Julia Kudła[1], Piotr Filipkowski[2]

Analiza systemu bezpieczeństwa informacji w kontekście regulacji techniczno-prawnych w służbie zdrowia

Streszczenie
W artykule przedstawiono analizę systemu bezpieczeństwa informacji w ochronie zdrowia. Mając na uwadze to, że aplikacje składające się na system bezpieczeństwa są tworzone bezpośrednio na podstawie aktów prawnych obowiązujących w państwie, na które z kolei wpływ mają międzynarodowe standardy techniczne, został zbadany stopień zgodności norm prawnych z normami technicznymi związanymi z tematyką ochrony informacji w służbie zdrowia. Dana zależność była obserwowana w zakresie obszaru regulacji oraz cech informacji, na które składają się kryteria jakości informacji i atrybuty ochrony informacji, za pomocą metodologii zaproponowanej przez prof. J. Oleńskiego, związanej z modelem N i modelem P. Pozytywnie została zweryfikowana hipoteza o niewystarczająco silnym odwzorowaniu norm technicznych w aktach prawnych.
Słowa kluczowe: system bezpieczeństwa informacji, służba zdrowia

1. Wprowadzenie

W artykule przedstawiono charakterystykę systemu bezpieczeństwa informacji w ochronie zdrowia. Na formę oprogramowania funkcjonującego w jego ramach bezpośrednie przełożenie mają akty prawne obowiązujące w państwie. Te z kolei często są tworzone na podstawie międzynarodowych standardów technicznych redagowanych przez takie specjalistyczne organizacje normalizacyjne, jak ISO (International Organization for Standardization). Za cel tej pracy przyjęto dokonanie analizy systemu bezpieczeństwa informacji w służbie zdrowia ze szczególnym uwzględnieniem regulacji, które mają wpływ na jego konstrukcję.

[1] Szkoła Główna Handlowa w Warszawie, Kolegium Analiz Ekonomicznych, Niestacjonarne Studia Doktoranckie, julia.ren.kudla@gmail.com.
[2] Szkoła Główna Handlowa w Warszawie, Kolegium Analiz Ekonomicznych, Zakład Zarządzania Informatyką, Instytut Informatyki i Gospodarki Cyfrowej, pfilip@sgh.waw.pl.

Przedmiotem badania było określenie współzależności między normami prawnymi a technicznymi, tak aby możliwe było zweryfikowanie hipotezy o niewystarczająco silnym odwzorowaniu norm technicznych w aktach prawnych.

Na potrzeby niniejszej pracy przez pojęcie systemu bezpieczeństwa informacji rozumie się zorganizowaną w celu zapewnienia bezpieczeństwa arystotelesowską całość istniejącą w systemie informacyjnym, będącą efektem synergii wzajemnie powiązanych ze sobą relacjami i dynamicznych części o danej strukturze i organizacji[3]. Opisywany system powinien charakteryzować się określonymi właściwościami i jakością, jak również przejawiać *kompleksowość* zastosowanych zabezpieczeń[4]. Do analizy wybrano akty prawne i normy techniczne uznane za te o największym wpływie na bezpieczeństwo danych w służbie zdrowia. Zostały one przedstawione w tabeli 1.

Tabela 1. Akty prawne i normy techniczne wykorzystane w analizie systemu bezpieczeństwa informacji w służbie zdrowia

Akty prawne	Skrót
Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, DzU z 1997 r., nr 133, poz. 883	u.o.d.o.
Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, DzU z 2009 r., nr 52, poz. 417	u.p.p.
Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, DzU z 2011 r., nr 113, poz. 657	u.s.i.o.z.
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, DzU z 2004 r., nr 100, poz. 1024	r.d.p.d.o.
Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, DzU z 2012 r., poz. 526	r.k.r.i.
Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania, DzU z 2015 r., poz. 2069	r.r.z.d.m.
Normy techniczne	
ISO/IEC 27000:2016 Information technology – Security techniques – Information security management systems – Overview and vocabulary	ISO 27000

[3] Na podstawie: P. Filipkowski, *Istota i cel systemu*, w: *Wstęp do informatyki gospodarczej. Zajęcia laboratoryjne*, red. K. Polańska, Oficyna Wydawnicza SGH, Warszawa 2015, s. 11.

