliwią przystosowanie się do dynamicznie zmieniających się rynków technologicznych.

Wytyczne zawarte w planowanej reformie polityki normalizacyjnej w zakresie transparentnych zasad ujawniania informacji o prawach własności intelektualnej i warunkach licencjonowania, wspólnie z nowymi przepisami antymonopolowymi w zakresie porozumień korporacyjnych, stwarza podstawy do obniżenia opłat licencyjnych, co ułatwia wejście firmy na rynek.

Większe stosowanie norm przy dostawach systemów informatycznych i świadczonych usług IT umożliwią większą konkurencyjność i zmniejszą ryzyko uzależnienia się od jednego dostawcy.

Przyjęcie Europejskiej Strategii Interoperacyjności i Europejskich Ram Interoperacyjności jest kluczowym działaniem w ramach upowszechniania interoperacyjności w administracji publicznej. W tym celu wymagana jest analiza wprowadzenia mechanizmów do licencjonowania informacji dotyczących interoperacyjności przy zapewnieniu konkurencyjności i promocji innowacyjności.

[1] Digital Economy and Society Index – złożony wskaźnik opracowany przez Komisję Europejską (DG CNECT) w celu dokonania oceny rozwoju krajów Unii Europejskiej na drodze do gospodarki cyfrowej i społeczeństwa cyfrowego.

Polska wypełniła tę regulację, wydając rozporządzenie Rady Ministrów z 12 kwietnia 2012 roku w sprawie tak zwanych Krajowych Ram Interoperacyjności, które dotyczą sposobu wyboru środków, metod i standardów stosowanych do opracowania, implementacji, eksploatacji i doskonalenia systemu informatycznego, wprowadzenia określonych procedur organizacyjnych oraz metod wyboru norm, standardów, dobrych praktyk w zakresie interoperacyjności organizacyjnej, semantycznej i technologicznej, przy zapewnieniu neutralności technologicznej. Interoperacyjność może być uzyskana przez:

- stosowanie norm, kompatybilnych standardów i procedur,
- możliwość zastąpienia produktu, procesu, usługi bez zakłócenia informacji między podmiotami a ich klientami, przy zachowaniu wymagań funkcjonalnych współpracujących systemów,
- przydatność produktów, procesów i usług do wspólnego użytkowania, przy zapewnieniu spełnienia istotnych wymagań i uniknięcia niepożądanych efektów.

Interoperacyjność na poziomie organizacyjnym jest realizowana przez:

- informowanie o sposobie dostępu i zakresie serwisów oraz wskazanie miejsca ich publikacji,
- ujednolicenie procedur w celu zapewnienia współpracy podmiotów,
- publikowanie opisów procedur obowiązujących przy załatwianiu spraw drogą elektroniczną.

Na poziomie semantycznym interoperacyjność jest osiągana przez stosowanie ustalonych struktur danych i znaczenia danych w tych strukturach, publikowanych w repozytorium interoperacyjności oraz stosowanie w rejestrach odwołań do rejestrów zawierających dane referencyjne.

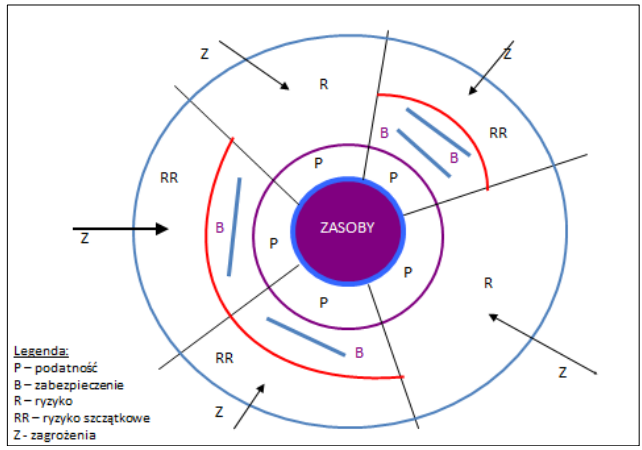
Poziom technologiczny może być osiągnięty przez stosowanie Polskich Norm, norm międzynarodowych oraz standardów uznanych za tak zwane dobre praktyki [ICT 2009]. W tym rozporządzeniu zapisano, że każda instytucja realizująca zadania publiczne powinna wdrożyć System Zarządzania Bezpieczeństwem Informacji według normy PN-ISO/IEC 27001, co z kolei implikuje wykorzystanie norm w celu ustanowienia zabezpieczeń (PN-ISO/IEC 27002), zarządzania ryzykiem (PN-ISO/IEC 27005) oraz odtwarzania techniki informatycznej po katastrofie (PN-ISO/IEC 24762). Natomiast projektowanie, wdrażanie, eksploatowanie, monitorowanie i utrzymanie oraz udoskonalanie zarządzania systemami informatycznymi powinno się odbywać z uwzględnieniem norm dotyczących systemu zarządzania usługami IT (PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2).

