Monika Dobska Paweł Dobski

ROLA ZNORMALIZOWANYCH SYSTEMÓW

W ZARZĄDZANIU PODMIOTAMI LECZNICZYMI

Fundusze Europejskie Wiedza Edukacja Rozwój
Uniwersytet Gdański
Unia Europejska Europejski Fundusz Społeczny
Difin

ść to uporczywe dążenie do ciągłej doskonałości

e Zofii

Monika Dobska Paweł Dobski

ROLA ZNORMALIZOWANYCH SYSTEMÓW W ZARZĄDZANIU PODMIOTAMI LECZNICZYMI

Difin

ROZDZIAŁ 2

Podstawowe znormalizowane systemy w zarządzaniu podmiotami leczniczymi

2.1. Ewolucja koncepcji zarządzania jakością w usługach medycznych

Normalizacja systemów zarządzania przyczynia się do podtrzymania i poprawy jakości, dostarczając informacji menedżerom o aktualnych, zalecanych i wzorcowych kierunkach zarządzania jakością i innych pokrewnych oraz zwiększając bezpieczeństwo i wartość dla konsumentów. Omawiając podstawowe, znormalizowane systemy zarządzania, należy przybliżyć i wyjaśnić terminologię w przedmiotowym zakresie.

Jakość jest pojęciem złożonym i trudnym do jednoznacznego zdefiniowania. Kategoria ta może przyjmować różne znaczenia w zależności od kontekstu, w jakim zostanie użyta. Problemy interpretacyjne wynikają w dużej mierze z powszechności tego zjawiska. Ciągły i mimowolny kontakt człowieka z jakością doprowadził do pewnej obojętności wobec tej kategorii i traktowania jej jako elementu koniecznego, warunkującego wybór danego wyrobu lub rodzaju aktywności. Zainteresowanie zagadnieniami jakości w skali powszechnej było i nadal jest powodowane potrzebami praktyki występującymi głównie w obszarach (Dobski, 2012, s. 10):

- wytwarzania/świadczenia usług,
- wymiany handlowej,
- eksploatowania produktów/korzystania z usług.

biorstw towarzyszy rozwój kwalitologii[11] – nauki o jakości. Jako pierwszy nazwę tę zaproponował w latach siedemdziesiątych ubiegłego stulecia R. Kolman (2002, s. 255), wskazując, że jest to interdyscyplinarna dziedzina wiedzy zajmująca się wszelkimi zagadnieniami dotyczącymi jakości.

Studia literaturowe oraz analiza aktywności rynkowej przedsiębiorstw jednoznacznie wskazują, że kategorie jakościowe systematycznie poszerzają i ugruntowują swoją pozycję w systemie pojęć i działań o charakterze społecznym, gospodarczym i naukowym. Należy podkreślić, że obszar zastosowania zagadnień związanych z jakością stale ewoluuje. O ile początkowo uwaga badaczy i praktyków skoncentrowana była na procesach produkcyjnych, wyrobach przemysłowych i związanych z tym procesach kontroli technicznej, o tyle dzisiaj można zaobserwować przełom w kwalitologii. Jego konsekwencją jest rozszerzenie obiektu badań na nowe produkty, procesy i systemy z uwzględnieniem powiększającego się spektrum aspektów badawczych.

Na tym tle warto zwrócić uwagę na interdyscyplinarny charakter kwalitologii, który wynika z powiązania z:

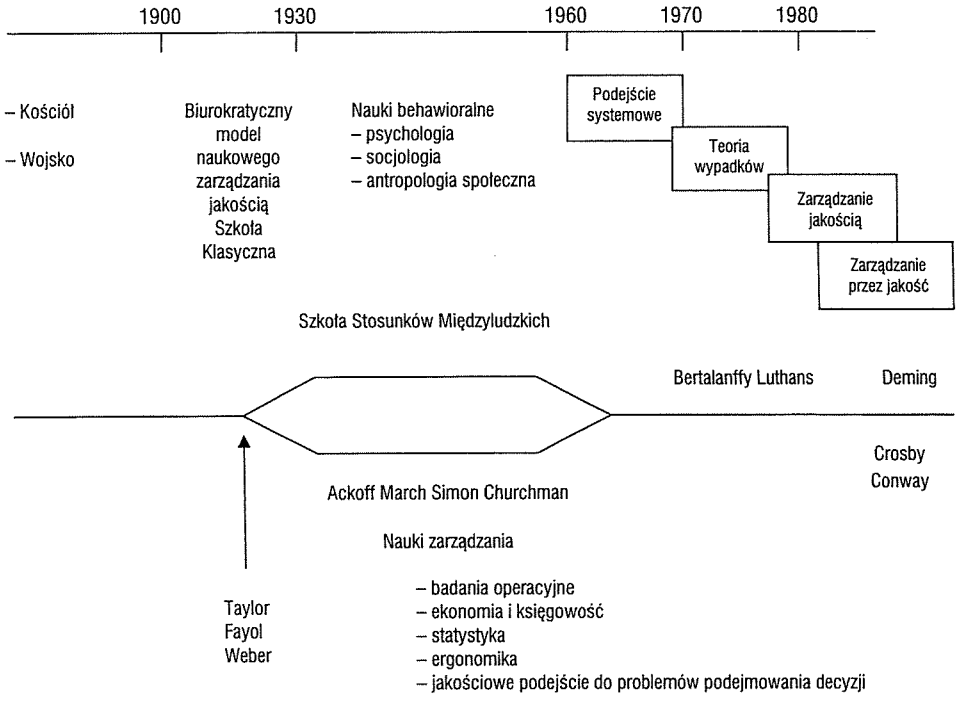
- matematyką – formuła współzależności w przemianach jakościowych;
- cybernetyką – tworzenie struktur systemów sterowania jakością;
- socjologią – badanie jakości życia;
- psychologią – badanie motywacji działań w zakresie jakości – psychologiczne kryteria jakości;
- biologią – badanie optymalnych warunków realizacji procesów życiowych;
- sozologią – analiza związków ochrony środowiska z jakością życia;
- metrologią – formułowanie metod pomiaru kryteriów jakości oraz sprzętu do kontroli jakości wyrobów;
- materiałoznawstwem – dobór właściwości surowców i materiałów;
- towaroznawstwem – badanie użyteczności produktów i usług, kontrola jakości w obrocie towarowym, organoleptyczne kryteria jakości;
- ekonomią – badanie ekonomicznych uwarunkowań optymalnej jakości oraz analizy kosztów jakości;
- teorią organizacji i zarządzania – ustalenie zasad organizacji systemów jakości i zarządzania tymi systemami;
- prawoznawstwem – prawne uwarunkowania działań projakościowych.

---

[11] Etymologicznie nazwa ta wywodzi się od łacińskiego słowa *qualitas* (jakość) i greckiego słowa *logos* (nauka).

cji sięgają początków teorii zarządzania, której podwaliny stworzyli F.W. Taylor, H. Fayol, M. Weber – twórcy klasycznej szkoły zarządzania[12]. F.W. Taylor opracował zbiór zasad znany pod nazwą naukowej organizacji pracy, której celem było ustalenie najlepszych metod wykonywania dowolnego zadania oraz szkolenia i motywowania robotników. Rozwój myślenia organizacji i zarządzaniu do lat osiemdziesiątych przedstawiono na rysunku 2.1.

Rysunek 2.1. Zarządzanie przez jakość (TQM) do lat osiemdziesiątych XX w. a rozwój myślenia o organizacji i zarządzaniu



Źródło: Pike, Barnes 1996, s. 39.

[12] W opracowanie teorii, której celem było zwiększenie wydajności pracy, oprócz F.W. Taylora swój wkład wnieśli H. L. Gautt oraz F. i L. Gilbertowie.

zarządzania jakości,ą należy wyodrębnić trzy etapy: kontrolę, sterowanie i zarządzanie. Aspektem, który przyczynił się do wyodrębnienia pierwszego etapu, było założenie o nieuchronności błędu. Wynika z tego zasadność przeprowadzenia kontroli, którą można podzielić na (Hamrol, Mantura 2006, s. 91–92):

- *kontrolę techniczną*, której obiektem jest wyrób będący rezultatem procesu technologicznego, ujmowany wyłącznie w przestrzeni cech technicznych. Ten typ ma właściwości biernej kontroli restrykcyjnej. Wyniki jej służą wyłącznie przyjęciu lub odrzuceniu wyrobu oraz ocenie pracownika;
- *kontrolę jakości*, która uwzględnia nie tylko techniczną, ale także profilaktyczną perspektywę analizy. Podejście to rozkłada odpowiedzialność za jakość na jednostki wykonawcze i zarządcze oraz wprowadza element samokontroli. Kontrola ma wówczas właściwości czynnej kontroli odbiorczo-profilaktycznej i wykorzystuje metody statystycznej kontroli jakości.

Ze względu na to, iż niniejsza publikacja odnosi się do sfery zarządzania usługami, a nie zarządzania przedsiębiorstwami produkcyjnymi, dla uporządkowania koncepcji jakościowych kluczowe z nich zostały przedstawione w tabeli 2.1.

Należy mieć na uwadze, iż problematyka jakości w sferze produkcji jest jedynie wprowadzającą, a kanwą dalszych rozważań jest teoria usług.

Problematykę jakości usług w literaturze zagranicznej podejmowali tacy autorzy, jak: Ch. Grönroos (1982), E. Gummesson (1979; 1983), A. Parasuraman, L.L. Berry i V. Zeithmal (1985), R.C. Lewis i B.M. Booms (1983), V.E. Sasser, P.R. Olsen, D.D. Wyckoff (1978). Jednak pierwsza konferencja poświęcona temu zagadnieniu odbyła się dopiero w 1988 roku w Karlstadt (Szwecja) i była zatytułowana *Quality Management*. Pokłosiem tego wydarzenia były publikacje wspomnianego już E. Gummessona, który pisząc o jakości usług, dokonał jej rozbioru na cztery jakości cząstkowe: 1. projektu (*design quality*), 2. wykonania (*production*), 3. dostaw (*delivery*), 4. relacji (*relational quality*). K. Rogoziński zmodyfikował ten podział w celu jak najlepszego dopasowania jakości do usług, stosując opis czynnościowy. Tak ujęta jakość jest bowiem dającą się odwzorować na *continuum* czasowym sekwencją działań składających się na proces doskonalenia obsługi nabywcy (Dobska 2013, s. 198).

Tabela 2.1. Kluczowe aspekty kompleksowego zarządzania jakością w świetle koncepcji Ph.B. Crosby'ego, W.E. Deminga, J.M. Jurana, A.V. Feigenbauma i K. Ishikawy

Zagadnienie	Autor				
	Ph.B. Crosby	W.E. Deming	J.M. Juran,	A.V. Feigebaum	K. Ishikawa
Definicja jakości	zgodność z oczekiwaniami	spełnienie oczekiwań rynku przy niskich kosztach	przydatność użytkowa	jakość jest efektem właściwej organizacji i zarządzania	nie definiował ale jes autorem myśli „jakoś zaczyna się i kończy wykształceniu"
Wykonanie standardu a motywacja	zero defektów	– różne skale badania jakości, – zalecane stosowanie metod statystycznych	przeciwny nakłanianiu pracowników do wykonywania pracy z bezwzględną precyzją	ciągłe motywowanie pracowników do osiągania i oceny jakościowych wyników przedsiębiorstwa	ciągłe doskonalenie stanu istniejącego przy czynnym udziale wszystkich zatrudnionych osób
Struktura koncepcji	14 kroków ulepszania jakości	14 punktów dla kierownictwa	10 kroków ulepszania jakości	*Total Quality Control* – TQC	zastosowanie w praktyce siedmiu tradycyjnych narzęd jakości
Statystyczny proces kontroli	odrzucenie statystycznej akceptacji poziomu jakości	proponuje statystyczne metody kontroli jakości	zaleca umiarkowane stosowanie statystycznych metod kontroli jakości. Statystyczny proces kontroli nie może być głównym narzędziem TQM	zwolennik kontroli inspekcyjnej	rozwinął propozycje Deminga i Shewharta w zakresie statystyczn kontroli jakości – koncepcja CWQC

Zagadnienie	Autor				
	Ph.B. Crosby	W.E. Deming	J.M. Juran,	A.V. Feigebaum	K. Ishikawa
Stopień odpowiedzialności kierownictwa wyższych szczebli	kierownictwo ponosi odpowiedzialność za jakość	odpowiedzialność za 94% problemów związanych z jakością	odpowiedzialność za ponad 80% problemów związanych z jakością	rozłożenie odpowiedzialności na pracowników wszystkich działów	odpowiedzialność najwyższego kierownictwa za jakc
Podstawy usprawniania	– proces, nie program; – określenie celu usprawnień	– ciągła redukcja odchyleń; – cele bez metody realizacji należy eliminować	projekt po projekcie; podejście zespołowe do problemu; ustalanie celów	przełożenie. przyjętej strategii jakości na .specyfikacje techniczne i .marketingowe, odpowiadające potrzebom nabywców	podejście zespołowe problemu
Praca zespołowa	zespoły usprawniania jakości	– udział pracowników w podejmowaniu decyzji; – przełamywanie barier między działami organizacji	propagowanie kół jakości oraz pracy zespołowej	zwolennik stałego zaangażowania wszystkich pracowników w działaniach na rzecz jakości	twórca kół jakości
Koszty jakości	koszt niezgodności; jakość nic nie kosztuje	brak poziomu optymalnego, ciągłe usprawnianie	jakość nie jest za darmo, można określić poziom optymalny	koszty jakości stanowią miarę działalności w ramach kontroli jakości	bezpośrednio nie wypowiadał się. Eksponując aspekt kontroli przyczynił s do rozwoju sterowan procesami

Zagadnienie	Autor			
	Ph.B. Crosby	W.E. Deming	J.M. Juran,	A.V. Feigebaum	K. Ishikawa
Zaopatrzenie i dostawy towarów	– określone zapotrzebowanie; – większość problemów związana jest z nabywcą	wymaganie prowadzenia ewidencji statystycznych oraz wykresów kontrolnych	– problemy o charakterze kompleksowym, – wprowadzenie formalnych badań dostaw	jakość należy kontrolować u samego źródła wszystkich procesów, a więc także u dostawców	odpowiedzialność za jakość spoczywa na wszystkich działach także na zaopatrzeni
Ocenianie dostawców	– ważne ocenianie dostawców; – wskazane ocenianie nie nabywców; – audyty jakościowe bezużyteczne	krytyczne podejście do oceny dostawców	należy oceniać dostawców a także aktywnie pomagać im w doskonaleniu oferty	zadaniem menedżerów jest wspieranie prac na rzecz jakości a nie tylko stanie na jej straży	należy usuwać przyczyny, a nie symptomy niskiej jakości
Jedno źródło dostaw	brak zdania	zdecydowanie tak.	nie koniecznie. Może skutkować zlekceważeniem przez dostawcę wyzwań stawianych przez konkurencję	brak zdania	brak zdania

Źródło: Dobski 2012, s. 38–39.