[4] Ibidem, s. 27.

Normy techniczne	
ISO/IEC 27001:2013 Information technology l' Security techniques – Information security management systems – Requirements	ISO 27001
ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls	ISO 27002
PN-ISO/IEC 27005:2014–01 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji	ISO 27005
PN-ISO/IEC 27006:2016–12 Technika informatyczna – Techniki bezpieczeństwa – Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji	ISO 27006
ISO/IEC 27017:2015 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services	ISO 27017
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 27018
PN-ISO/IEC 12052:2012 Informatyka w ochronie zdrowia – Obrazowanie cyfrowe i przesyłanie obrazów w medycynie (DICOM), łącznie z przepływem zadań i zarządzaniem danymi	DICOM
PN-EN ISO 10781:2015–11 Informatyka w ochronie zdrowia – Model funkcjonalny systemu elektronicznej dokumentacji zdrowotnej HL7	HL7
ISO 27799:2016 Health informatics – Information security management in health using ISO/IEC 27002	ISO 27799

Źródło: opracowanie własne.

Ratownictwo medyczne to w istocie „gotowość ludzi, zasobów i jednostek organizacyjnych do podejmowania medycznych czynności ratunkowych"[5] i jako taki jest systemem organizacyjnym, który stanowi jeden z kluczowych filarów bezpieczeństwa zdrowotnego obywateli. System Państwowego Ratownictwa Medycznego (dalej PRM) realizuje zadania państwa, oferując pomoc każdej osobie znajdującej się w stanie nagłego zagrożenia zdrowotnego[6]. Głównym celem funkcjonowania systemu ratownictwa medycznego jest bowiem ratowanie życia i zdrowia ludzkiego bez względu na czas, miejsce i możliwości płatnicze pacjenta. Skuteczna realizacja tej misji jest uwarunkowana efektywną współpracą podmiotów działających w ramach jego struktury[7].

[5] R. Gałązkowski, *Ratownictwo medyczne w Polsce. Komentarz do Ustawy z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym*, Wydawnictwo Centrum Szkolenia Policji w Legionowie, Warszawa 2007, s. 7.

[6] Tekst jedn. DzU z 2016 r., poz. 1868, art. 1.

[7] A. Trzos, M. Kapler, *Zarządzanie ratownictwem medycznym przy wykorzystaniu rozwiązań systemowych i nowoczesnych technologii informatycznych*, w: *Medycyna ratunkowa w Polsce*, red. J. Jakubaszko, Polsce Towarzystwo Medycyny Ratunkowej, Wrocław 2010, s. 145.

Prawidłowy przepływ informacji podczas akcji ratunkowej ma kluczowe znaczenie dla skutecznej działalności służb medycznych. Jakość wymiany informacji pomiędzy służbami działającymi na miejscu, a także między nimi a dyspozytorami, osobami koordynującymi oraz miejscami, z których i do których są transportowani poszkodowani może decydować o sprawności systemu wykorzystywanego w nagłych zdarzeniach[8].

W zależności od fazy przeprowadzanej akcji ratowniczej inny jest charakter przekazywanej informacji. Pierwsze informacje są niezwykle istotne, ponieważ determinują fazę reagowania. Z powodu nieprecyzyjnie przekazanej informacji, np. od przypadkowego świadka, może dojść do niewłaściwej reakcji na zdarzenie. W związku z częstym utrudnieniem dotyczącym pozyskiwania informacji od osoby dokonującej zgłoszenia, zwykle za pierwszą wiarygodną informację uznaje się tę otrzymaną od służb ratowniczych z miejsca zdarzenia. Udzielają one takich informacji, jak: dokładna lokalizacja zdarzenia, zagrożenia obecne i potencjalne, liczba ofiar, charakter obrażeń, wymagana pomoc. Informacje te są w trybie natychmiastowym przekazywane wszystkim służbom obecnym podczas akcji ratunkowej, na ich podstawie dokonuje się segregacji medycznej[9].