Bezpieczeństwo informacyjne (cyberbezpieczeństwo)

Użytkownicy korzystający z internetu powinni czuć się bezpieczni – zero tolerancji dla cyberprzestępczości. Zaawansowane usługi internetowe, na przykład bankowość elektroniczna czy e-zdrowie, e-edukacja, jako nowoczesne technolo-

gie powinny być wiarygodne. Coraz częściej komputery użytkowników końcowych są narażone na zagrożenia, których rozpowszechnienie jest tak duże, że staje się poważnym problem i konieczne jest podejmowanie działań systemowych.

Bezpieczeństwo informacji jest problemem rozpatrywanym w wielu aspektach. Znormalizowany ogólny model bezpieczeństwa informacji przedstawia rysunek 1.



Rysunek 1. Ogólny model bezpieczeństwa informacji [Krawiec 2012]

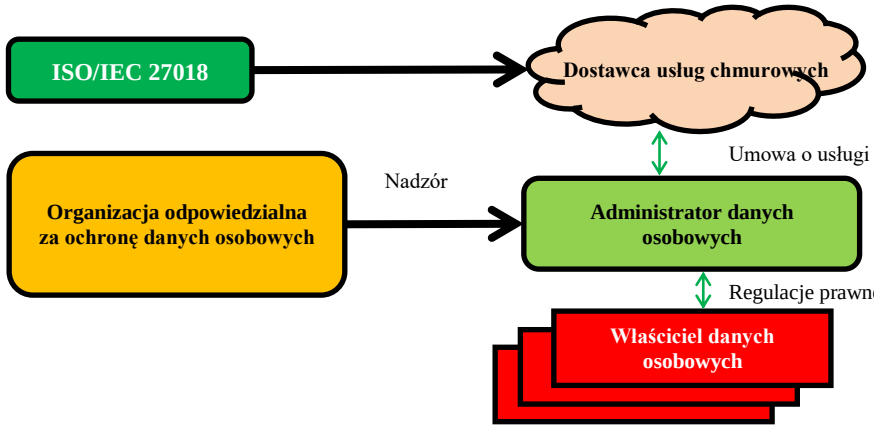
Zabezpieczenia mogą być skuteczne, jeśli ryzyko związane z zagrożeniami lub podatnościami będzie zminimalizowane. Sprowadzenie ryzyka do poziomu akceptowalnego może czasami wymagać wprowadzenie kilku zabezpieczeń. Nie wprowadza się zabezpieczeń, jeśli poziom ryzyka jest akceptowalny, nawet jeśli istnieją podatności, gdyż nie są znane zagrożenia, które te podatności mogłyby wykorzystać. Wszystkie te ograniczenia determinują wybór konkretnych zabezpieczeń. Najogólniej można podzielić zagrożenia na zależne od człowieka (świadome, przypadkowe) oraz niezależne (środowiskowe), co przedstawiono w tabeli 1.