1. Jakość w percepcji usługobiorcy (QP) – jest jakością odczytaną, doświadczoną i percypowaną przez nabywcę. Budowana przez kumulowanie doświadczeń i momentów pracy, a jej kulminacją jest kryterium prawdy wieńczące cały cykl obsługi nabywcy. Można ją zmierzyć i opisać wykorzystując model SERVQUAL, zawierający uniwersalny zestaw kryteriów ocen jakościowych (Rogoziński 2000, s. 14–23).
2. Jakość w faktach i normach (QF) – tym mianem można określić to wszystko, co składa się na jakość usług dającą się precyzyjnie określić, zmierzyć, czasami zestandaryzować. Można ją traktować jako jakość skwantyfikowaną (Rogoziński 2000, s. 14–23).
3. Jakość w relacjach (QR) – wypracowuje obszar kompromisu i wzajemnego akceptowania odmiennych punktów widzenia na jakość: QF (ciążącej ku standaryzacji) a QP (kojarzonej z jakością pojmowaną subiektywnie). Ponadto przez wbudowanie jakości usług w relacyjny kontekst możliwa staje się transpozycja jakości w desygnat wartości. Wyeksponowany zostaje także wymiar czasowy uwzględniający nie tylko wynik końcowy, ale również biorący pod uwagę to, co dzieje się i wydarza w trakcie wykonania usługi (Rogoziński 2000, s. 14–23). Dzięki marketingowi relacji staje się możliwe doskonalenie obsługi nabywcy. Należy przy tym uwzględnić takie przesłanki, jak: zróżnicowane poziomy zaangażowania uczestników usługowej relacji, perspektywę współpracy, wybór i desygnowanie odpowiedniego usługodawcy do stałej bądź wyłącznej obsługi określonego klienta, programy jakościowej prewencji i procedury reklamacyjne uwzględniające preferencyjne traktowanie lojalnych/stałych klientów. Elementy te stają się danymi, które w badaniach jakościowych można uchwycić i rozpisać na QF (jakość w faktach) (Rogoziński 2000, s. 14–23).
4. Jakość synkretyczną (QS) – będącą obszarem kompromisu czy „wypadkową" rozbieżności, ale rezultat wspólnej projekcji i realizacji tego, co dzięki relacjom ukazuje się jako wartościowe, cenne, obiektywnie dobre. Jakość synkretyczna posługuje się kryteriami zweryfikowanymi pośrednio poprzez budowanie relacji i wypracowuje kompromisowe atrybuty jakości. Te ostatnie K. Rogoziński nazwał *kwaliami*, wykorzystując je do opisu i oznaczenia jakości usług „ponad podziałami".

zróżnicowanego zestawu miar bądź kryteriów. I tak na przykład (Kogoziński 2000, s. 14–23):

- QF1 – czas realizacji usługi; QF2 – normatywne wyposażenie techniczne, QF3 – poziom kwalifikacji usługodawcy;
- QP – odzwierciedla rozpoznane i preferowane przez nabywcę kryteria ocen. QP1 – przewrażliwiony na punkcie czystości, QP2 – podejrzliwy i nieufny, QP3 – wegetarianin;
- QR – jako punkt wyjścia można posłużyć się kryptonimem z „drabiny lojalności nabywcy". QR1 – potencjalny klient, QR2 – nowy nabywca, QR3 – „stary klient", QR4 – adwokat;
- QS – obszar kwaliów, który deskryptywnie można ująć w postaci formuły:

$$qa \rightarrow x: \text{F2/ P3/ R4},$$

oznaczać to będzie, że:
kwalium charakteryzujące usługę *a* wykonywaną dla nabywcy *x*, powstałą w wyniku przyjęcia kompromisowego rozwiązania polegającego na wykonywaniu usługi wprawdzie poza godzinami otwarcia firmy, ale w czasie najdogodniejszym dla nabywcy, przez budzącego największe zaufanie wykonawcę, ponieważ klient ma szansę awansować do grupy klientów „adwokatów".

Zastosowanie teorii usług, wypracowanej przez szkołę szwedzką i ugruntowanej przez szkołę poznańską reprezentowaną przez badaczy skupionych wokół K. Rogozińskiego, zaowocowało pracami przybliżającymi tematykę jakości w usługach medycznych. Warte lektury w tym zakresie są publikacje M. Wiśniewskiej (2009, 2021) czy K. Rogozińskiego (2000). Autorzy przedstawiają nie tylko podejście definicyjne, lecz także rozpatrują ujęcia jakości w odniesieniu do stopnia implementacji. Poniżej zostały omówione pojęcia jakości, przedstawione w monografii M. Dobskiej (2013) (por. tabela 2.2).

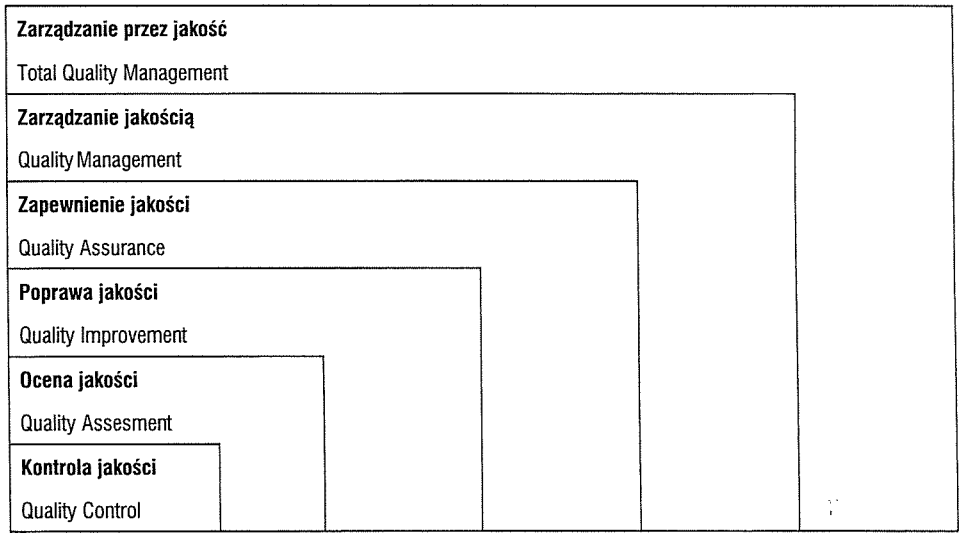
Wraz z wyodrębnieniem definicji jakości w literaturze zaczęły się pojawiać określenia: kontrola jakości, ocena jakości, poprawa jakości, zapewnienie jakości odnoszące się do usług medycznych. Dla uporządkowania i scharakteryzowania tych pojęć w pracy posłużono się schematem H. Lenartowicz (por. rysunek 2.2).

Lp.	Autor/organizacja	Definicja
1.	A. Donabedian	Jakość opieki zdrowotnej to taki rodzaj opieki, w której maksymalizuje się mierzalne dobro pacjenta, biorąc pod uwagę równowagę oczekiwanych korzyści i strat towarzyszących procesowi opieki na wszystkich jej etapach. Przez pojęcie „jakość" rozumieć można społeczny konstrukt reprezentujący koncepcje i wartości zdrowia, oczekiwania co do relacji pomiędzy świadczącymi opiekę a odbiorcami oraz punkt widzenia pacjenta na funkcje i role systemu ochrony zdrowia (Donabedian 1988, s. 173–192, za: Lenartowicz 1998, s. 10). Wymiary jakości: (1) techniczny – w którym odpowiadamy na pytanie, czym dysponujemy, (2) nietechniczny – w którym odpowiadamy na pytanie: jak postępujemy z usługobiorcą, (3) środowiskowy – w którym odpowiadamy na pytanie, gdzie przebiega proces usługi. Wszystkie te wymiary są komplementarne (Detyna, Detyna 2011, s. 95).
2.	E.J. Gancher, R.J. Coffey	Jakość to spełnienie określonych wymagań klienta (Gancher, Coffey 1993, za: Lenartowicz 1998, s. 10; Kautsch, Frączek 2000, s. 29).
3.	JCAHO	Jakość to stopień, w jakim każda usługa świadczona pacjentowi dostarczana jest zgodnie z aktualnym stanem wiedzy, podnosi prawdopodobieństwo uzyskania pożądanego wyniku opieki i redukuje prawdopodobieństwo niepożądanych rezultatów (Lewthers 1997, s. 87; Zając 1999, s. 168; Włodarczyk 1996, s. 307; Marciniak, 1999, s. 5).
4.	Narodowa Szwedzka Rada Zdrowia i Opieki Społecznej (SIS)	Na jakość składają się wszystkie te cechy produktu usługowego, które zebrane razem sprawiają, że produkt może zaspokoić wypowiedziane i nieświadome potrzeby nabywcy (Rosen, 1994, s. 40–42).
5.	K. Opolski, E. Szemborska	Jakość można zdefiniować jako ogół cech i właściwości produktu bądź usługi, które to cechy decydują o zdolności tegoż wyrobu lub usługi do zaspokojenia stwierdzonych lub przewidywanych potrzeb odbiorcy (Opolski, Szemborska 1997, s. 22).
6.	J. Ovretveit	Jakość w opiece zdrowotnej polega na pełnym zaspokajaniu zapotrzebowania na usługi lecznicze, przy możliwie najniższych kosztach własnych świadczeniodawców, w ramach obowiązujących regulacji i limitów ustanowionych przez władze administracyjne i instytucje „kupujące" (Murkowski, Nowacki i Koronkiewicz 1996, s.12–13).

7.	IOM (Institute of Medicine, USA)	Jakość to stopień, w jakim usługi zdrowotne kierowane do pacjentów zwiększą prawdopodobieństwo pożądanych skutków zdrowotnych i są zgodne z bieżącym stanem wiedzy zawodowej (Legido-Quigley i in. 2008, s. 2).
8.	Departament Zdrowia (Wielka Brytania)	Jakość usług medycznych oznacza: profesjonalizm w działaniu, dbałość o wysokie kwalifikacje personelu, wykonanie czynności we właściwym czasie oraz świadczenie usługi prawidłowo za pierwszym razem (Legido-Quigley i in. 2008, s. 2).
9.	R.S. Maxwell	Jakość usług zdrowotnych zależna jest od spełnienia oczekiwań w następujących wymiarach jakości: *dostępności* mierzonej skalą możliwości uzasadnionego korzystania z opieki niezależnie od ograniczeń, jakie mogą się wiązać z położeniem geograficznym, odległością, pieniędzmi, czasem, wiekiem, językiem, transportem, architekturą budynków itp.; *równości* – świadczenie opieki dla całej populacji zgodnie z rozpoznanymi potrzebami, niezależnie od kulturowego, społecznego charakteru czy innych cech osobowych pacjentów; *adekwatności* – rodzaje świadczeń zdrowotnych, pakiet usług, procedury dostosowane do rzeczywistych potrzeb zdrowotnych społeczności, które są potrzebne, oczekiwane i wymagane przez jednostkę; *akceptacji* – opieka zdrowotna uwzględnia kulturowe i religijne wartości odbiorców; *efektywności* – dostępne zasoby, np. finanse, budynki, wyposażenie, najwyższy efekt przy najniższych kosztach; *skuteczności* – opieka spełnia swoją funkcję w kategoriach korzyści i efektów zdrowotnych jednostki oraz populacji, której służy (Ksykiewicz, Rusecki 1996, s. 148; Murkowski, Nowacki i Koronkiewicz 1996, s. 12; Lenartowicz 1998, s. 38; Whitfield 1999, s. 141; Sprawozdanie Pełnomocnika Rządu, s. 9).
10.	Światowa Organizacja Zdrowia (WHO)	Jakość opieki zdrowotnej to poziom realizacji wewnętrznych systemów ochrony zdrowia, w celu poprawy zdrowia oraz wrażliwości na uzasadnione oczekiwania społeczeństwa (Legido-Quigley i in. 2008, s. 2). Jakość to także rezultat (jakość techniczna), sposób użycia środków (wydajność ekonomiczna), organizacja usług oraz satysfakcja pacjenta (WHO 1988, s. 79)*.

* W biurze krajowym WHO w Danii jakość krajowych systemów opieki zdrowotnej jest sumą pięciu czynników: systemów, technologii i narzędzi, ludzi, kierunków działania.

Źródło: Dobska 2013, s. 182.



Źródło: Lenartowicz 1998, s. 14.

Omawianie poszczególnych pojęć rozpoczęto od poziomu najniższego. I tak, *kontrola jakości (Quality Control* – QC) jest zespołem czynności mających na celu przetestowanie wszystkich elementów pracy i działań, które mogą być zdefiniowane, pomierzone i sprawdzone (skontrolowane). Kontrolę jakości można więc rozpatrywać pod kątem standardów i norm. Są zwykle formułowane przez osoby kontrolujące i nadzorujące, bez udziału wykonawców, co ma niekorzystny na nich wpływ, albowiem obniża ich zainteresowanie i poczucie odpowiedzialności za jakość. Powinna służyć sprawdzeniu zgodności stosowanych wartości poszczególnych parametrów z ich wartościami optymalnymi[13].

[13] Celem kontroli jakości w pracowni radiologicznej jest na przykład: a) wykrywanie uszkodzeń po instalacji lub głównej naprawie, uszkodzeń, które mogłyby mieć wpływ na jakość obrazu lub narażenie pacjentów na promieniowanie, b) ustalenie wyjściowego poziomu sprawności przydatnego do porównań, c) wykrywanie przyczyn pogorszenia sprawności aparatu rentgenowskiego, d) ustalenie porównywalnych parametrów ekspozycji dla różnych aparatów rentgenowskich. Dzienna kontrola jakości (*daily QC*) jest obowiązkiem techników obsługujących pacjentów. Testy półroczne i roczne prowadzone są przez wykwalifikowanych techników kontroli jakości. Kontrola jakości w przypadku diagnostyki rentgenologicznej oznacza maksymalizowanie prawdopodobieństwa, że obrazy rentgenograficzne będą zawierać adekwatną informację diagnostyczną przy jednoczesnym użyciu potencjalnie minimalnej dawki promieniowania i koszcie badania pacjenta (Wójtowicz 1983, s. 16; Lenartowicz 1998, s. 13–14; Whitfield 1999, s. 141; Chmielewski 2000, s. 54–55).

poziomu jakości. Zwykle obejmuje badanie stopnia satysfakcji pacjenta z przebiegu leczenia, głównie z opieki i pobytu w szpitalu. Może także obejmować satysfakcję pracowników z wykonywanej pracy. Ponadto ocena jakości może funkcjonować jako samodzielna analiza bądź też stanowić etap szerszych programów poprawy jakości. Do obecnie istniejących systemów oceny jakości dodaje się także ocenę podmiotu leczniczego prowadzoną przez różne strony, np. NFZ, który dokonuje oceny w trakcie rangowania ofert.

Poprawa jakości (Quality Improvement) odnosi się do podniesienia jakości określonego komponentu opieki. Jest programem szerszym od oceny, gdyż zwykle obejmuje, oprócz ustalenia stanu faktycznego, identyfikacji czynników sprzyjających i utrudniających, także warianty poprawy oraz udoskonalenie badanego wycinka rzeczywistości. Poprawa jakości może dotyczyć np. skrócenia czasu oczekiwania pacjentów w izbie przyjęć, w konsultacyjnym gabinecie specjalisty itp.[14]

Zapewnienie jakości (Quality Assurance – QA) jest podejściem znacznie pogłębionym i rozszerzonym. QA to zaplanowany system działań rzetelnie wykonywanych, zapewniający, że usługi są zgodne z przyjętymi standardami. Oznacza pozytywną deklarację, intencję oraz gotowość do usunięcia wszelkich stwierdzonych niedociągnięć. Stanowi formalną gwarancję (poręczenie) uzyskania usługi na możliwym do przyjęcia, akceptowalnym poziomie. Obejmuje ocenę i pomiar aktualnego poziomu wytwarzania bądź testowania usług oraz skuteczne działania modyfikujące te procesy. Pojęcie zapewnienia jakości jest nadrzędne wobec technologii medycznych, od której oczekuje się sprawdzenia skuteczności i bezpieczeństwa wykorzystywanych metod, ustalenia norm, stosowania technologii i osiągnięcia zamierzonych wyników, a także określenia stosunku między nakładami finansowymi a rezultatami. Model zapewnienia jakości jest preferowany w wielu organizacjach opieki zdrowotnej, w których dąży się do zapobiegania ewentualnym problemom wcześniej, zanim wystąpią (Marciniak 1999, s.78; Lenartowicz 1998, s. 15 i 35–39; Niżankowski 2000, s. 417; Cleland 1995, s. 27).