Informacja pozyskiwana przez PRM odgrywa ogromną rolę w sytuacji ratowania ludzkiego życia i zdrowia przez osoby będące w pełnej gotowości, by odpowiedzieć na wezwanie pomocy. W związku z tym ochrona tej informacji i dbałość o jej bezpieczeństwo są niezwykle istotne.

2. Analiza współzależności norm technicznych i aktów prawnych w kontekście zastosowania systemów teleinformatycznych w służbie zdrowia

2.1. Metodologia

W badaniu systemu bezpieczeństwa informacji w służbie zdrowia wykorzystano analizę porównawczą norm technicznych i aktów prawnych, aby wyznaczyć współzależności występujące pomiędzy tymi dokumentami i ich wpływ na stan bezpieczeństwa informacji. Zastosowane podejście odnosi się do

[8] *Logistyka działań służb ratowniczych w zdarzeniach masowych*, www.logistyka.net.pl/bank-wiedzy/logistyka/item/download/79374_e8eb9b881028a4493ed98fb3a30d173e (data odczytu: 23.04.2017).

[9] Ibidem.

modelu N i modelu P przedstawionych przez prof. Józefa Oleńskiego na konferencji „Informacja w społeczeństwie XXI wieku" w Olsztynie[10].

U podstaw powstawania norm technicznych leżą potrzeby rynkowe związane ze wzrostem jakości produktów i usług, a także bezpieczeństwa. Kluczową kwestią może być taka organizacja uwarunkowań prawnych, aby tworzone na ich podstawie aplikacje i systemy informatyczne infrastruktury państwa miały jak najwydajniejszą żywotność i by optymalizowane były wydatki na ich aktualizację[11].

2.2. Analiza zgodności ze względu na cechy informacji

W tabeli 2 przedstawiono, które akty prawne oraz normy techniczne uwzględniają dane atrybuty ochrony informacji oraz kryteria jakości informacji[12]. Macierz ta obrazuje skupienie poszczególnych dokumentów regulujących ochronę informacji na danych cechach informacji, a ponadto daje możliwość przeglądu, które spośród atrybutów i kryteriów są wykorzystane najczęściej, natomiast które sporadycznie. Przede wszystkim z przedstawionego ujęcia wynika, że ustawodawca oraz twórcy norm technicznych uznali za najistotniejsze takie cechy, jak tajność i integralność informacji.

Tabela 2. Atrybuty ochrony informacji i kryteria jakości informacji ujęte w danych aktach prawnych i normach technicznych

	Tajność	Integralność	Dostępność	Rozliczalność	Niezaprzeczalność	Autentyczność	Relewantność	Dokładność	Aktualność	Kompletność	Spójność	Odpowiedniość formy	Wiarygodność
u.o.d.o.	x			x		x			x	x			
u.p.p.	x		x				x	x				x	
u.s.i.o.z.	x	x	x	x		x	x		x	x		x	
r.d.p.d.o.	x	x		x									
r.k.r.i.	x	x	x	x	x	x							
r.r.z.d.m.	x	x				x	x		x	x	x	x	x

[10] J. Oleński, *Przyszłość rozwoju e-państwa, strategie rozwoju e-państwa w perspektywie 2030*, wykład z konferencji „Informacja w społeczeństwie XXI wieku", Olsztyn 2017.

[11] J. Oleński, *Infrastruktura informacyjna państwa w globalnej gospodarce*, Wydawnictwo UW, Warszawa 2006, s. 571.