Tabela 1. Rodzaje zagrożeń [Krawiec 2012]

Zależne od człowieka		**Niezależne od człowieka**
Świadome	**Przypadkowe**	**Środowiskowe**
Podsłuchanie	Pomyłki	Klęski żywiołowe (trzęsienie ziemi, pożar, powódź, wyładowania atmosferyczne, burze magnetyczne)
Hacking (wprowadzenie kodu złośliwego, modyfikacja informacji, szpiegostwo przemysłowe, sabotaż)	Skasowanie pliku	
	Przekierowania	

Systemy wspierające zarządzanie informacją są ważnymi aktywami każdej instytucji. Zapewnienie odpowiedniego poziomu bezpieczeństwa informacji jest niezbędne dla utrzymania pozycji rynkowej, zachowania płynności finansowej, spełnienia wymagań prawnych czy wizerunku instytucji tak mocno nadszarpniętego podczas ostatnich ataków hakerów na witryny rządowe w ramach protestów przeciwko porozumieniu ACTA.

Bardzo ważną kwestią w społeczeństwie informacyjnym jest budowa zaufania poprzez ochronę prywatności. Ma to szczególne znaczenie w odniesieniu do ochrony danych osobowych przetwarzanych w chmurze.



Rysunek 2. Zarządzanie danymi osobowymi w chmurze [ISO/IEC 27018:2014]

Zagrożenia stają się coraz bardziej wyrafinowane i przysparzają znacznych strat w wymiarze materialnym i niematerialnym. Bezpieczeństwo informacji poprzez minimalizację ryzyka w działalności biznesowej i ochronie infrastruktury krytycznej jest ważne zarówno dla sektora publicznego, jak i komercyjnego. Podstawą bezpieczeństwa informacji powinny być procedury bezpieczeństwa wspierane przez środki techniczne.

Określenie rodzaju mechanizmów zarządzania bezpieczeństwem informacji wymaga starannego i szczegółowego planowania, przy zaangażowaniu wszystkich pracowników danej instytucji. Wybór zabezpieczeń powinien być poprzedzony określeniem wymagań bezpieczeństwa, zidentyfikowaniem ryzyka, ustaleniem jego poziomu akceptacji oraz sposobu postępowania z ryzykiem, a także wytycznych w zakresie zarządzania ryzykiem w instytucji. Skuteczna ochrona informacji zależy od następujących czynników [**PN-ISO/IEC 27001:2014-12**]:

– polityki bezpieczeństwa informacji i celów biznesowych,
– zaangażowania kierownictwa,
– zrozumienia wymagań bezpieczeństwa informacji oraz zarządzania ryzykiem,

- podejścia instytucji do zagadnień bezpieczeństwa informacji,
- propagowania wymagań i zaleceń bezpieczeństwa informacji wśród współpracowników,
- finansowania działań związanych z zarządzaniem bezpieczeństwem informacji,
- zapewnienia odpowiedniej świadomości, kształcenia i szkoleń,
- ustanowienia procedury zarządzania incydentami związanymi z bezpieczeństwem informacji,
- wdrożenia mierników efektywności systemu zarządzania bezpieczeństwem informacji.

Problematyka dotycząca bezpieczeństwa informacyjnego (cyberbezpieczeństwa) jest uwzględniona w Polityce ochrony cyberprzestrzeni Rzeczypospolitej Polskiej (uchwała Rady Ministrów z 25 czerwca 2013 roku), Europejskiej Agendzie Cyfrowej (Polskiej Agendzie Cyfrowej), a ściślej w Europejskich Ramach Interoperacyjności (Krajowych Ramach Interoperacyjności – rozporządzenie Rady Ministrów z 12 kwietnia 2012 roku), w doktrynie Biura Bezpieczeństwa Narodowego z 2015 roku pod nazwą „Bezpieczeństwo informacyjne". Bezpieczeństwo informacyjne obejmuje również ochronę danych osobowych (ustawa o ochronie danych osobowych), własności intelektualnej (ustawa o prawie autorskim i prawach pokrewnych) oraz tajemnicę przedsiębiorstwa (ustawa o ochronie konkurencji i konsumentów). Kształcenie powinno się opierać na normach międzynarodowych ISO/IEC dotyczących systemowego podejścia do bezpieczeństwa informacji.