[14] Warto zauważyć, że pracownik zaangażowany w proces poprawy jakości obsługi klienta to taki, który: zna i rozumie sytuację firmy, zna zakres swoich uprawnień, obowiązków i odpowiedzialności, co wzmacnia jego samodzielność, jest doceniany, nagradzany lub jasno i rzetelnie karany, jest traktowany przez pracodawcę w sposób podmiotowy (Lenartowicz 1998, s. 16; Marciniak 1999, s. 9; Cleland 1995, s. 26; Siewierski 1997, s. 20).

rencji Światowej Organizacji Zdrowia w Lublanie. Organizacja ta stawia bowiem krajom europejskim żądanie jasnej strategii w zakresie ciągłego doskonalenia jakości opieki uwzględniającej kontrolę kosztów[15].

Należy podkreślić, iż sfera jakości mocno została rozbudowana na rynku amerykańskim, gdzie ewolucja pojęć związana jest z rozwojem koncepcji w praktyce. I tak, *Quality Assurance* jest przez niektórych autorów uważane za sformułowanie przestarzałe i jest zastępowane przez pojęcie *Continuous Quality Improvement* (stała poprawa jakości) (Kubik 1999, s. 344–345; Rogoziński 1998, s. 94–95)[16]. Podobnie jak pojęcie *Risk Management* (RM)[17], definiowane zarówno jako czynność, jak i nazwa sekcji szpitalnej zajmującej się kontrolą jakości usług leczniczych[18]. Ważnym terminem jest *Quality Assurance* – zwykle

[15] Zgodnie z kartą podstawowe zasady programów jakości to: identyfikacja najlepszych wyników, jasne i precyzyjne określanie celów, profesjonalna samoocena i samoregulacja, włączenie pacjentów do procesu doskonalenia jakości opieki zdrowotnej. W celu zapewnienia jakości można przyjąć następujący program działań: określanie zapotrzebowania na usługi medyczne w miejscu działania, planowanie zatrudnienia zgodnie z potrzebami zdrowotnymi, wyposażenie pracowników w sprzęt niezbędny do wykonania usług na wysokim poziomie, zatrudnienie osób o odpowiednich kwalifikacjach zawodowych, stosowanie okresu próbnego zakończonego oceną pracownika, opracowanie kryteriów oceny .pracowników, wprowadzanie systemu premiowania najlepszych pracowników, motywowanie do podnoszenia kwalifikacji, badanie poziomu satysfakcji klientów (Hischfeld 1997, s. 1–3, za: Lenartowicz 1998, s. 38; Nadziejko, Ścibor 1999, s. 98).

[16] W marketingu relacyjnym K. Rogoziński wprowadził pojęcie doskonalenia obsługi nabywcy.

[17] *Risk management* (w wolnym tłumaczeniu – działalność zmniejszająca ryzyko) jest zarówno nazwą oddziału (sekcji), który znajduje się w każdym szpitalu w Stanach Zjednoczonych, jak i nazwą działalności profesjonalnej pracowników szpitala. Działalność ta ma na celu z jednej strony ostrzeganie przed ryzykownymi czynnościami leczniczymi, z drugiej identyfikowanie zdarzeń, które mogą stanowić niebezpieczeństwo wszczęcia procesu przeciwko szpitalowi. Podstawową funkcją *Risk Management Departament* jest koordynowanie czynności zapobiegających oskarżeniom szpitala ze strony pacjentów o zaniedbania w działalności leczniczej i korygowanie zaistniałych niedociągnięć. Inną funkcją jest rozpatrywanie wydarzeń lub wypadków (*incident reports*), które mogą być potencjalnymi przyczynami roszczeń pacjentów o odszkodowanie. Analizowanie takich zagrożeń prowadzi do identyfikacji zagrożeń i niedbalstwa ze strony personelu, do ewentualnego korygowania niebezpiecznych praktyk, a tym samym zapobiegania powtórzenia się podobnych zdarzeń w przyszłości (Kubik 1999, s. 344).

[18] *Quality Assurance Department* to dział złożony z etatowych pracowników szpitala, profesjonalistów medycznych, których zadaniem jest sprawdzenie działalności leczniczej lekarzy (a także innych profesjonalistów) pod kątem ewentualnych „odchyleń" tej działalności od ogólnie przyjętych standardów opieki zdrowotnej. Odbywa się to przez selekcję tych kart chorobowych, w których pacjenci demonstrowali niespodziewane, negatywne wyniki leczenia (np. zgon, infekcje, nagłe

i wykrycie niedociągnięć ze strony zewnętrznych czynników kontrolujących (np. PRO – Professional Review Organization)[19] niesie daleko idące konsekwencje, a wewnętrzna weryfikacja daje możliwości wprowadzenia szybkich zmian[20]. Risk Management i Quality Assurance wykrywają nie tylko niedociągnięcia, korygują je i przeciwdziałają oskarżeniom o niedbalstwo lecznicze, a także poprawiają reputację instytucji opieki zdrowotnej. Są jednak i różnice. Głównym zadaniem Risk Management jest ochrona interesów szpitala, podczas gdy, podstawowym zadaniem Quality Assurance jest ochrona pacjen-

zaostrzenia stanu chorobowego), a następnie retrospektywne analizowanie postępowanie leczniczego. Odchylenia od normy są aktualizowane i ustala się pewien wzór (*pattern*) charakterystyczny dla danego lekarza. Odchylenia od przyjętego standardu, powtarzające się częściej niż zwykle u pewnych lekarzy, nasuwają podejrzenie o niekompetencję.

[19] *Peer review* jako forma kontroli usług lekarskich wyprowadzona została po raz pierwszy w 1972 r. w charakterze Professional Standards Review Organizations (PSRO). PSRO miały na celu przez swoją akcję kontrolną propagować skuteczną i ekonomicznie wydajną, właściwą jakość opieki zdrowotnej. Działalność PSRO oceniona została jako niewystarczająca, gdyż nie potrafiła ukierunkować swoich celów. PSRO zostały w 1984 r. zastąpione przez Professional Review Organizations (PRO), które miały osiągnąć cele, zarówno odnośnie do jakości opieki zdrowotnej, jak i do stopnia używalności usług medycznych. PRO są prywatnymi organizacjami profesjonalnymi typu non profit skupiającymi lekarzy i pielęgniarki, a także personel administracyjny, zatrudniony na zasadzie kontraktu w celu przeglądu (*review*) opieki prowadzonej przez lekarzy w szpitalach. Lekarze podlegający przeglądowi wybierani są losowo, chyba że istnieje podejrzenie w konkretnym przypadku, że lekarz prowadzi usługi poniżej ustalonych przez wiedzę i praktykę norm. Stąd też PRO spełnia funkcję „policjantów" lekarzy w ocenie prowadzonej przez nich praktyki. PRO jest w Stanach Zjednoczonych organizacją dokonującą oceny jakości prawie wyłącznie u lekarzy medycyny i w przypadku osteopatii.

[20] *Quality Assurance* (QA) w każdym kraju jest wypadkową formy organizacyjnej medycyny, regulacji prawnych, ustaleń politycznych i kultury społecznej. Zwykle opiera się na kilku filarach: a) prawnych koncepcjach odpowiedzialności szpitala za wynik podjętego leczenia, czyli na fakcie, że szpital z jednej strony bierze na siebie odpowiedzialność za działania związane z leczeniem, z drugiej strony ma prawo do wnikania w przebieg działalności zawodowej zatrudnionych osób, b) inicjatywach organizacyjnych osób odpowiedzialnych za leczenie (PRO), c) inicjatywach opartych przede wszystkim na naukowych podstawach pojmowania jakości w usługach medycznych. Pomimo dużego wysiłku w połowie lat dziewięćdziesiątych w większości krajów europejskich rozwój systemów zapewnienia jakości znajdował się zaledwie na wczesnym etapie. Jedynie w Wielkiej Brytanii i Holandii można uznać ten poziom za dość zaawansowany. Przyjęte tam zostały założenia polityczne, przygotowano regulacje prawne, powstały instytucje i organizacje zajmujące się popularyzacją i implementacją systemów QA. W krajach skandynawskich i Islandii również następował szybki rozwój, głównie dzięki dużemu wsparciu rządów oraz zaangażowaniu organizacji profesjonalnych lekarzy rodzinnych (Tomasik 1998, s. 182).

a w przypadku Quality Assurance następuje porównanie prowadzonej opieki do obowiązujących standardów.

Kontrola jakości stała się na tyle istotnym zagadnieniem, że w części krajów doczekała się osobnych regulacji. I tak, w Niemczech zalecenia ustawodawcy zostały skonkretyzowane we Wspólnej Komisji Federalnej (G-BA) i muszą być realizowane w poszczególnych szpitalach. Zgodnie z obowiązującym ustawodawstwem, wszystkie zakłady powinny co dwa lata publikować w Internecie ustrukturyzowane sprawozdanie dotyczące jakości. Dzięki takiemu rozwiązaniu Niemcy są liderem w dziedzinie sprawozdawczości dotyczącej jakości. W przypadku niespełnienia lub nieznacznego przekroczenia wytyczonych wskaźników, szpital jest wzywany do poprawy.

Weryfikacja i kontrola jakości dotyczy także działań prowadzonych przez poszczególne grupy zawodowe. Niemiecki Instytut Stosowanych Badań nad Pielęgniarstwem (DIP) poprosił grupę zawodową pielęgniarek o wskazanie wskaźników jakości, a następnie na podstawie tych wskaźników opracowano ankietę dla szpitali, pytając o częstość występowania działań niepożądanych.

Podobnie jak w Niemczech, w Austrii, w wyniku reformy z 2005 roku, uchwalono obszerną ustawę federalną w sprawie jakości świadczeń zdrowotnych, która wymaga regularnej sprawozdawczości dotyczącej jakości. Dzięki takim uregulowaniom ma zostać zapewniona przejrzystość w sferze jakości.

Analogicznie w Republice Czeskiej, Ministerstwo Przemysłu i Handlu w roku 2000 na podstawie uchwały gabinetu nr 458/2000 w sprawie narodowej strategii promowania jakości, utworzyło tzw. Czeską Radę ds. Jakości. Składa się z przedstawicieli ministerstw, organizacji i związków zawodowych oraz organizacji pozarządowych (NGO). W wyniku tej inicjatywy w Ministerstwie Zdrowia utworzono Radę ds. Jakości w Służbie Zdrowia, aby integrować i koordynować istniejące programy w zakresie jakości i włączyć je do systemu promowania jakości (zgodnie z koncepcją Ministerstwa Zdrowia i koncepcją ramową Europejskiego Regionu WHO Zdrowie 21) (Papouschek, Bőhlke 2008, s. 55).

Ostatnim, najbardziej kompleksowym stopniem wdrażania jakości do szpitali jest *Total Quality Management* (TQM) – *zarządzanie przez jakość*. W polskiej literaturze nie ma jednoznacznego przekładu terminu TQM. Najczęściej tłumaczy się go jako: totalne zarządzanie jakością (Wawak 1995, s. 25), globalne zarządzanie jakością, kompleksowe zarządzanie jakością (Sloan 1993) czy też zarządzanie przez jakość (Wawak 1997, s. 205–206; 1999, s. 205–206; Kindlarski 1993). Niektórzy autorzy stosują także tłumaczenie zarządzanie projakościowe (Szomański 1995, s. 75) czy też, jeszcze częściej, zarządzanie jakością. A przecież,

jest tłumaczeń nazwy, tak wiele jest definicji.

TQM postrzegane jest jako: filozofia zarządzania[22], strategia zarządzania[23], metoda zarządzania (PN EN 28402 1993; Oakland 1992, s. 13) i proces stałego doskonalenia (Total Quality 1988, s. 1; Lewandowski 1998, s. 10). Należy zaznaczyć, że powyższy podział nie wyczerpuje wszystkich możliwych klasyfikacji[24]. Zaprezentowane określenia i charakterystyki TQM różnią się bowiem stopniem szczegółowości. Niezwykle istotne na tym tle jest ujęcie statyczne zarządzania przez jakość wprowadzające TQM do usług. Model takiego wprowadzenia przedstawił K. Rogoziński (1998, s. 242–245). Skoncentrował go wokół trzech M. Pierwsze to *Management*, który oznacza sformułowanie misji, celów strategicznych i wyprowadzonej z niej wizji prowadzenia biznesu, ukształtowanie odpowiedniej kultury organizacji, wybór struktury, zdefiniowanie jakości wewnętrznej, przygotowanie materialjakości, wypracowanie adekwatnego do nich stylu zarządzania. Z kolei drugie M to *Mistrzostwo zawodowe* – oznacza opracowanie, właściwy wybór i perfekcyjne stosowanie procedur realizacyjnych i powiązanych z nimi systemów motywacyjnych. Trzecie M to *Marketing relacyjny* utożsamiany z orientacją zewnętrzną, jako otwarcie się na otoczenie, w tym szczególnie na nabywców, którzy jako współprojektanci jakości i współwytwórcy usługi są włączani w strukturę. Powyższy model uzyskuje dynamizm dzięki przenikaniu się dwóch ruchów (sił), z których jeden ma charakter zstępujący, drugi zaś wstępujący. *Ruch zstępujący, czyli rozwinięcie*, polega na dyfuzji wyprowadzonych z misji celów i wykorzystaniu do tego marketingowej interpretacji jakości. Orientacja na jakość przesądza o sposobie spełnienia funkcji wykonawczych i marketingowych oraz ukierunkowuje na powiększanie wartości wspólnie dodanej. Cały proces zostaje przejrzany i przeanalizowany jako potencjalnie jakościotwórczy. Oznacza to, że z każdej najmniejszej cząstki struktury, elementu bądź jednostkowych zachowań można wyprowadzić lub zrekonstruować jakość, za jej pośrednictwem zaś odtworzyć kulturę organizacji. Kolejna kategoria to *ruch wstępujący, czyli zwijanie*. Zwijanie jest najpierw odpowiedzią udzieloną przez każdy świadomy element struktury, daną i potwierdzoną w zachowaniu – działaniu – pracy – postawie – zaangażowaniu, a następnie powrotem do źródła (kultury organizacji), by w nim potwierdzić trafność powyższych zachowań. Jest więc ruchem oddolnym, który siłę motoryczną czerpie z satysfakcji, wspina się na coraz wyższy poziom realizacji. Dzięki niemu jakość, rozumiana jako doskonalenie obsługi nabywcy, staje się formą samodoskonalenia usługodawcy (współtworzącego całość, którą jest ucząca się organizacja). Ostatnim elementem, który się pojawia, jest *przecinanie się i krzyżowanie*. Każdy element organizacji powinien dać wyobrażenie o całości, czyli na podstawie dwustronnej relacji usługowej można wnioskować o rozumieniu jakości i znaczeniu, jakie się jej nadaje. Zatem niemal każda osoba należąca do personelu kontaktowego ma wszczepiony jakościowy hologram, na podstawie którego można określić znaczenie jakości oraz zrekonstruować newralgiczne dla realizacji strategii miejsca krzyżowania się funkcji marketingowych – zarządczych – realizacyjnych i wykorzystać umiejscowiony w nich personel do budowania zespołów jakości (Rogoziński 1998, s. 244–245).

Biorąc pod uwagę powyższe założenia, można przyjąć, że kompleksowe zarządzanie przez jakość w usługach „to sposób zarządzania charakteryzujący się podejściem systemowym zorientowanym na cele strategiczne oraz zdolnością do ciągłej poprawy. Jest to możliwe poprzez aktywne działanie kierownictwa oraz mobilizację personelu. mającą na celu włączenie nabywcy w proces doskonalenia obsługi" (Dobska 2013, s. 122).