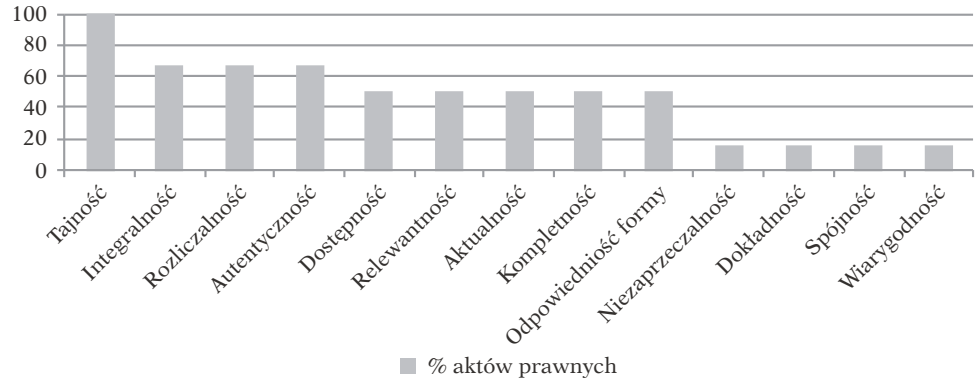
[12] K. Liderman, *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012, s. 18–19.

cd. tabeli 2

	Tajność	Integralność	Dostępność	Rozliczalność	Niezaprzeczalność	Autentyczność	Relewantność	Dokładność	Aktualność	Kompletność	Spójność	Odpowiedniość formy	Wiarygodność
ISO 27000	x	x	x		x	x	x				x		
ISO 27001	x	x	x				x					x	
ISO 27002		x	x	x		x		x	x	x			
ISO 27005	x	x	x	x	x	x							
ISO 27006	x	x	x		x								
ISO 27017	x	x	x	x							x	x	
ISO 27018	x	x	x	x							x	x	
DICOM												x	
HL7	x	x					x						
ISO 27799	x	x	x	x		x		x	x	x			

Źródło: opracowanie własne.

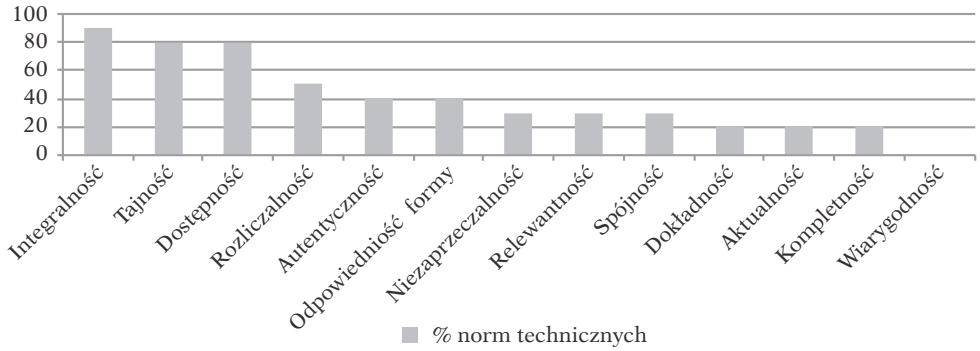
W celu badań porównawczych zostało stworzone zestawienie wykorzystania we wskazanych aktach prawnych i normach technicznych cech informacji. Na rysunkach 1 i 2 przedstawiono udział ilościowy atrybutu ochrony informacji bądź kryterium jakości informacji w opisywanych w artykule aktach prawnych/normach technicznych.



Rysunek 1. Cechy informacji wskazane w aktach prawnych (w %)

Źródło: opracowanie własne.