Terminologia dotycząca cyberbezpieczeństwa to już nie tylko rozumienie takich pojęć, jak: *phising*, *malware* (oprogramowanie złośliwe), wirus, robak czy trojan, lecz także znajomość takich terminów, jak: *rogueware* (symulacje zakażone wirusem w celu ściągnięcia fałszywego oprogramowania antywirusowego), *ransomware* (zastraszanie użytkowników przez podszywanie się pod organy ścigania lub organizacje chroniące prawa autorskie), *malvertising* (reklamy online rozprzestrzeniające złośliwy kod) oraz *spear-phishing* (instalacja dedykowanego oprogramowania szpiegowskiego na komputerach).

Program Operacyjny Innowacyjna Gospodarka

Program Operacyjny Innowacyjna Gospodarka (POIG) jest jednym ze sposobów realizacji celów określonych w Narodowych Strategicznych Ramach Odniesienia. Głównym celem POIG jest wspieranie innowacyjności. Cele szczegółowe POIG, które są bezpośrednio związane z nauką, to wzrost konkurencyjności nauki oraz wykorzystanie technologii informacyjnych. W odniesieniu do społeczeństwa informacyjnego POIG zakładał realizację w ramach 7. priorytetu – budowa elektronicznej administracji oraz 8. priorytetu – zwiększanie innowacyjności gospodarki. Te priorytety są realizowane w synergii, aby

e-usługi publiczne przyczyniały się do rozwoju gospodarczego i zmniejszały bariery administracyjne w odniesieniu do działalności innowacyjnej.

Nadal jednak jest zbyt mało sukcesów w tym obszarze, zatem każdy pozytywny przykład godny jest naśladowania i skorzystania z doświadczeń instytucji, które takie projekty zrealizowały.

Portal e-Norma – przykład skutecznego wdrożenia

W latach 2010–2013 Polski Komitet Normalizacyjny (PKN) realizował projekt Portal e-Norma – część II. Projekt był realizowany w ramach Programu Operacyjnego Innowacyjna Gospodarka, Priorytet VII – Społeczeństwo informacyjne, budowa elektronicznej administracji.

Zharmonizowany ze „Strategią Informatyzacji PKN na lata 2009–2013" projekt miał na celu wdrożenie rozwiązań polegających na stworzeniu publicznej platformy elektronicznej umożliwiającej powszechny dostęp firm, instytucji naukowych, publicznych i innych użytkowników do informacji i usług normalizacyjnych, integrację referencyjnych rejestrów i zasobów normalizacyjnych. Przedsięwzięcie było realizowane w ramach następujących podsystemów:

- Portal Polski Zasób Normalizacyjny (PZN) – platforma sprzętowo-programowa ORACLE oparta na Sun Exadata Database Machine oraz system zbudowany w technologii Spring i JEE,
- System Wirtualizacji Zasobów – system na platformie Microsoft Office SharePoint Server (repozytorium dokumentów w formacie XML), BizTalk Adapter oraz serwer bazodanowy,
- System Cyfrowej Sprzedaży Produktów i Usług – zastosowane technologie: Magento Community, PHP, MySQL, Java,
- Zarządzanie wiedzą normalizacyjną i e-Learning – system zbudowany na platformie Java; zastosowano technologię responsywną dostosowaną do urządzeń stacjonarnych i mobilnych.

Wskaźniki produktu oraz rezultatu przedstawiono odpowiednio w tabelach 2 i 3 [**portal e-Norma 2009**].

Tabela 2. Wskaźniki produktów

Nazwa wskaźnika	Jednostka	2009 rok	Planowano 2013 rok	Realizacja 2013 rok
Wydajność bazy danych PZN	IOPS[2]	46 673	225 000	375 000
Elektroniczne zasoby w formacie XML	%	0	100	100
Liczba nowych platform elektronicznych	–	0	1	1 (www.wiedza.pkn.pl)

[2] *Input-output per second* (liczba operacji wejścia–wyjścia na sekundę).