---

[21] Przyjęty w polskiej literaturze termin „zarządzanie przez jakość" często błędnie utożsamiany jest z terminem „zarządzanie jakością". Dążenie do jakości totalnej (*total quality*) wymaga określonego systemu zarządzania procesami uzyskiwania jakości oraz sposobu jej doskonalenia. Takie zarządzanie, nazywane *quality management* (QM), kładzie nacisk na rozwiązania systemowe zapewnienia jakości, stosowanie narzędzi sterowania jakością, planowanie jakości, na właściwe określenie polityki jakości oraz wyznaczanie wymiernych i konkretnych celów jakościowych (Wawak 1999, s. 205). Z opinią tą zgadzają się także E. Kindlarski i J. Bagiński (1994, s. 2–3), pisząc, że zarządzanie jakością należy zdefiniować jako aspekt całości funkcji zarządzania, które ustalają politykę jakości, cele i odpowiedzialność, jak również środki urzeczywistniające te zadania w ramach systemu jakości, także jako planowane sterowanie jakością, zapewnienie jakości i doskonalenie jakości. Zagadnienia te zostały poruszone w pracy M. Rechy (1997, s. 12). R. Karaszewski (1999c, s. 12) z kolei uważa, że zarządzanie przez jakość szeroko wykraczało poza horyzont działań wchodzących w zakres zarządzania jakością. Jest ono sposobem zarządzania, a raczej filozofią zarządzania zakładającą podporządkowanie idei kompleksowej totalnej jakości wszystkich podstawowych płaszczyzn funkcjonowania organizacji i w ten sposób udoskonalaniu jej efektywności, elastyczności i konkurencyjności.

[22] TQM jako filozofia zarządzania (Wasilewski 1998a, s. 20; 1998b, s. 32; Zymonik 1999, s. 316). Podobnie definicję TQM przedstawia R. Karaszewski (1999a, s. 12), dodając do niej dążenie do tzw. demokratyzacji zarządzania poprzez ograniczanie liczby poziomów w strukturach organizacyjnych.

[23] Definicję taką podaje także British Quality Association. TQM to zespołowa filozofia zarządzania przedsiębiorstw, zgodnie z którą potrzeby klienta oraz cele przedsiębiorstwa są nierozłączne (British Quality Association Newsletter 1989, s. 20).

[24] Z. Kłos (1994; 1999, s. 8–10) podaje dodatkowe definicje TQM, mianowicie: a) jako sposób zarządzania, system wszechstronnego oddziaływania na jakość wyrobu lub usługi; b) jako specyficzne ujęcie kultury organizacyjnej przedsiębiorstwa; c) jako opartą na szerokim udziale pracowników koncepcję społeczno-gospodarczą; d) TQM to tworzenie systemów społeczno-technicznych i sterowanie nimi (zob. także: Broniewska 1996; Oakland 1992, s. 35; Łuczak 1998, s. 15).

Podejście systemowe do organizacji oznacza zwrócenie uwagi na aspekty wymiany pomiędzy samą instytucją a jej otoczeniem. Sprzężenie zwrotne między tymi dwoma sferami jest warunkiem koniecznym do działania. I tak, podmiot może realizować swoje zadania w postaci świadczenia usługi czy też produkcji dóbr, pobierając zasoby z otoczenia, a organizacja oddaje efekt swojej działalności na zewnątrz. Taka forma wymiany jest możliwa przy systemie otwartym. Podejście systemowe jest niezwykle istotne w teorii organizacji i zarządzania ze względu na to, iż pokazuje konieczność holistycznego spojrzenia na organizację, a nie badanie jej poszczególnych fragmentów. Należy także podkreślić, iż podejście systemowe przyczyniło się do rozwoju techniki modelowania i projektowania. W naukach o zarządzaniu i jakości jest konsekwencją wiązania organizacji jako systemu otwartego z otoczeniem i prowadzenia z nim wymiany (zgodnie z teorią systemów L. von Bertalaniffy'ego, por. www.isss.org/lumLVB.htm).

Teoria systemowa znalazła swoje odzwierciedlenie w *systemach zarządzania*. Prekursorem opisu systemu zarządzania w polskiej literaturze był A. Koźmiński (1971) Wskazywał, iż w organizacji zachodzą procesy decyzyjne, a podstawowymi elementami systemu są: mechanizmy ludzkiego zachowania, role społeczne i organizacyjne, system informacyjny, mechanizmy kierowania zespołami pracowniczymi i czynniki techniczne. Dogłębnej analizy systemów zarządzania w polskiej literaturze dokonała A. Stawowy (2018, s. 244–254), wskazując m.in. na definicje:

- A. Gościńskiego (1968) – autor rozróżnia system zarządzania, który stanowią cele strategiczne i operacyjne, zadania, decyzje i potrzeby informacyjne oraz podsystem informacyjny rozumiany jako bazy danych i układ obszarów decyzyjnych. W skład struktury systemu wchodzą: projektowanie i produkcja wyrobów, planowanie i kontrola materiałów, sprzedaż;
- J. Trzcieniewskiego (1980), który uważa, iż system zarządzania jest podsystemem, w skład którego wchodzą powiązane elementy, służące realizacji celów instytucji, doborowi metod i środków do działania, powiązaniu i zharmonizowaniu działań indywidualnych i zespołowych;
- T. Mendla i H. Witczaka (1982), którzy zdefiniowali system jako spójny zbiór zasad, celów i kryteriów, środków, metod podejmowania decyzji, wywierania nie wykonawczego wpływu oraz kontrolowania. W skład tak zdefiniowanego systemu wchodzą: czynniki zarządzania, wymagania metody i techniki;
- L. Szybińskiego (1984), który zdefiniował system jako zbiór obiektów zmierzających do spowodowania realizacji przez instytucję określonych celów;
- A. K. Koźmińskiego i K. Obłoja (2008), którzy nawiązują do systemu zarządzania poprzez opis instrumentów zarządzania, tj.: kultury organizacyjnej, struktury, procedury operacyjnej i strategii. Elementy te stanowią według autorów wewnętrznie spójne zespoły służące utrzymaniu równowagi funkcjonalnej organizacji;
- G. Bełzy (2011), który w swojej pracy definiuje system jako całokształt wartości i celów, regulacji i struktur oraz metod i praktyk, a także relacji między nimi warunkujących proces zarządzania organizacją.

A. Stawowy (2018, s. 251) podkreśla, iż systemowość organizacji polega na tym, że organizacja jako system jest czymś więcej niż sumą jej składowych. Uporządkowane relacje i sposób oddziaływania na siebie jej elementów powoduje powstanie wartości dodanej. System tak powinien być zaprojektowany, aby wielkość owej wartości dodanej była możliwie największa w warunkach, w których funkcjonuje organizacja. Kluczową rolą systemu jest ochrona stabilności organizacji przed negatywnym wpływem otoczenia, poprzez zapewnienie jej odpowiedniej elastyczności, dzięki której jest zdolna odpowiednio wcześniej reagować na zmiany oraz dostosować się do nich. Dlatego też system zarządzania oznacza sposób zorganizowania elementów organizacji, dzięki któremu możliwe jest osiąganie celów organizacji oraz zapewnienie ciągłości i stabilności jej funkcjonowania. Systemy zarządzania mogą dotyczyć jednej lub kilku dyscyplin, np. jakości, środowiska, bezpieczeństwa i higieny pracy, zarządzania finansami czy energią.

Wartą podkreślenia jest definicja podana przez normę ISO 9000:2015 (PN-EN ISO 9001, luty 2016), która przez system zarządzania, rozumie zbiór powiązanych lub wzajemnie oddziałujących elementów organizacji do ustanowienia polityk i celów oraz procesów do osiągania tych celów (ISO 9000:2015, pkt 3.5.3). Zakres systemu może obejmować całą organizację, określone i zidentyfikowane funkcje i działy lub co najmniej jedną funkcję w grupie organizacji.

Systemy zarządzania nie tylko strukturalizują poszczególne grupy działań (planowanie, organizowanie, przewodzenie i kontrolowanie/doskonalenie), ale umożliwiają zarządzanie, zwiększając tym samym wydajność zasad, procedur, procesów stosowanych w organizacji. Jak wskazuje D. Senczyk (2014, s. 155), system zarządzania powinien posiadać następuje elementy:

- zasoby – dzięki którym może działać, a więc zarówno materialne, jak i niematerialne, składowe;
- procesy – dzięki którym cel jest możliwy do realizacji;
- wejścia – dane, wytyczne, informacje, potrzebne do budowy systemu;
- wyjścia – dzięki którym zostaje osiągnięty cel.

Na tym tle T. Borys wprowadza pojęcie *sformalizowanego i znormalizowanego systemu zarządzania jakością*. Według autora (Borys 2011, s. 33) sformalizowany system zarządzania jest spójnym zestawem rozwiązań systemowych, mających zapewnić, że organizacja świadomie planuje, realizuje, kontroluje i doskonali swoją działalność. Wymagania dla takiego systemu są ujednolicone, czyli opracowane i przedstawione w dostępnym dokumencie, a spełnienie ich jest weryfikowane przez organizację zewnętrzną. Jak podkreśla J. Łuczak (2004, s. 100), wyraźny nurt formalizacji umożliwia wzrost wiarygodności przedsiębiorstwa oraz wzrost konkurencyjności poprzez lepsze wykorzystanie zasobów, stabilność procesów czy też zmniejszenie strat.

Natomiast *system znormalizowany* rozumiany jest taki system sformalizowany, którego struktura i zasady funkcjonowania zostały opisane w normach krajowych czy międzynarodowych, w tym europejskich.

Istotne staje się wyjaśnienie samego pojęcia „znormalizowane systemy zarządzania". Według J. Łańcuckiego (2016, s. 14) systemy objęte procesem normowania sprzyjają ustanowieniu niezbędnego, minimalnego zestawu wymagań, których spełnienie powinno umożliwić osiągnięcie przez organizację zaplanowanych, zgodnych z wymaganiami klientów wyników.

Istota *normalizacji* została zawarta w preambule Rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 1025/2012 z dnia 25 października 2012 r. (Dz.U. UE L 316 z 14.11.2012 r.) i wskazuje, iż celem normalizacji jest określenie dobrowolnych specyfikacji technicznych i jakościowych, którym mogą odpowiadać obecne lub przyszłe produkty, procesy produkcji lub usługi. Do podstawowym zasad w dziedzinie normalizacji zostały zaliczone: spójność, przejrzystość, otwartość, konsensus, dobrowolność stosowania, niezależność od szczególnych interesów i skuteczność. Parlament Europejski w pkt. 11 cytowanej preambuły wskazuje, iż normy dotyczące usług są dobrowolne, a impuls do ich opracowywania powinny stanowić czynniki rynkowe. J. Łańcucki (2016, s. 12) podkreśla, iż przestrzeganie dobrowolnych norm ma służyć:

- łatwiejszemu dostępowi do rynku,
- poprawie wyników działalności,
- wspieraniu przepisów w zakresie zdrowia i bezpieczeństwa,
- wspieraniu prywatności, bezpieczeństwa i interoperacyjności w zakresie technologii informacyjno-komunikacyjnych (ICT),
- reagowaniu na główne wyzwania społeczne.

Ważnym aspektem jest odniesienie się do krajowej ustawy o normalizacji, tj. ustawy z dnia 12 września 2002 roku o normalizacji (Dz.U. 2002 Nr 169, poz. 1386). Ustawa określa podstawowe cele i zasady normalizacji oraz jej organizację i finansowanie. Wyraźnie wskazuje, iż Polska Norma jest normą krajową, przyjętą w drodze konsensu i zatwierdzoną przez krajową jednostkę normalizacyjną, powszechnie dostępną, oznaczoną symbolem PN. Może być wprowadzeniem normy europejskiej lub międzynarodowej. Na podstawie ustawy o normalizacji został powołany Polski Komitet Normalizacyjny jako krajowa państwowa jednostka normalizacyjna, realizująca cele zawarte w art. 3 niniejszej ustawy.

Aksjologiczną podstawę znormalizowanych systemów zarządzania skorelowanych z trzema ładami koncepcji zrównoważonego rozwoju (ład społeczny, gospodarczy, przestrzenno-przyrodniczy) stanowi etyka biznesu i koncepcja społecznej odpowiedzialności. Podczas gdy etyka biznesu wymaga przestrzegania zasad moralnego, uczciwego i lojalnego postępowania w stosunku do klientów wewnętrznych i zewnętrznych, to społeczna odpowiedzialność przedsiębiorstw oznacza obowiązek wprowadzania społecznych kryteriów do procesów podejmowania decyzji strategicznych oraz do ich realizowania zapewniającego kojarzenie szeroko rozumianych korzyści środowiska z własnym interesem jednostek gospodarczych (Ejdys 2011, s. 12).

Stosowanie podejścia znormalizowanego prowadzi do formalizacji i dokumentowania szczególnie typowych i powtarzalnych działań. Wiąże się to z takimi zjawiskami, jak: wnikliwe analizowanie problemów, jednoznaczne przekazywanie wyczerpujących informacji, optymalne uporządkowanie celów i czynności, łatwość kontroli i egzekwowania odpowiedzialności, minimalizowanie błędów. Niewłaściwie prowadzona normalizacja sprzyja nadmiernej biurokratyzacji oraz utrwaleniu się rutynowych sposobów działania, co może być czynnikiem hamującym interwencję i wdrażanie korzystnych zmian (Hamrol 2017, s. 15).

Jak wskazuje J. Ejdys (2011, s. 20–21), idea standaryzacji zakłada swobodę w interpretowaniu ogólnych wymagań i ich dostosowaniu do potrzeb jednostek organizacyjnych w celu maksymalizacji indywidualnych korzyści. Znormalizowane systemy zarządzania stanowią tylko jedno z narzędzi, które może być wykorzystane w procesie zarządzania organizacją. Autorka wskazuje, iż

czynia się do zaangażowania najwyższego kierownictwa i pracowników w proces ciągłego doskonalenia. Doskonalenie, jako fundamentalna zasada znormalizowanych systemów, polega na stopniowym poprawianiu procesów i wyników oraz stanowi proces dostosowania się do zmian. Ta potrzeba doskonalenia wynika z:

- teoretycznych założeń i wymogów formalnych stawianych dla systemów zarządzania w aspekcie doskonalenia,
- wewnętrznych potrzeb jednostek organizacyjnych posiadających takie systemy,
- zmieniających się uwarunkowań zewnętrznych i nowych trendów na rynku.

Znormalizowane systemy są często integrowane ze sobą. Poszczególne elementy są w takiej sytuacji współzależne i powiązane ze sobą – często interakcyjnie. D. Senczyk (2014, s. 158) wyróżnia następujące poziomy integracji, podkreślając, iż zintegrowany system zarządzania to system spełniający wymagania co najmniej dwóch norm:

- Integracja I typu – integracja systemów zgodnych z ISO 9001, ISO 14001, PN – N – 45001;
- Integracja II typu – dotyczy wdrażania systemów zarządzania bazujących na normie ISO 9000 wraz z odpowiednimi rozszerzeniami i dodatkowymi wymaganiami;
- Integracja III typu – polegająca na łączeniu systemu ISO 9001 z więcej niż jednym rozszerzeniem;
- Integracja IV typu – do której zaliczamy systemy stanowiące połączenie systemów typu I z systemem typu II lub połączenie któregokolwiek z tych systemów z systemami o odrębnej strukturze stosowanymi w różnych branżach, np. HACCP (ang. *Hazard Analysis and Critical Control Points*, pol. System Analizy Zagrożeń i Krytycznych Punktów Kontroli dla przemysłu spożywczego), GMP (ang. *Good Manufacturing Practice*, pol. Dobra Praktyka Wytwarzania – przemysł farmaceutyczny), GLP (ang. *Good Laboratory Practice*, pol. Dobra Praktyka Laboratoryjna), system zarządzania bezpieczeństwem informacji ISMS (ang. *Information Security Management System*, pol. Sieć Cyfrowa z Integracją Usług).