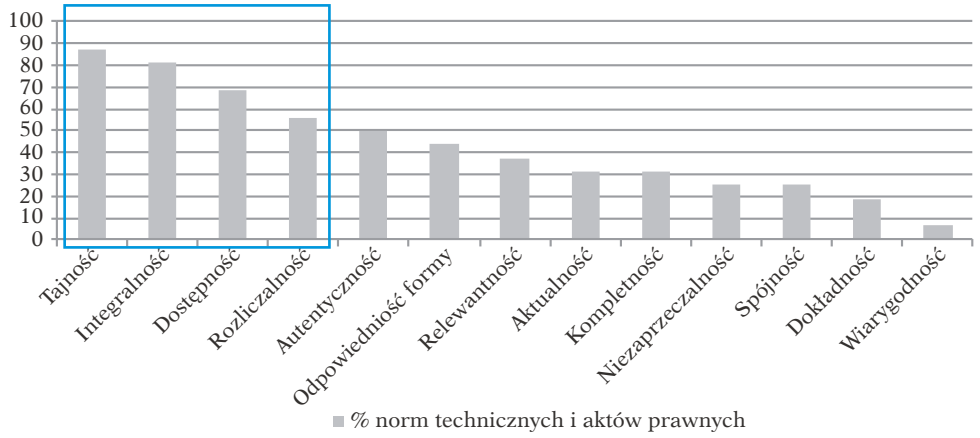
Ponad połowa aktów prawnych odnoszących się (w sposób bezpośredni bądź pośredni) do bezpieczeństwa informacji w służbie zdrowia reguluje przez wzgląd na takie cechy informacji, jak tajność, integralność, rozliczalność oraz autentyczność. Znacznie mniejsza ich część była pisana przy uwzględnieniu niezaprzeczalności, dokładności, spójności i wiarygodności.



Rysunek 2. Cechy informacji wskazane w normach technicznych (w %)

Źródło: opracowanie własne.

W przypadku norm technicznych najczęstsze wykorzystanie zaobserwowano w przypadku integralności, tajności i dostępności, natomiast zdecydowanie rzadkie dla wiarygodności, kompletności, aktualności oraz dokładności. W związku z tym można zauważyć, że twórcy standardów technicznych przywiązali większą wagę cesze jaką jest dostępność informacji, aniżeli polski ustawodawca.

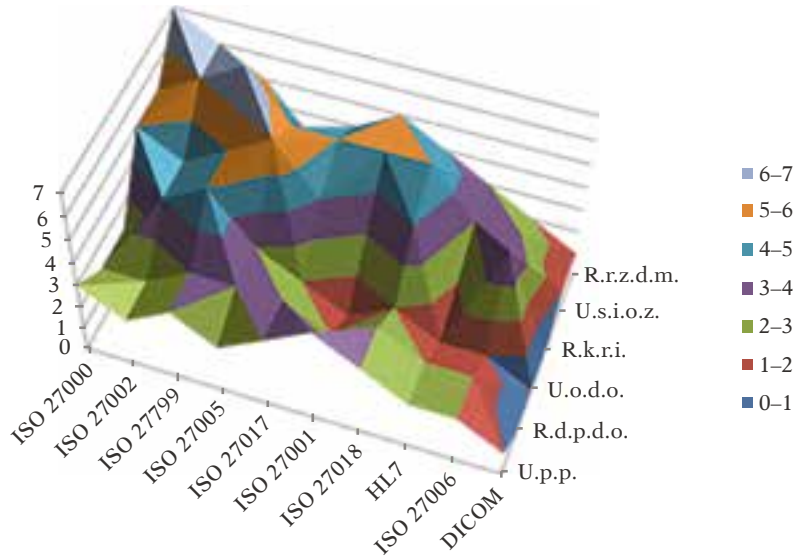


Rysunek 3. Cechy informacji wskazane w normach technicznych i aktach prawnych (w %)

Źródło: opracowanie własne.

Analiza wykazała, że przy tworzeniu wymienionych aktów prawnych i norm technicznych za najistotniejsze cechy informacji uznano tajność, integralność, dostępność oraz rozliczalność. Do nich nawiązuje ponad połowa analizowanych dokumentów (rysunek 3).

W dalszym kroku, z wykorzystaniem tabeli 2, skonstruowano macierz obrazującą stopień podobieństwa aktów prawnych i norm technicznych ze względu na wykorzystanie cech informacji. Spośród wymienionych aktów prawnych r.r.z.d.m. i u.s.i.o.z. wykazują największą dbałość o przejawienie w praktyce zdefiniowanych cech informacji (zidentyfikowano w nich największą liczbę opisanych cech). Poza cechami zawartymi w u.s.i.o.z., r.r.z.d.m. zawiera także spójność i wiarygodność. Wizualizacja zaprezentowana na rysunku 4 obrazuje liczbę pokrywających się cech informacji uporządkowaną malejąco.