Tabela 3. Wskaźniki rezultatu

Nazwa wskaźnika	2009 rok	Planowano 2013 rok	Realizacja 2013 rok
Liczba podmiotów, które skorzystały z usług online	0	3000	> 3000
Liczba rejestrów publicznych dostępnych online	0	1	1
Liczba udostępnionych usług publicznych online	1	4	4

Rezultaty są zdefiniowane jako efekty bezpośrednio powstałe po zakończeniu projektu. Ponieważ projekt koncentruje się na szerokim udostępnieniu przedsiębiorcom i obywatelom, a także instytucjom publicznym zdigitalizowanych zasobów i usług normalizacyjnych, określano następujące wskaźniki rezultatów:

Liczba usług publicznych powstałych w wyniku realizacji projektu opiera się na zasadniczym założeniu projektu, zgodnie z którym następujące usługi będą oferowane w ramach portalu:

- czytelnia online – odczytywanie zasobów bezpośrednio podczas przeglądania strony internetowej,
- sklep online oferujący normy, książki i czasopisma o tematyce normalizacyjnej,
- informacje i porady normalizacyjne online,
- kursy e-learningowe mające na celu popularyzację wiedzy normalizacyjnej.

Osiągnięto cel generalny projektu, czyli wzrost konkurencyjności polskiej gospodarki w wyniku zastosowania technologii informatycznych w procesach tworzenia, promocji i rozpowszechniania norm. Portal e-Norma ma również zdefiniowane następujące cele szczegółowe:

- poprawa skuteczności i efektywności działania PKN w wyniku szerokiego zastosowania w pełni zintegrowanych systemów informatycznych,
- rozwój systemu dostępu wszystkich zainteresowanych osób i klientów, w szczególności przedsiębiorców, do informacji i usług PKN,
- zwiększenie konkurencyjności polskich przedsiębiorstw na wspólnym rynku europejskim i na rynkach międzynarodowych.

Beneficjentami projektu są eksperci techniczni, którym dostarczono nowych narzędzi informatycznych do prac normalizacyjnych, przedsiębiorcy, którzy uzyskali swobodny, pełny dostęp do zasobów PKN, oraz instytucje publiczne i społeczeństwo, które mają możliwość łatwego dostępu do zdigitalizowanych zasobów normalizacyjnych.

Podsumowanie – wnioski

W zakresie kształcenia i zatrudniania specjalistów IT w Polsce pozostaje jeszcze wiele do zrobienia. Większa liczba absolwentów kierunków ścisłych niż w większości krajów Unii Europejskiej nie przekłada się na zwiększenie liczby

specjalistów z dziedziny IT pracujących w kraju. Kluczem do konkurencyjnej gospodarki cyfrowej jest stworzenie warunków łatwego dostępu do internetu oraz promowanie umiejętności informatycznych wśród obywateli, co jest istotnym czynnikiem pobudzającym rozwój społeczeństwa cyfrowego. Jest to również warunek *sine qua non* sukcesu gospodarczego.

W warunkach rozwoju społeczeństwa cyfrowego normalizacja odgrywa kluczową rolę w aspekcie interoperacyjności, cyberbezpieczeństwa oraz kompetencji cyfrowych (na przykład Krajowe Ramy Kwalifikacji) poprzez czynny udział w opracowaniu norm z zakresu IT, a także poprzez bierne uczestnictwo w działalności normalizacyjnej, czyli wykorzystaniu sprawdzonych rynkowo najnowszych osiągnięć nauki i techniki.

Literatura

Europejska Agenda Cyfrowa według stanu na 16 czerwca 2015 roku. Materiały OIDE.

ICT Shaping the World: A Scientific View (2009), ETS.

ISO/IEC 27018:2014 Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. ISO, Genewa.

Krawiec J. (2012), *Zabezpieczanie danych*, cz. I: *SZBI – systemowa pewność danych*, „ITprofessional" nr 6.

PN-ISO/IEC 27001:2014-12 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania, Warszawa.

Portal e-Norma w Polskim Komitecie Normalizacyjnym, część II – Studium Wykonalności (2009), Warszawa.