Jak wskazuje A. Hamrol (2017, s. 55), zastosowanie zintegrowanego systemu zarządzania daje wiele korzyści:

- zastosowanie tych samych metod wdrażania, weryfikowania, zatwierdzania i nadzorowania dokumentów;
- wprowadzenie jednolitego systemu dokumentacji;
- osiągnięcie wysokiego standardu jakościowego, zapewniającego wzrost konkurencyjności na rynku;
- ograniczenie kosztów utrzymania systemów;
- możliwość prowadzenia szkoleń obejmujących wszystkie zintegrowane aspekty;
- możliwość jednoczesnego prowadzenia audytów i certyfikacji;
- zmniejszenie liczby personelu zajmującego się utrzymaniem systemu;
- zapobieganie konfliktom wynikającym z funkcjonowania niezależnych systemów;
- zmniejszenie nakładów na wdrożenie systemów.

Głównymi przesłankami integracji systemów zarządzania są:

- struktura norm wykorzystująca cykl Deminga PDCA (plan – do – *check-act*);
- podobne zestawienie wymagań;
- wspólne kluczowe procesy: odpowiedzialność kierownictwa, zasoby, realizacja procesów, pomiary, analizy, doskonalenie;
- przyjęcie podejścia procesowego.

W zakresie tworzenia znormalizowanych systemów, w architekturze systemów wykorzystano koncepcję *High Level Structure* (ang. HLS, pol. Struktura Wysokiego Poziomu), zawartą w zasadach opracowywania dokumentów normatywnych przez Międzynarodową Organizację Normalizacyjną ISO. Załącznik – *Annex SL Proposal for management system standards* (załącznik SL, znany również jako załącznik L w wydaniu z 2019 roku), określa, w jaki sposób pisać normy ISO Management System Standard (MSS). Zapewnia nową strukturę dla standardów systemów zarządzania, zastępując historyczny przewodnik ISO 83 i rozszerzając strukturę bazową. Załącznik opisuje ramy ogólnego systemu zarządzania, które powinny być rozwijane poprzez dodawanie wymagań specyficznych dla danej dyscypliny. Koncepcja ta bazuje na dwóch założeniach:

1. Unifikacji struktury wszystkich norm dla systemów zarządzania.
2. Identyczności bazowej tekstu, terminologii i podstawowych definicji stosowanych we wszystkich normach systemów zarządzania.

Koncepcja HLS zakłada nie tylko stosowanie prostego języka, ale także sam wygląd ogólny. Struktura HLS odnosi się do:

1. Zakresu – określenia zamierzonych wyników systemu zarządzania.

czynia się do zaangażowania najwyższego kierownictwa i pracowników w proces ciągłego doskonalenia. Doskonalenie, jako fundamentalna zasada znormalizowanych systemów, polega na stopniowym poprawianiu procesów i wyników oraz stanowi proces dostosowania się do zmian. Ta potrzeba doskonalenia wynika z:

- teoretycznych założeń i wymogów formalnych stawianych dla systemów zarządzania w aspekcie doskonalenia,
- wewnętrznych potrzeb jednostek organizacyjnych posiadających takie systemy,
- zmieniających się uwarunkowań zewnętrznych i nowych trendów na rynku.

Znormalizowane systemy są często integrowane ze sobą. Poszczególne elementy są w takiej sytuacji współzależne i powiązane ze sobą – często interakcyjnie. D. Senczyk (2014, s. 158) wyróżnia następujące poziomy integracji, podkreślając, iż zintegrowany system zarządzania to system spełniający wymagania co najmniej dwóch norm:

- Integracja I typu – integracja systemów zgodnych z ISO 9001, ISO 14001, PN – N – 45001;
- Integracja II typu – dotyczy wdrażania systemów zarządzania bazujących na normie ISO 9000 wraz z odpowiednimi rozszerzeniami i dodatkowymi wymaganiami;
- Integracja III typu – polegająca na łączeniu systemu ISO 9001 z więcej niż jednym rozszerzeniem;
- Integracja IV typu – do której zaliczamy systemy stanowiące połączenie systemów typu I z systemem typu II lub połączenie któregokolwiek z tych systemów z systemami o odrębnej strukturze stosowanymi w różnych branżach, np. HACCP (ang. *Hazard Analysis and Critical Control Points*, pol. System Analizy Zagrożeń i Krytycznych Punktów Kontroli dla przemysłu spożywczego), GMP (ang. *Good Manufacturing Practice*, pol. Dobra Praktyka Wytwarzania – przemysł farmaceutyczny), GLP (ang. *Good Laboratory Practice*, pol. Dobra Praktyka Laboratoryjna), system zarządzania bezpieczeństwem informacji ISMS (ang. *Information Security Management System*, pol. Sieć Cyfrowa z Integracją Usług).

Jak wskazuje A. Hamrol (2017, s. 55), zastosowanie zintegrowanego systemu zarządzania daje wiele korzyści:

- zastosowanie tych samych metod wdrażania, weryfikowania, zatwierdzania i nadzorowania dokumentów;
- wprowadzenie jednolitego systemu dokumentacji;
- osiągnięcie wysokiego standardu jakościowego, zapewniającego wzrost konkurencyjności na rynku;
- ograniczenie kosztów utrzymania systemów;
- możliwość prowadzenia szkoleń obejmujących wszystkie zintegrowane aspekty;
- możliwość jednoczesnego prowadzenia audytów i certyfikacji;
- zmniejszenie liczby personelu zajmującego się utrzymaniem systemu;
- zapobieganie konfliktom wynikającym z funkcjonowania niezależnych systemów;
- zmniejszenie nakładów na wdrożenie systemów.

Głównymi przesłankami integracji systemów zarządzania są:

- struktura norm wykorzystująca cykl Deminga PDCA (plan – do – *check-act*);
- podobne zestawienie wymagań;
- wspólne kluczowe procesy: odpowiedzialność kierownictwa, zasoby, realizacja procesów, pomiary, analizy, doskonalenie;
- przyjęcie podejścia procesowego.

W zakresie tworzenia znormalizowanych systemów, w architekturze systemów wykorzystano koncepcję *High Level Structure* (ang. HLS, pol. Struktura Wysokiego Poziomu), zawartą w zasadach opracowywania dokumentów normatywnych przez Międzynarodową Organizację Normalizacyjną ISO. Załącznik – *Annex SL Proposal for management system standards* (załącznik SL, znany również jako załącznik L w wydaniu z 2019 roku), określa, w jaki sposób pisać normy ISO Management System Standard (MSS). Zapewnia nową strukturę dla standardów systemów zarządzania, zastępując historyczny przewodnik ISO 83 i rozszerzając strukturę bazową. Załącznik opisuje ramy ogólnego systemu zarządzania, które powinny być rozwijane poprzez dodawanie wymagań specyficznych dla danej dyscypliny. Koncepcja ta bazuje na dwóch założeniach:

1. Unifikacji struktury wszystkich norm dla systemów zarządzania.
2. Identyczności bazowej tekstu, terminologii i podstawowych definicji stosowanych we wszystkich normach systemów zarządzania.

Koncepcja HLS zakłada nie tylko stosowanie prostego języka, ale także sam wygląd ogólny. Struktura HLS odnosi się do:

1. Zakresu – określenia zamierzonych wyników systemu zarządzania.

nych w danej normie.
3. Terminów i definicji – wspólnych dla całego standardu.
4. Kontekstu organizacji – zrozumienia wewnętrznych i zewnętrznych problemów, potrzeb i oczekiwań stron zainteresowanych, systemów zarządzania i jego zakresu.
5. Przywództwa – odpowiedzialności i zaangażowania najwyższego kierownictwa, polityki, ról organizacyjnych, obowiązków.
6. Planowania – działań mających na celu przeciwdziałanie ryzyku i szansom, ustanowienie celów jakościowych i planowania ich osiągnięcia.
7. Wsparcia – w zakresie wymaganych zasobów, kompetencji, świadomości, komunikacji i udokumentowanych informacji.
8. Działań operacyjnych – planowania i nadzoru nad działaniami operacyjnymi.
9. Oceny efektów działalności – monitorowania, pomiaru, analizy i oceny, audytu wewnętrznego, przeglądu zarządzania.
10. Poprawy i doskonalenia – niezgodności, działań naprawczych i ciągłego doskonalenia.

Strukturę ramową wymagań przedstawiono w tabeli 2.3.

Na bazie struktury HLS zostały spisane wymagania m.in. dla norm:

- ISO 9001:2015 – Systemy zarządzania jakością – wymagania.
- ISO 14001:2015 – Systemy zarządzania środowiskowego – wymagania wraz z wytycznymi dotyczącymi stosowania.
- ISO 22000:2018 – Systemy zarządzania bezpieczeństwem żywności – wymagania dla każdej organizacji w łańcuchu żywnościowym.
- ISO/IEC 27001:2013 – Technologie informacyjne – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – wymagania.
- ISO 37001:2016 – Systemy zarządzania antykorupcyjnego – wymagania wraz ze wskazówkami dotyczącymi stosowania.
- ISO 44001:2017 – Systemy zarządzania relacjami biznesowymi opartymi na współpracy – wymagania i ramy.
- ISO 45001:2018 – Systemy zarządzania bezpieczeństwem i higieną pracy – wymagania wraz z wytycznymi dotyczącymi stosowania.
- ISO 50001:2018 – Systemy zarządzania energią – wymagania wraz z wytycznymi dotyczącymi stosowania.
- ISO 55001:2014 – Zarządzanie aktywami – Systemy zarządzania – wymagania.

Struktura HLS		CYKL PCDA
1.	Zakres normy	
2.	Powołania normatywne	
3.	Terminy i definicje	
4.	Kontekst organizacji	PLAN
4.1.	Zrozumienie organizacji i jej kontekstu	
4.2.	Zrozumienie potrzeb i oczekiwań stron zainteresowanych	
4.3.	Określenie zakresu systemu zarządzania XXX	
4.4.	System zarządzania XXX	
5.	Przywództwo	
5.1.	Przywództwo i zaangażowanie	
5.2.	Polityka	
5.3.	Rola, odpowiedzialność i uprawnienia w organizacji	
6.	Planowanie	
6.1.	Działania mające na celu określenie ryzyka i możliwości	
6.2.	Cele XXX i planowanie osiągnięcia celów	
7.	Wsparcie	DO
7.1.	Zasoby	
7.2.	Kompetencje	
7.3.	Świadomość	
7.4.	Komunikacja	
7.5.	Udokumentowane informacje	
8.	Działania operacyjne	
8.1.	Planowanie i nadzór nad działaniami operacyjnymi	
9.	Ocena efektów działalności	CHECK
9.1.	Monitorowanie, pomiary, analiza i ocena	
9.2.	Audyt wewnętrzny	
9.3.	Przegląd zarządzania	
10.	Doskonalenie	ACT
10.1.	Niezgodność i działania korygujące	
10.2.	Ciągłe doskonalenie	

Źródło: opracowanie własne.

Początków znormalizowanego podejścia do jakości można dopatrywać się w roku 1959, w zapisach dokumentu *MIL – Q – 9858* zawierającego wymagania dla programu jakości. Został on wprowadzony przez Departament Obrony Stanów Zjednoczonych dla dostawców przemysłu zbrojeniowego. Po ich zmodyfikowaniu w roku 1963 stały się podstawą budowania systemu zapewnienia jakości obowiązującego wszystkich dostawców armii amerykańskiej. Było to związane m.in. z konfliktem w Wietnamie. Dowództwo armii amerykańskiej chciało zagwarantować, aby sprzęt dostarczany żołnierzom był sprawny w warunkach bojowych. W 1985 roku International Organization for Standardization (ISO) z siedzibą w Genewie podjęła pracę nad stworzeniem powszechnie akceptowanych norm międzynarodowych. W wyniku prac Komitetu Technicznego ISO TC 176 ustanowiona została w 1986 roku norma ISO 8402. Przełomowym okazał się jednak rok 1987, w którym Międzynarodowa Organizacja Normalizacyjna ISO przyjęła zbiór norm znanych jako seria ISO 9000. Ich celem było wypracowanie wspólnych pojęć i zharmonizowanie wymagań dotyczących jakości w poszczególnych krajach. W założeniu normy miały mieć charakter międzynarodowy i uniwersalny. W tym samym roku kraje Europejskiej Wspólnoty Gospodarczej (EWG) i Europejskiego Stowarzyszenia Wolnego Handlu (EFTA) przyjęły normy w niezmienionej postaci jako wzorce europejskie oznaczone symbolem EN 290025, dokonując ich aktualizacji co sześć do ośmiu lat 26.

W roku 2015 miała miejsce ostatnia nowelizacja normy ISO 9001, ze względu na określenie wspólnej struktury systemów zarządzania oraz wprowadzenia wspólnego podstawowego tekstu, terminów i definicji (zgodnie z *załącznikiem SL do Dyrektywy ISO\IEC – część 1 – Skonsolidowany Suplement ISO* – o czym szerzej była mowa w podrozdziale 2.2 pracy). Warto zwrócić uwagę, iż same

[25] Skrót ISO pochodzi od greckiego słowa *isos* oznaczającego równy, równać do standardu. Skrót ISO nie pochodzi od *International Organization for Standarization*, pomimo że w potocznym rozumieniu jak i w niektórych publikacjach ma to miejsce.

[26] Nowelizacja norm przebiega według następującego procesu: (1) WDs (*Working Drafts*) – projekty robocze opracowywane w Working Groups; (2) CD (*Committee Draft*) – projekt normy Komitetu Technicznego ISO; (3) DIS (Draft International Standard) – projekt normy międzynarodowej ankietowany w krajowych Komitetach Technicznych; (4) FDIS (*Final Draft International Standard*) – końcowy projekt normy ISO po ankiecie (przegłosowany i zatwierdzony do publikacji).

i funkcjonowania systemu, opierają się na wspomnianym już cyklu Deminga – PDCA[27]. Połączenie zarządzania procesami z podejściem opartym na ryzyku oraz uwzględnieniem cyklu PCDA na wszystkich poziomach organizacji stało się nową podstawą struktury normy (por. rysunek 2.3).

Tabela 2.4. Proces nowelizacji norm ISO serii 9000

Rok normalizacji	Charakter nowelizacji
1987	Pierwsze wydanie normy
1994	Pierwsza „mała" nowelizacja
2000	Druga „duża" nowelizacja (polskie wydanie PN-EN ISO 9001:2001)
2008	Trzecia „mała" nowelizacja (polskie wydanie PN-EN ISO 9001:2009)
2015	Czwarta „duża" nowelizacja (polskie wydanie PN-EN ISO 9001:2015)

Źródło: opracowanie własne.