Rysunek 4. Stopień zgodności aktów prawnych i norm technicznych pod względem kryteriów jakości informacji i atrybutów ochrony informacji

Źródło: opracowanie własne.

Największą zgodność zaobserwowano pomiędzy r.r.z.d.m. i ISO 27000 oraz u.s.i.o.z. i ISO 27799, a wartość tej miary wyniosła aż 7 wspólnych cech informacji. R.r.z.d.m. jest w dużej mierze zgodne także z ISO 27002, ISO 27799 i ISO 27001. U.s.i.o.z. wykazuje wysoką zgodność pod tym względem z ISO 27000, ISO 27002, ISO 27005, ISO 27017, ISO 27001, ISO 27018. Także r.k.r.i. jest podobne w ten sposób do ISO 27000, ISO 27005, ISO 27799. Poza tym jeszcze

u.o.d.o i ISO 27799 miały aż 5 wspólnych cech informacji. W ten sposób aktami prawnymi, które wykazują największe podobieństwo pod badanym kątem do standardów technicznych są: r.r.z.d.m., u.s.i.o.z. i r.k.r.i.

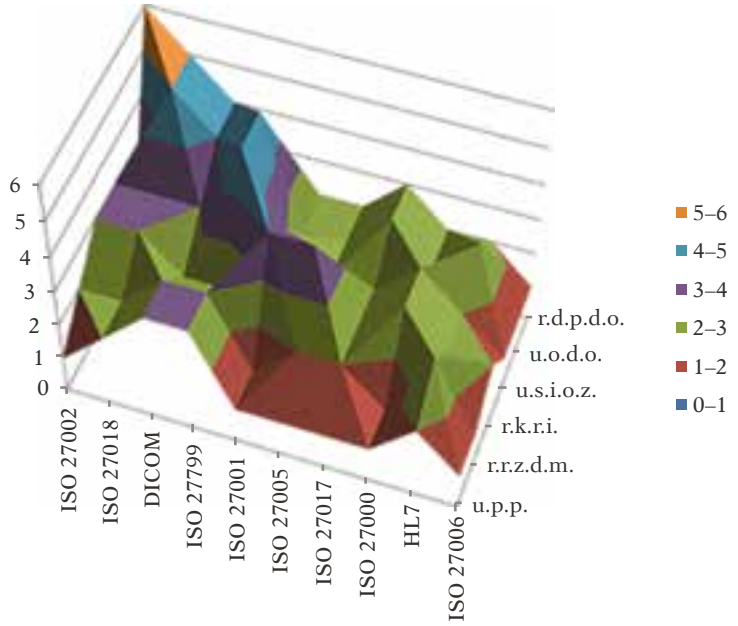
2.3. Analiza zgodności ze względu na zakres obszaru regulacji

Na potrzeby analizy zgodności w obszarze regulacji zbudowano macierz określającą, w jakim stopniu wybrane akty prawne i normy techniczne są ze sobą zgodne pod kątem obszaru regulacji. Wyniki przedstawiono na rysunku 5. Stopień zgodności został określony z wykorzystaniem skali zdefiniowanej w tabeli 3.