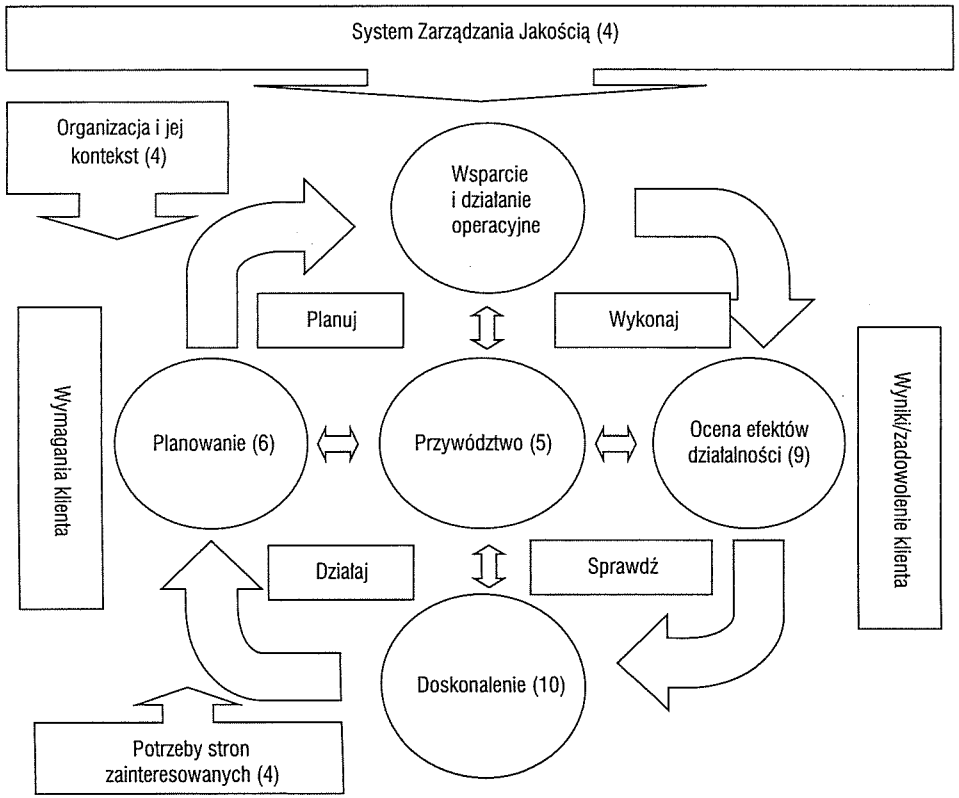
I tak, w normie ISO 9001:2015:

- *Plan – Planowanie* – odnosi się do: rozdziału 4 – Organizacji i jej kontekstu oraz rozdziału 6 – Planowania.
- *Do – Wykonanie* – odnosi się do rozdziału 7 – wsparcia oraz rozdziału 8 – działań operacyjnych.
- *Check – Sprawdzenie* – to przede wszystkim rozdział 9, czyli ocena efektów działania.
- *Act – Działanie* – to rozdział 10 – Doskonalenie.

Podobnie jak we wcześniejszych wydaniach norm, także obecnie kluczowym aspektem jest uruchomienie procesu ciągłego doskonalenia. Podejmowane w tym zakresie działania powinny obejmować:

- doskonalenie wyrobów i usług w celu spełnienia wymagań pacjenta oraz przyszłych potrzeb i oczekiwań;
- korygowanie, zapobieganie lub ograniczanie niepożądanych skutków;
- doskonalenie efektów działań i skuteczności systemu jakości.

[27] W literaturze można spotkać się z tłumaczeniem polskim cyklu, nazwa PWSD to: *p* – planuj, *w* – wykonaj, *s* – sprawdź i *d* – działaj.



Źródło: opracowanie własne na podstawie PN-EN ISO 9001: 2015 (numery na rysunku odpowiadają rozdziałom normy ISO 9001: 2015).

2.3.1. Wymagania normy ISO 9001:2015

Podstawę wymagań normy ISO 9001:2015 stanowi:

1. Wprowadzenie kontekstu organizacji.
2. Uwzględnienie podejścia opartego na ryzyku.
3. Elastyczne podejście do dokumentacji.
4. Uwzględnienie wiedzy organizacji.
5. Wprowadzenie zarządzania zmianami na poziomie operacyjnym.
6. Położenie szczególnego nacisku na proces ciągłego doskonalenia.

1. Zakres normy	
2. Powołanie normatywne	
3. Terminy i definicje	
4. Kontekst organizacji	PLAN
4.1. Zrozumienie organizacji i jej kontekstu	
4.2. Zrozumienie potrzeb i oczekiwań stron zainteresowanych	
4.3. Określenie zakresu systemu zarządzania jakością	
4.4. System zarządzania jakością i jego procesy	
5. Przywództwo	
5.1. Przywództwo i zaangażowanie	
5.2. Polityka	
5.3. Role, odpowiedzialność i uprawnienia w organizacji	
6. Planowanie	
6.1. Działania odnoszące się do ryzyk i szans	
6.2. Cele jakościowe i planowanie ich osiągnięcia	
6.3. Planowanie zmian	
7. Wsparcie	DO
7.1. Zasoby	
7.2. Kompetencje	
7.3. Świadomość	
7.4. Komunikacja	
7.5. Udokumentowane informacje	
8. Działania operacyjne	
8.1. Planowanie i nadzór nad działaniami operacyjnymi	
8.2. Wymagania dotyczące wyrobów i usług	
8.3. Projektowanie i rozwój wyrobów i usług	
8.4. Nadzór nad procesami, wyrobami i usługami dostarczanymi z zewnątrz	
8.5. Produkcja i dostarczanie usługi	
8.6. Zwolnienie wyrobów i usług	
8.7. Nadzór nad niezgodnymi wyjściami	

9.1. Monitorowanie, pomiary, analiza i oceny	CHECK
9.2. Audyt wewnętrzny	
9.3. Przegląd zarządzania	
10. Doskonalenie	ACT
10.1. Postanowienia ogólne	
10.2. Niezgodności i działania korygujące	
10.3. Ciągłe doskonalenie	

Źródło: opracowanie własne.

I tak, określenie *kontekstu organizacji* stanowi pretekst do tego, aby skłonić osoby zarządzające podmiotami leczniczymi do przeprowadzenia analizy otoczenia przy uwzględnieniu metod analizy strategicznej. Stanowi to wartość dodaną do wdrożenia systemu jakości, gdyż pozwala zmniejszyć obszar niepewności, jaki towarzyszy prowadzonej działalności. Ma to szczególne znaczenie w odniesieniu do podmiotów udzielających świadczeń medycznych, w przypadku których dynamika zmian zachodzących w otoczeniu jest szczególnie duża. Monitorowanie czynników zewnętrznych i wewnętrznych wiąże się z analizą zarówno mikro-, jak i makrootoczenia (omówionych w rozdziale pierwszym niniejszej pozycji). Zrozumienie kontekstu organizacji jest istotne do określenia kluczowych elementów systemu, takich jak zakres systemu zarządzania, procesy, polityka, cele jakościowe, ryzyka i szanse.

Obowiązek *szacowania ryzyk* stworzył warunki po temu, aby w większym stopniu zminimalizować prawdopodobieństwo wystąpienia sytuacji mogących stanowić zagrożenie dla pracowników, klientów jak i samej organizacji. Wynika to z faktu, że dokonując analizy, należy wskazać skutki występowania i jego prawdopodobieństwo. Ryzyk nie można całkowicie wyeliminować, ponieważ są wpisane w prowadzenie działalności gospodarczej, ale można wykazać, które są na poziomie akceptowalnym, a które na nieakceptowalnym. Podejście zaproponowane w nowym wydaniu normy przyjmuje traktowanie ryzyka nie jako pojedynczego elementu, co zmusza organizacje do systematyczności w zakresie prowadzonych analiz. W normie ISO 9001:2015 ryzyko rozumiane jako „wpływ niepewności" odnosi się do niepewności osiągania głównego celu, a więc dostarczania wyrobów i usług zgodnych z wymaganiami oraz dążenie do zwiększenia zadowolenia klienta. Ma to odzwierciedlenie w następujących rozdziałach:

pod uwagę czynniki wymienione w 4.1. – zrozumienie organizacji i jej kontekstu i 4.2. – zrozumienie potrzeb i oczekiwań stron zainteresowanych.

- Rozdział 5 – Przywództwo – najwyższe kierownictwo powinno promować w organizacji świadomość podejścia opartego na ryzyku.
- Rozdział 6 – Planowanie – zwraca uwagę na to, iż podjęte działania odnoszące się do ryzyk i szans powinny być proporcjonalne do potencjalnego wpływu na zgodność wyrobów i usług.
- Rozdział 8 – Działania operacyjne – działania związane z zapobieganiem ryzyk powinny być wdrożone zgodnie z wymaganiami pkt 8.1. – planowanie i nadzór nad działaniami operacyjnymi.
- Rozdział 9 – Ocena efektów działania – organizacja powinna mierzyć, monitorować, analizować i oceniać dane i informacje oraz wykorzystać wyniki analizy danych do oceny skuteczności działań podjętych w celu uwzględnienia ryzyka i szans.
- Rozdział 10 – Doskonalenie – organizacja powinna korygować, zapobiegać i redukować niepożądane skutki i doskonalić system zarządzania jakością oraz aktualizować ryzyka i szanse.

Istotnym aspektem wprowadzonym do znowelizowanej normy jest *uelastycznienie w podejściu do dokumentacji*. Pojęcie *udokumentowanej informacji* odnosi się do dokumentacji, która powinna być nadzorowana i utrzymywana przez organizacje, przy czym nośnik, na którym jest zawarta, pozostaje dowolny. Elastyczność przejawia się nie tylko w decydowaniu, jakie dokumenty powinny zostać określone, także w jakich obszarach będą one stosowane, ponad te, które określono w normie.

Interpretując pojęcie udokumentowanej informacji, warto odnieść się do definicji pojęcia „dokument". Zgodnie z normą ISO 9000 jest to informacja i jej nośnik. Dokumentem jest przykładowo: specyfikacja, plan jakości, instrukcja, formularz czy też zapis. *Zapisem* jest szczególna postać dokumentu, w którym przedstawiono uzyskane wyniki lub dowody przeprowadzonych działań (w przypadku podmiotu leczniczego może to być karta choroby pacjenta czy też wyniki jego badań).

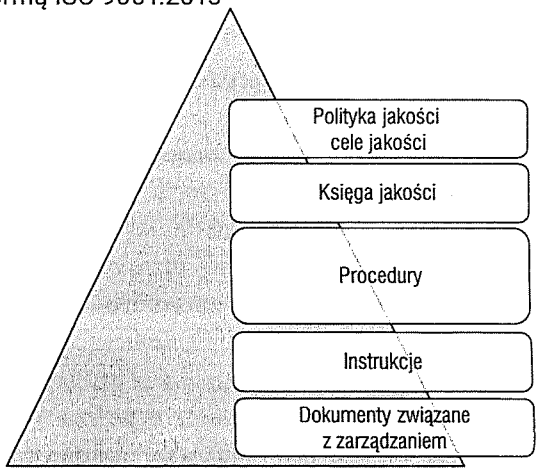
Dokonując hierarchizacji dokumentacji jakościowej, można wyróżnić następujące poziomy:

- Poziom 1 – dokumenty obejmujące zbiór wartości, celów i zamierzeń organizacji: polityka jakości, cele jakościowe. Wymagania normy ISO 9001 narzucają obowiązek opracowania polityki jakości i nakreślenia celów jakościowych.

księgi jakości, który może m.in. zawierać tę politykę i opisywać ogólne cele jakościowe. Jej opracowanie nie jest jednak obowiązkowe.

- Poziom 2 – procedury – dokumenty systemowe zawierające informacje w odniesieniu do audytów, postępowania z produktami/usługami niezgodnymi z wymaganiami.
- Poziom 3 – instrukcje jako dokumenty wskazujące wykonanie zadań oraz dokumenty związane z zarządzaniem.

Rysunek 2.4. Struktura dokumentacji systemu jakości zgodnego z normą ISO 9001:2015



Polityka jakości i cele – określenie nadrzędnych założeń związanych z prowadzoną działalnością.
Księga jakości (wariantowo) – jest dokumentem, w którym zawarte jest ustalenie polityki jakości oraz opisany jest system jakości. Księga jakości jest swoistym spisem treści podejmowanych działań w ramach systemu zarządzania jakością.
Procedury – systemowe: nadzór nad udokumentowanymi informacjami, nadzór nad wyrobem niezgodnym, audyt wewnętrzny, działania korygujące.
Instrukcje – instrukcje systemowe – standardy postępowania, instrukcje techniczne (np. obsługa urządzeń).
Dokumentacja związana z zarządzaniem – akty normatywne, dokumenty zewnętrzne (akty prawne, np. ustawy o zawodach, Kodeks Cywilny, Prawo Zamówień Publicznych), regulamin wewnętrzny, statut organizacji, zarządzenia dyrekcji).

Źródło: opracowanie własne.

macja udokumentowana – organizacja powinna określić:

- zakres systemu zarządzania jakością,
- politykę jakości,
- cele organizacji,
- kryteria oceny oraz zatwierdzania dostawców.

Ponadto organizacja powinna przechowywać udokumentowane informacje w formie zapisów (dowodów) w zakresie:

1) kalibracji sprzętu pomiarowego,
2) szkoleń, umiejętności i doświadczenia personelu,
3) przeglądu wymagań produktu, usługi,
4) przeglądu projektowania i rozwoju,
5) danych wejściowych do produktu lub usługi,
6) kontroli projektu lub rozwoju,
7) danych wyjściowych produktu lub usługi,
8) zmian w projekcie lub rozwoju,
9) właściwości produktu lub usługi,
10) zapis dotyczący rejestru własności klienta,
11) zapis nadzoru nad zmianami produktu, usługi,
12) zgodności produktu zgodnie z kryteriami akceptowalności,
13) niezgodności,
14) monitorowania i mierzenia wyników,
15) planu audytów wewnętrznych,
16) zapis z przeprowadzonego przeglądu kierownictwa,
17) wyników audytów wewnętrznych,
18) działań korygujących.

Warto wspomnieć, iż jeśli organizacja nie prowadzi jakiegoś procesu, jest automatycznie zwolniona z konieczności posiadania zapisów określonych wymaganiami rozdziału 8.3.

W przygotowaniu dokumentacji opisującej system zarządzania pomocnym jest przygotowanie mapy procesów. Przedstawia ona procesy główne i wspomagające (inaczej – wspierające, pomocnicze). Co do zasady procesy dzieli się na zarządcze – realizowane na poziomie najwyższego kierownictwa, np. opracowanie celów strategicznych rozwoju danej placówki, zarządzanie inwestycjami; główne – dodające wartość dla klienta (w tym przypadku pacjenta) oraz wspierające.

niają usługę medyczną, można wyróżnić m.in. identyfikację i przegląd wymagań pacjentów, aktywność informacyjną pozwalająca pozyskać i utrzymać pacjentów, ich obsługę w miejscu świadczenia oraz badanie satysfakcji klientów wewnętrznych i zewnętrznych. Procesami wspierającymi natomiast mogą być następujące: zarządzanie personelem (w tym szkolenie pracowników) oraz infrastrukturą (w tym łączność i zarządzanie informacją), zakup i nadzór nad dostawcami, a także logistyka (transport, magazynowanie). Przykładowa mapa procesów została przedstawiona na rysunku 2.5.

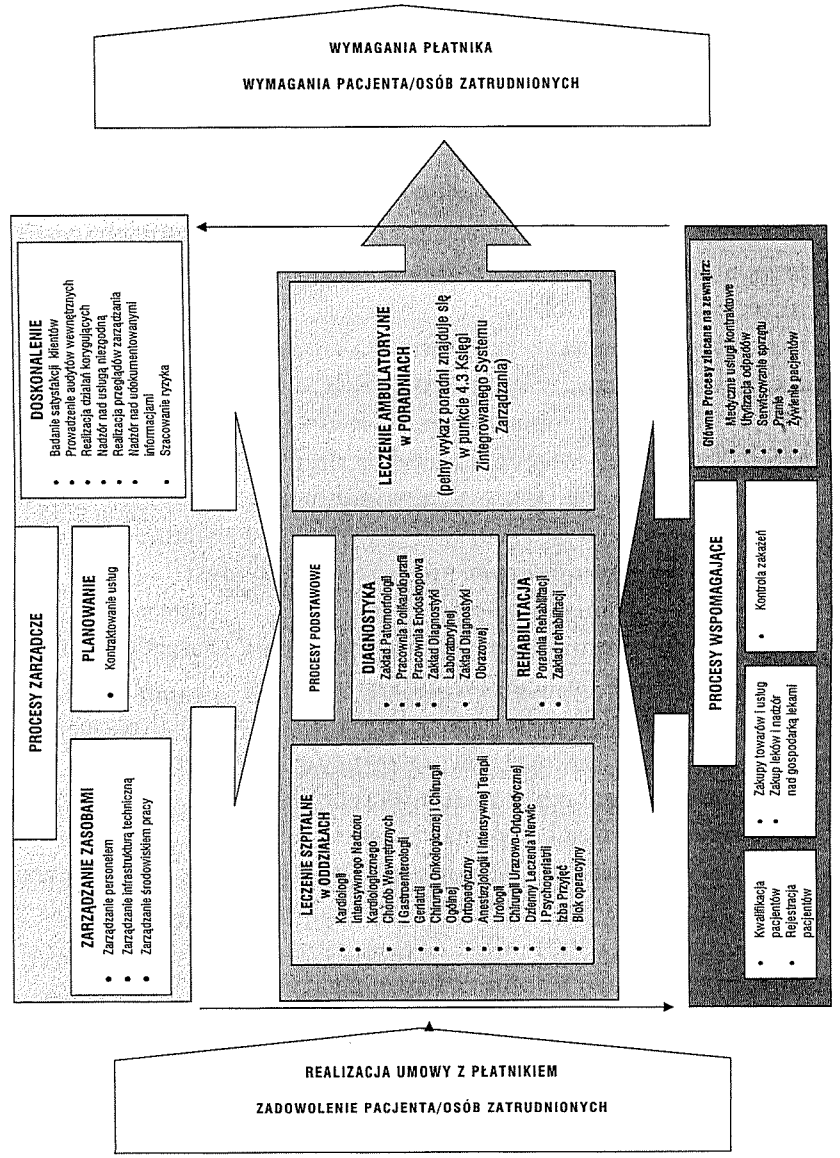
Wymienione przykładowe procesy powinny być możliwe szczegółowo opisane i podlegać nieustannemu doskonaleniu. W świetle wymagań normy ISO 9001 znowelizowanej w 2015 roku istotnym staje się także definiowanie oraz określenie współzależności między elementami procesu.

W normie ISO 9001:2015 istnieją również wymagania dotyczące *wprowadzenia zmian na poziomie systemu i poziomie operacyjnym*. Organizacje zgodnie z wytycznymi powinny rozważyć wszelkie możliwości wystąpienia zmian. W przypadku placówki medycznej mogą one wynikać z:

- informacji zwrotnych od pacjentów – weryfikacja poprzez badania ich satysfakcji,
- reklamacji ze strony pacjentów i ich rodzin,
- wyników audytów wewnętrznych,
- wyników przeglądu ze strony najwyższego kierownictwa.

Architektura systemu zarządzania jakością zgodnego z normą ISO 9001:2015 opiera się na uwzględnieniu takich filarów, jak:

1. Określenie kontekstu organizacji.
2. Zidentyfikowanie strony zainteresowanych.
3. Przeprowadzenie przeglądu procesów.
4. Przeprowadzenie analizy strategicznej. Zidentyfikowanie szans i zagrożeń.
5. Określenie planu dla wybranych szans i zagrożeń.
6. Określenie planu monitorowania.
7. Określenie planu komunikacji.
8. Wdrożenie dokumentów systemowych.
9. Przeprowadzenie audytów.
10. Przeprowadzenie przeglądu kierownictwa.



Rysunek 2.5. Mapa procesów

Źródło: opracowanie własne.

obejmuje następujące etapy:

Etap 1 – Przygotowanie

Przygotowanie do wdrożenia systemu obejmuje podjęcie decyzji w odniesieniu do:

- powołania osoby na stanowisko pełnomocnika ds. zapewnienia jakości – osoba powinna być zatrudniona na umowę o pracę, mieć wiedzę w zakresie procesów, które odbywają się w organizacji, chętnie podnosić swoje kwalifikacje w zakresie kompetencji jakościowych. Do zadań pełnomocnika należy:
  - proponowanie szczegółowych celów jakościowych w zgodzie z obowiązującą polityką jakości,
  - nadzór nad realizacją szczegółowych celów jakościowych,
  - kompleksowe prowadzenie, nadzorowanie i koordynacja wszelkich spraw związanych z funkcjonowaniem systemu zarządzania jakością zgodnie z ISO 9001:2015,
  - nadzór nad dokumentacją systemową: aktualizacja i wycofywanie dokumentacji nieaktualnej,
  - organizowanie i kompleksowe prowadzenie audytów,
  - nadzór nad działaniami korygującymi,
  - przygotowanie kompleksowych materiałów dla właściciela do okresowych przeglądów funkcjonowania systemu,
  - proponowanie szkoleń dla personelu zakładu z zakresu doskonalenia systemu zarządzania jakością (dla pracowników i audytorów),
  - utrzymywanie kontaktów z jednostką certyfikującą,
  - wysuwanie propozycji doskonalenia systemu;
- zakupu normy właściwej – powołany pełnomocnik ds. zapewnienia jakości w imieniu organizacji, dokonuje zakupu norm: ISO 9000: 2015, ISO 9001:2015, ISO 9004:2018. Zakupu można dokonać poprzez stronę internetową Polskiego Komitetu Normalizacyjnego w Warszawie;
- wyboru firmy consultingowej wspierającej proces wdrożenia lub też konsultanta/konsultantów posiadających wiedzę w przedmiotowym zakresie. Przy wyborze firmy należy wziąć pod uwagę następujące kryteria: cenę obejmującą cały zakres prowadzonych prac – tj. zarówno szkoleń, jak i przygotowania dokumentacji systemowej, listy z referencjami z wdrożonych systemów. Istotnym jest zwrócenie uwagi na liście referencyjnej zakresu prowadzonych prac oraz typu placówki, w jakiej system został wdrożony;

wstępnego. Raport z takiego audytu pozwoli na realne oszacowanie kosztów wdrożenia oraz przygotowania harmonogramu prowadzonych prac.

Etap 2 – Opracowanie dokumentacji systemowej

Na tym etapie następuje równolegle:

- prowadzenie wizyt studyjnych poszczególnych obszarów prowadzonej działalności, które powinny zawierać następujące fazy działania: audyt obszaru wraz ze wskazaniem konieczności wprowadzenia działań korygujących, wprowadzenie nowej dokumentacji w odpowiedzi na zmieniające się przepisy prawne, wykonanie konieczność analiz skuteczności i poprawności działania;
- przeprowadzenie szkoleń dla pracowników: szkolenia ogólne – informacyjne z zakresu normy ISO 9001:2015, celów i zakresu stosowania, korzyści z wdrożenia oraz przedstawienie harmonogramu prac;
- przeprowadzenie szkoleń dla wybranych audytorów wewnętrznych. Szkolenia warsztatowe powinny zostać zakończone przeprowadzeniem wraz z firmą zewnętrzną audytu wewnętrznego, oraz przygotowaniem raportu z audytu.

Etap 3 – Testowanie

W czasie minimum trzech miesięcy następuje wdrożenie przygotowanych i skonsultowanych dokumentów wraz wdrożeniem procedur. W okresie tym system jest korygowany oraz zbierane są opinie pracowników co do możliwości wprowadzenia korekt i poprawek. Ponadto powinien odbyć się przegląd zarządzania, który jest formą audytu wewnętrznego prowadzonego przez najwyższe kierownictwo. Raport z przeglądu zarządzania stanowi także ważne źródło do wprowadzania zmian w systemie. Etap testowania zawiera wstępną ocenę osiągnięcia założonych wskaźników po to, aby potwierdzić ocenę parametrów procesów: zarządzania infrastrukturą, zarządzania środowiskiem pracy, zarządzania personelem, nadzorem nad dokumentacją itd.

2.3.2. Znaczenie normy ISO 9001:2015 dla organizacji oraz problemy związane z jej wdrożeniem

Zgodnie z deklaracją twórców normy ISO mają przyczyniać się nie tylko do rozwoju normalizacji na całym świecie, ale także powinny ułatwiać współpracę pomiędzy organizacjami działającymi w różnych krajach, świadczenie

obejmuje następujące etapy:

Etap 1 – Przygotowanie

Przygotowanie do wdrożenia systemu obejmuje podjęcie decyzji w odniesieniu do:

- powołania osoby na stanowisko pełnomocnika ds. zapewnienia jakości – osoba powinna być zatrudniona na umowę o pracę, mieć wiedzę w zakresie procesów, które odbywają się w organizacji, chętnie podnosić swoje kwalifikacje w zakresie kompetencji jakościowych. Do zadań pełnomocnika należy:
  - proponowanie szczegółowych celów jakościowych w zgodzie z obowiązującą polityką jakości,
  - nadzór nad realizacją szczegółowych celów jakościowych,
  - kompleksowe prowadzenie, nadzorowanie i koordynacja wszelkich spraw związanych z funkcjonowaniem systemu zarządzania jakością zgodnie z ISO 9001:2015,
  - nadzór nad dokumentacją systemową: aktualizacja i wycofywanie dokumentacji nieaktualnej,
  - organizowanie i kompleksowe prowadzenie audytów,
  - nadzór nad działaniami korygującymi,
  - przygotowanie kompleksowych materiałów dla właściciela do okresowych przeglądów funkcjonowania systemu,
  - proponowanie szkoleń dla personelu zakładu z zakresu doskonalenia systemu zarządzania jakością (dla pracowników i audytorów),
  - utrzymywanie kontaktów z jednostką certyfikującą,
  - wysuwanie propozycji doskonalenia systemu;
- zakupu normy właściwej – powołany pełnomocnik ds. zapewnienia jakości w imieniu organizacji, dokonuje zakupu norm: ISO 9000: 2015, ISO 9001:2015, ISO 9004:2018. Zakupu można dokonać poprzez stronę internetową Polskiego Komitetu Normalizacyjnego w Warszawie;
- wyboru firmy consultingowej wspierającej proces wdrożenia lub też konsultanta/konsultantów posiadających wiedzę w przedmiotowym zakresie. Przy wyborze firmy należy wziąć pod uwagę następujące kryteria: cenę obejmującą cały zakres prowadzonych prac – tj. zarówno szkoleń, jak i przygotowania dokumentacji systemowej, listy z referencjami z wdrożonych systemów. Istotnym jest zwrócenie uwagi na liście referencyjnej zakresu prowadzonych prac oraz typu placówki, w jakiej system został wdrożony;

wstępnego. Raport z takiego audytu pozwoli na realne oszacowanie kosztów wdrożenia oraz przygotowania harmonogramu prowadzonych prac.

Etap 2 – Opracowanie dokumentacji systemowej

Na tym etapie następuje równolegle:

- prowadzenie wizyt studyjnych poszczególnych obszarów prowadzonej działalności, które powinny zawierać następujące fazy działania: audyt obszaru wraz ze wskazaniem konieczności wprowadzenia działań korygujących, wprowadzenie nowej dokumentacji w odpowiedzi na zmieniające się przepisy prawne, wykonanie konieczność analiz skuteczności i poprawności działania;
- przeprowadzenie szkoleń dla pracowników: szkolenia ogólne – informacyjne z zakresu normy ISO 9001:2015, celów i zakresu stosowania, korzyści z wdrożenia oraz przedstawienie harmonogramu prac;
- przeprowadzenie szkoleń dla wybranych audytorów wewnętrznych. Szkolenia warsztatowe powinny zostać zakończone przeprowadzeniem wraz z firmą zewnętrzną audytu wewnętrznego, oraz przygotowaniem raportu z audytu.

Etap 3 – Testowanie

W czasie minimum trzech miesięcy następuje wdrożenie przygotowanych i skonsultowanych dokumentów wraz wdrożeniem procedur. W okresie tym system jest korygowany oraz zbierane są opinie pracowników co do możliwości wprowadzenia korekt i poprawek. Ponadto powinien odbyć się przegląd zarządzania, który jest formą audytu wewnętrznego prowadzonego przez najwyższe kierownictwo. Raport z przeglądu zarządzania stanowi także ważne źródło do wprowadzania zmian w systemie. Etap testowania zawiera wstępną ocenę osiągnięcia założonych wskaźników po to, aby potwierdzić ocenę parametrów procesów: zarządzania infrastrukturą, zarządzania środowiskiem pracy, zarządzania personelem, nadzorem nad dokumentacją itd.

2.3.2. Znaczenie normy ISO 9001:2015 dla organizacji oraz problemy związane z jej wdrożeniem

Zgodnie z deklaracją twórców normy ISO mają przyczyniać się nie tylko do rozwoju normalizacji na całym świecie, ale także powinny ułatwiać współpracę pomiędzy organizacjami działającymi w różnych krajach, świadczenie

innymi techniki i ekonomii (Łańcucki 2006, s. 96). Głównym celem wdrażanych systemów zarządzania jakością jest zatem lepsze spełnienie oczekiwań klientów, poprawa i doskonalenie procesów świadczenia usługi. Doskonalenie organizacji poprzez zdobywanie zaufania klientów, poprawa organizacji pracy, szybszy przepływ informacji, nadzór nad prowadzoną dokumentacją – to kolejne argumenty na wdrożenie systemu.

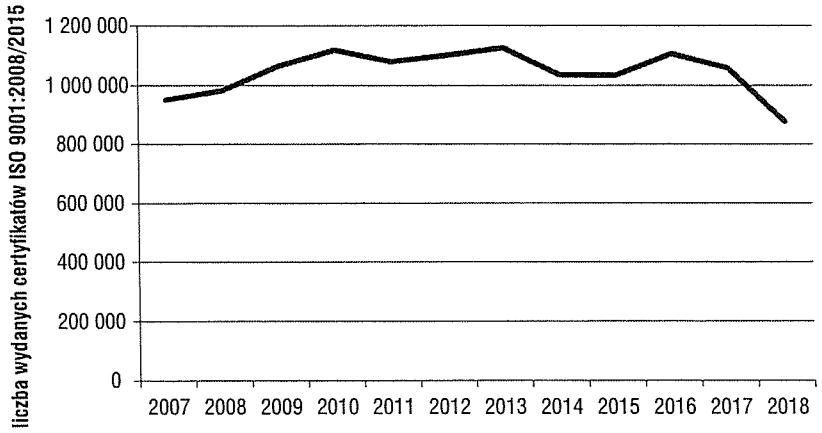
Tabela 2.6. Liczba wydanych certyfikatów ISO 9001:2008/ 2015 na koniec danego roku

	Lata												
	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Wydane cert. ISO	982 832	1 064 785	1 118 510	1 079 647	1 101 272	1 126 460	1 036 321	1 033 936	1 106 356	1 058 504	877 620	886 521	916 842
Wzrost wydanych cert. w ujęciu rok do roku (w %)	3,3	8,3	5,1	-3,5	2,0	2,3	-8,1	-0,2	0,7	-4,3	-1,8	1,0	3,77

Źródło: *The ISO Survey of Certifications* – 2020.

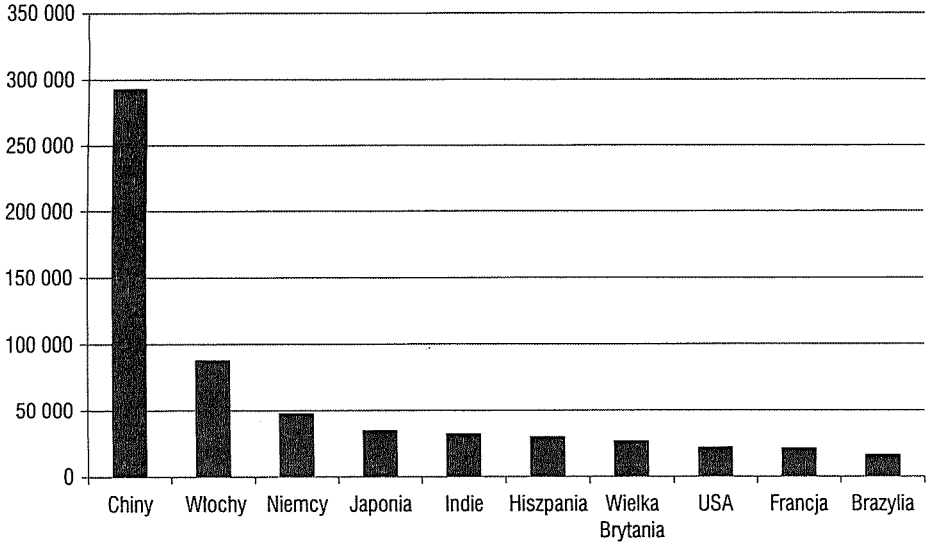
Z przedstawionych w tabeli danych wynika, że liczba wydawanych certyfikatów do 2010 roku rosła. Od roku 2011 tendencja z małymi odstępstwami uległa zmianie i po szczytowym roku 2013, w którym wydano 1 126 460 nowych certyfikatów, coraz mniej organizacji decyduje się na poddanie audytowi certyfikującemu, choć w ostatnich latach można zaobserwować wzrost.