Tabela 3. Skala zastosowana do określenia budowy macierzy zgodności

	Opis słowny	Charakterystyka
(1)	Brak zgodności	• Brak choćby pośredniej zbieżności tematycznej.
(2)	Pośrednio podobne tematyką	• Brak bezpośredniej zbieżności tematycznej. • Pojedyncze punkty w ustawie mogą odnosić się do tematyki danej normy technicznej
(3)	Podobna tematyka	• Poruszany podobny temat, ale regulacje dotyczą zupełnie innych aspektów. • Tematy mogą się uzupełniać, nawet jeśli bezpośrednio nie regulują tego samego.
(4)	Zgodność na bardzo niskim poziomie	• Regulacje dotyczą podobnych aspektów, jednak inne są zalecane rezultaty. • Mogą pojawić się pojedyncze odwołania do danych norm technicznych.
(5)	Zgodność na niskim poziomie	• Regulacje dotyczą po części tych samych aspektów. • Mogą pojawić się pojedyncze odwołania do danych norm technicznych.
(6)	Zgodność na średnim poziomie	• Regulacje pokrywają się pod kątem jakościowym, jednak zauważalne jest to jedynie w poszczególnych fragmentach aktu prawnego. • Mogą wystąpić pojedyncze odwołania do danych norm technicznych.
(7)	Wyraźna zgodność	• Regulacje pokrywają się w znacznej mierze pod kątem objętościowym i jakościowym, tj. znaczna część aktu prawnego pokrywa się ze standardem technicznym.
(8)	Pełna zgodność	• Regulacje pokrywają się niemal w pełni pod kątem objętościowym i jakościowym, tj. cały akt prawny pokrywa się ze standardem technicznym. • Występują także nawiązania do danej normy technicznej w akcie prawnym.

Źródło: opracowanie własne.



Rysunek 5. Stopień zgodności norm prawnych i technicznych (z wykorzystaniem skali opisanej w tabeli 3)

Źródło: opracowanie własne.

Na wykresie przedstawionym na rysunku 5 najwyżej położony obszar, gdzie zbieżność tematyczna została określona jako „zgodność na średnim poziomie", dotyczy norm ISO 27002 i r.d.p.d.o. Kolejna co do siły współzależność, oznaczona jako „zgodność na niskim poziomie", wystąpiła pomiędzy ISO 27018 i u.o.d.o./r.d.p.d.o., a także między ISO 27799 i u.o.d.o./u.s.i.o.z. Posiłkując się opisaną skalą, można stwierdzić, że akty prawne regulujące bezpieczeństwo informacji (w tym w służbie zdrowia) są w niskim stopniu opracowywane na podstawie międzynarodowych standardów technicznych związanych z tą tematyką.

3. Podsumowanie i kierunek dalszych badań

Zarówno polski ustawodawca, jak i ISO wydając regulacje związane z ochroną informacji, za najważniejsze uznali takie cechy informacji, jak tajność i integralność. Niewątpliwie ma to istotne przełożenie na ochronę informacji przed nieuprawnionym dostępem czy manipulacją. Porównując priorytetowość cech

informacji wymaganych w aktach prawnych i normach technicznych, jest zauważalne, że w ustawach i rozporządzeniach rzadziej jest poruszany temat związany z dostępnością danych ze względu na wymagania użytkownika lub systemu. Być może jest to aspekt warty większej uwagi ze strony regulatora. Aktami prawnymi w największym stopniu adekwatnymi do norm technicznych pod względem cech informacji w nich opisanych są r.r.z.d.m., u.s.i.o.z. oraz r.k.r.i. Ostatni z wymienionych zawiera zapis dotyczący wymagania, aby system bezpieczeństwa informacji został stworzony na podstawie polskiej normy ISO 27001. W samej analizie jednak nie została zaobserwowana szczególna zgodność tych dokumentów pod żadnym z badanych aspektów. U.s.i.o.z. jest kluczową ustawą w procesie opracowywania aplikacji bezpieczeństwa informacji, dlatego wynik ten jest niewątpliwie pozytywny w kontekście stanu bezpieczeństwa systemu. Z dalszej części analizy wynika, że normy prawne stanowiące o bezpieczeństwie informacji nie są w zadowalającym stopniu opracowywane na podstawie standardów technicznych stworzonych przez międzynarodowe organizacje specjalizujące się w tej tematyce.

Niestety potwierdza to postawioną hipotezę o niewystarczająco silnym odwzorowaniu norm technicznych w aktach prawnych. W związku z kosztownością dodatkowych aktualizacji norm prawnych w celu osiągnięcia coraz lepszego dostosowania do wymagań i potrzeb wynikających ze zmian zachodzących na rynku, wydaje się nieefektywne, by rozkładać w czasie dodawanie regulacji, które są proponowane przez instytucje specjalizujące się w kwestiach bezpieczeństwa informacji. O ile instytucje mogą podjąć własną inicjatywę, by wdrożyć aplikacje na podstawie standardów technicznych, co może jednocześnie wyróżnić je spośród innych i stworzyć przewagę konkurencyjną, o tyle jeśli nie jest to wymagane prawnie, nie tworzy to powszechnie obowiązującego standardu jakości funkcjonowania danego państwa. Prawo powinno iść w parze z normami technicznymi i możliwościami technologicznymi. Jeśli nie jest z nimi zgodne, może powodować to niedogodności, takie jak podatności na zagrożenia systemów opartych na ustawach i rozporządzeniach funkcjonujących w całym państwie, dyskomfort ze strony użytkownika systemu czy obciążenie nadmiernymi kosztami.

W przyszłości warto poszerzyć zakres analizy o badanie świadomości istniejących regulacji pośród osób odpowiedzialnych w danych jednostkach służby zdrowia za bezpieczeństwo informacji medycznej, np. na SOR-ach. Wykorzystanie danych przepisów mających zastosowanie w jednostkach ochrony zdrowia w praktyce także zasługuje na uwagę i analizę efektywności.

Bibliografia

Filipkowski P., *Istota i cel systemu*, w: *Wstęp do informatyki gospodarczej. Zajęcia laboratoryjne*, red. K. Polańska, Oficyna Wydawnicza SGH, Warszawa 2015, s. 11.

Gałązkowski R., *Ratownictwo medyczne w Polsce. Komentarz do Ustawy z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym*, Wydawnictwo Centrum Szkolenia Policji w Legionowie, Warszawa 2007, s. 7.

Kudła J., *Analiza systemu bezpieczeństwa informacji w kontekście regulacji techniczno-prawnych w służbie zdrowia*, praca magisterska, Szkoła Główna Handlowa, Warszawa 2017.

Liderman K., *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012, s. 18–19.

Oleński J., *Infrastruktura informacyjna państwa w globalnej gospodarce*, Uniwersytet Warszawski, Warszawa 2006, s. 571.

Oleński J., *Przyszłość rozwoju e-państwa, strategie rozwoju e-państwa w perspektywie 2030*, wykład z konferencji „Informacja w społeczeństwie XXI wieku", Olsztyn 2017.

Trzos A., Kapler M., *Zarządzanie ratownictwem medycznym przy wykorzystaniu rozwiązań systemowych i nowoczesnych technologii informatycznych*, w: *Medycyna ratunkowa w Polsce*, red. J. Jakubaszko, Polsce Towarzystwo Medycyny Ratunkowej, Wrocław 2010, s. 145.

Ustawa z dnia 8 września 2006 r., o Państwowym Ratownictwie Medycznym, tekst jedn. DzU z 2016 r., poz. 1868.

Źródła internetowe

Logistyka działań służb ratowniczych w zdarzeniach masowych, www.logistyka.net.pl/bank-wiedzy/logistyka/item/download/79374_e8eb9b881028a4493ed98fb3a30d173e (data odczytu: 23.04.2017).

Program „Od papierowej do cyfrowej Polski" – organizacja, strumienie i status prac, mc.gov.pl/files/od_papierowej_do_cyfrowej_polski-status_prac.pdf (data odczytu: 28.08.2017).

* * *

Analysis of information security system in the context of technical and legal regulations in health services

Abstract

The paper was prepared due to the need to investigate the issue of how the information security system in healthcare is shaped. Bearing in mind that applications that make up the security system are created directly on the basis of legal acts, which in turn are affected by international technical standards, the degree of compliance of legal norms with technical standards related to information protection in health services was investigated. A given dependence was observed in the area of regulation and information features, which include information quality criteria and information protection attributes, using the methodology proposed by prof. J. Oleński, associated with the N model and the P model. The paper confirms the hypothesis of insufficiently pronounced mapping of technical standards in legal acts.

Keywords: information security system, health services