Sukcesywny wzrost liczby wydawanych certyfikatów po 2000 roku wynikał z aktywności różnych organizacji w Azji, zwłaszcza w Chinach. Przedsiębiorstwa te chciały uwiarygodnić się w oczach partnerów przede wszystkim z Europy i Ameryki Północnej. Posiadanie certyfikatu stanowi bowiem często warunek konieczny nawiązania współpracy. Dodatkowo część podmiotów, które wcześniej wdrożyły system, utrzymują jego wymagania nie poddając się recertyfikacji. Sytuacja ta dotyczy także podmiotów leczniczych, które często traktują system ISO 9001:2015 jako pewien etap poprzedzający wdrożenie dużo bardziej wymagającego Programu Akredytacji Szpitali jak i Podstawowej Opieki Zdrowotnej.



Źródło: PThe ISO Survey of Certifications 2009–2019.

Wykres 2.2. Kraje, w których wydano najwięcej certyfikatów ISO 9001:2015 w 2018 roku



Źródło: The ISO Survey of Certifications 2019.

Ewolucja normy ISO 9001 powoduje, że od dawna przestała być kojarzona z firmami produkcyjnymi, a coraz częściej z podmiotami usługowymi.

się do aspektów kosztów i korzyści w zakresie wdrażania systemu. Do niewątpliwych korzyści można zaliczyć:

- usprawnienie organizacji pracy (np. opisy stanowisk pracy),
- usprawnienie przepływu informacji (np. regularne odprawy, Intranet),
- obniżenie kosztów (np. prowadzenie analiz w zakresie poziomu reoperacji, średnich czasów hospitalizacji czy błędów przed laboratoryjnych),
- kontrola dostawców (tworzenie list kwalifikowanych dostawców i ich ocena),
- zmniejszenie liczby usterek aparatury (rejestr urządzeń, rejestr usterek, paszporty urządzeń),
- zabezpieczenie się na wypadek roszczeń pacjentów (opracowanie standardów postępowania lekarskich, pielęgniarskich diagnostyki obrazowej itp.),
- skuteczniejszy nadzór nad dokumentacją medyczną (kompletność, czytelność, autoryzacja),
- budowanie wizerunku podmiotu dbającego o jakość,
- możliwość skuteczniejszego aplikowania o środki unijne (w przypadku niektórych wniosków za posiadanie certyfikatu można otrzymać dodatkowe punkty).

Wdrożenie systemu jest jednak wymagające. Do najczęstszych potencjalnych problemów, które pojawiają się w podmiotach leczniczych, należą:

- brak zaangażowania ze strony pracowników – w zakresie wdrażania systemów grupą zawodową, która jest najbardziej przeciwna wprowadzeniu zmian, są lekarze. Wynika to nie tyle z niechęci konsultacji dokumentacji, ile z braku czasu oraz małym stopniem utożsamiania się z organizacją, zwłaszcza u pracowników kontraktowych. Istotnym staje się promowanie konieczności rozwoju firmy oraz podkreślanie na szkoleniach i spotkaniach istoty zmian, determinowanych wpływem turbulentnego otoczenia;
- analiza kosztowa zakresu prowadzonych prac – koszty, które kierownicy zakładów powinni brać pod uwagę, związane są z: przygotowaniem dokumentacji systemowej przez firmę consultingową lub weryfikacją poprawności przygotowania dokumentacji z konsultantami, audytami systemów zarządzania jakością, przeprowadzeniem szkoleń, przygotowaniem dokumentacji, kosztami związanymi z certyfikacją;
- brak motywacji do działania na rzecz doskonalenia organizacji – system finansowania świadczeń zdrowotnych nie zachęca do podejmowania wysiłku na rzecz jakości; deficyty kadrowe, problemy infrastrukturalne czy aktualnie pojawiające się problemy epidemiczne (stan pandemii) powodują, że menadżerowie odkładają moment wdrożenia systemów na okres lepszej koniunktury itd.;
- to dotyczyć nie tylko osoby zarządzającej, ale także pełnomocników do spraw zapewnienia jakości;
- zbyt małe zaangażowanie kadry kierowniczej w prowadzone prace wdrożeniowe – powoduje to często opóźnienie lub też nawet w niektórych sytuacjach zatrzymanie procesu wdrożeniowego;
- brak wykształcenia kierunkowego osób koordynujących pracami wdrożeniowymi – mimo że znowelizowana w 2015 norma ISO 9001 nie wymaga od organizacji powoływania pełnomocnika do spraw zapewnienia jakości, to jednak taka osoba jest chętnie poszukiwana w zakładzie. Częstym problemem jest brak kształcenia w kierunku zarządzania podmiotami leczniczymi. Wprawdzie nie musi to być kierunek ekonomiczny, ale studia podyplomowe wskazywałyby pełnomocnikom możliwości szukania rozwiązań dla pojawiających się problemów w organizacji;
- zbyt mała wiedza na temat procesu wdrażania systemu – proces kojarzony jest często z wdrażaniem kolejnej dokumentacji, która nie rozwiąże problemów wewnętrznych, a wręcz spowoduje większą biurokrację w zakresie odbywających się procesów – procesy związane z obsługą pacjenta, procesy kadrowe, związane z rozliczaniem i dokumentowaniem realizowanych świadczeń;
- niechęć pracowników do wprowadzania zmian – takie zachowanie jest typowe w sytuacji niestabilnego otoczenia. Przy braku pewności dotyczących warunków zatrudnienia, wysokości kontraktowania świadczeń, stabilności w zakresie zatrudnienia kadry zarządzającej, personel jest sceptyczny do wprowadzania nowych rozwiązań.

Uniwersalizm normy, która często jest traktowana jako niepasująca do sfery usług medycznych. Często pojawiająca się obawa doprowadziła do opublikowania w 2017 roku normy EN-PN 15224:2017-02. Norma ta stanowi pewnego rodzaju tłumaczenie wymagań normy ISO 9001:2015 w zakresie działalności podmiotów leczniczych takich jak np. szpitale, podstawowa opieka zdrowotna, hospicja, ambulatoryjna opieka specjalistyczna, zakłady opiekuńczo-lecznicze. Dostosowała ona ogólne wymagania normy ISO 9001:2015 do warunków działalności placówek świadczących usługi medyczne. W normie tej uwypuklono takie obszary, jak: doskonalenie procesów klinicznych, zarządzanie ryzykiem w związku z udzielaniem świadczeń zdrowotnych, bezpieczeństwo pacjentów, zarządzaniem wiedzą i proces komunikacji. W normie EN-PN 15224:2017-02 uwzględniono zasady bezpośrednio odnoszące się do działalności podmiotów leczniczych (Lewandowski, Kożuch, Sasak 2018, s. 178):

wykorzystaniu aktualnej wiedzy medycznej;

- dostępność – pacjent powinien uzyskiwać dostęp do świadczeń medycznych adekwatnych na każdym etapie leczenia oraz w akceptowalnym przez niego czasie;
- ciągłość opieki – cała organizacja medyczna winna zapewnić ciągłość leczenia w zakresie diagnostyki, leczenia i innych niezbędnych działań;
- skuteczność – opieka nad pacjentem powinna być tak zorganizowana, aby przynosiła poprawę stanu zdrowia lub spowolnienie procesu choroby;
- efektywność – najlepsze wyniki leczenia powinny być osiągnięte przy optymalnym wykorzystaniu posiadanych zasobów, takich jak np. leki, aparatura medyczna, zasoby ludzkie;
- sprawiedliwość – opieka medyczna powinna być sprawowana adekwatnie do stanu pacjenta bez względu na jego status socjoekonomiczny, płeć, rasę, pochodzenie;
- opieka oparta na dowodach naukowych/wiedzy – stanowi rozwinięcie zasady dokładnej opieki, gdzie opieka powinna być sprawowana na podstawie rzetelnych badań naukowych i aktualnie dostępnej wiedzy;
- opieka skoncentrowana na pacjencie – opieka powinna uwzględniać integralność fizyczną, psychologiczną i społeczną pacjenta. Sprawowana opieka powinna zakładać holistyczne podejście do niego oraz zapewniać intymność i poszanowanie jego godności;
- zaangażowanie pacjentów – poprzez sprawną komunikację, należy zapewnić pacjentowi możliwość podejmowania decyzji dotyczących jego zdrowia oraz wyboru możliwości leczenia poprzez przekazanie rzetelnej wiedzy na temat zdrowia;
- bezpieczeństwo pacjentów – wymaga uwzględnienia wszelkich ryzyk, jakie mogą wystąpić w trakcie sprawowania opieki.

Należy jednak zauważyć, że norma EN-PN 15224:2017-02 pomimo uwzględnienia specyfiki działalności podmiotów leczniczych nie spotkała się z dużym zainteresowaniem wśród osób zarządzających podmiotami leczniczymi. Można przypuszczać, że wynikało to z faktu stosunkowo dużej popularności normy ISO 9001 w zakładach udzielających świadczeń zdrowotnych. Wdrożone wcześniej i utrzymywane przez lata systemy zarządzania jakością były doskonalone z uwzględnieniem wielu wymagań typowych dla usług medycznych. Decydenci uznali zatem, że wartość dodana wynikająca z wdrożenia wymagań kolejnej normy może być relatywnie niska.

z ISO 14001:2015 i wytyczne jego stosowania

Przyczyny przyjęcia systemowego podejścia do zarządzania środowiskowego zostały nakreślone w normie ISO 14001:2015. Wskazuje ona wyraźnie, iż oczekiwania społeczne dotyczące zrównoważonego rozwoju, transparentności oraz odpowiedzialności ewoluowały wraz ze zwiększającymi się restrykcjami wymagań prawnych, wzrastającymi zagrożeniami zanieczyszczenia środowiska, nieefektywnym użyciem zasobów, niewłaściwym zarządzaniem odpadami, zmianami klimatu, degradacją ekosystemów i zanikiem bioróżnorodności. Dlatego też celem normy międzynarodowej jest dostarczenie organizacjom konstrukcji, która zabezpieczy środowisko i będzie odpowiedzią na zmieniające się warunki środowiskowe przy zapewnieniu równowagi z potrzebami społecznymi i ekonomicznymi. Podaje ona wymagania, umożliwiające organizacji osiąganie wyników, które zakłada dla systemu zarządzania środowiskowego (PN-EN 14001:2015 pkt 01).

System zarządzania środowiskowego to element całego systemu zarządzania organizacją, w tym zarządzania podmiotem leczniczym. System ten należy uznać za dopełnienie systemu zarządzania jakością. O ile jednak system zarządzania jakością dotyczy zasadniczego obszaru działalności podmiotu leczniczego, jakim jest udzielanie świadczeń medycznych, o tyle zarządzaniem środowiskiem określa się zarządzanie tymi obszarami, które mogą mieć wpływ na środowisko naturalne. Według normy ISO 14000:2015 przez pojęcie „system zarządzania środowiskowego" należy rozumieć część ogólnego systemu zarządzania, obejmującą strukturę organizacyjną, planowanie, odpowiedzialność, zasady postępowania, procedury, procesy i środki potrzebne do opracowywania, wdrażania, realizowania, przeglądu i utrzymania polityki środowiskowej. Zarządzanie aspektami środowiskowymi odnosi się do wypełnienia zobowiązań dotyczących zgodności z wymaganiami oraz uwzględniania zagrożeń i możliwości. Zgodnie z pkt 3.2.1. normy 14000:2015 środowisko to termin odnoszący się do otoczenia, w którym działa organizacja, włącznie z powietrzem, wodą, ziemią, zasobami naturalnymi, florą, fauną, ludźmi i ich wzajemnymi zależnościami[28].

[28] Norma ISO 14001:2015 precyzuje także terminy: „aspekt środowiskowy" (pkt 3.2.2.) to element działań organizacji lub jej wyrobów lub usług, który ma lub może mieć wpływ na środowisko; warunki środowiskowe (pkt 3.2.3) to stan lub cechy środowiska określone w określonym momencie; oddziaływanie na środowisko (pkt 3.2.4.) to zmiana w środowisku zarówno korzystna, jak i niekorzystna, która w całości lub częściowo wynika z aspektów środowiskowych organizacji.

ści organizacji systemu zarządzania środowiskowego, można zaliczyć:

- chęć budowania wizerunku placówki, która troszczy się o stan środowiska naturalnego, co może pozytywnie wpływać na pozycję na rynku i relacje ze społecznością lokalną;
- rosnące znaczenie zagadnień dotyczących ochrony środowiska spowodowane wysoką świadomością dyrektorów, klientów i pracowników;
- wprowadzanie bodźców finansowych i prawnych, które stymulują organizacje do zmniejszania negatywnego oddziaływania na środowisko naturalne.

W odpowiedzi na tak zarysowujące się zmiany w zakresie ochrony środowiska Międzynarodowa Organizacja Normalizacyjna powołała w 1991 roku Strategiczną Grupę Doradczą ds. Środowiska (SAGE – Strategic Advisory Group of the Environment) w celu uzgodnienia projektu światowych standardów organizacyjnych w zakresie zarządzania środowiskowego – ISO 14000. W 1992 roku wydana została norma brytyjska dotycząca zarządzania ekologicznego BS 7750. Rok później Komisja Wspólnot Europejskich opublikowała zarządzenie nr 1836/93 związane z zarządzaniem ekologicznym Eco-Management and Audyt Scheme (EMAS), które obowiązuje w krajach będących członkami Unii Europejskiej (Urbaniak 2004, s. 230).

Norma ISO 14001 podobnie jak inne normy podlega procesowi nowelizacji. Pierwsze wydanie zostało opublikowane w roku 1996 (ISO 14001:1996 System zarządzania środowiskowego. Specyfikacje i wytyczne stosowania). Kolejne miało miejsce w roku 2004 (ISO 14001:2004 System zarządzania środowiskowego – Wymagania i wytyczne stosowania). Ostatnia nowelizacja nosząca status dużej nowelizacji została przeprowadzona w 2015 roku. W jej wyniku weszła w życie norma ISO 14001:2015 (ISO 14001:2015 – System zarządzania środowiskowego – Wymagania i wytyczne stosowania).

2.4.1. Wymagania normy ISO 14001:2015

Zasadniczym celem wdrożenia systemu zarządzania środowiskowego jest stworzenie warunków dla takiego funkcjonowania podmiotu leczniczego, by mógł w sposób świadomy i uporządkowany zmniejszać negatywny wpływ na środowisko w którym działa.

Wytyczne zawarte w normie ISO 14001:2015 nie określają dopuszczalnego poziomu wytwarzanych zanieczyszczeń, takich jak np. ścieki, gazy czy odpady. Organizacja taka jak podmiot leczniczy wyznacza je sama.

torowania i przestrzegania obowiązujących na terenie danego kraju aktów prawnych, można przyjąć, że nadrzędnym motywem wprowadzenia systemu zarządzania środowiskiem jest chęć zabezpieczenia organizacji przed wystąpieniem uchybień w świetle obowiązujących przepisów.

Norma ISO 14001:2015 w sposób stosunkowo elastyczny umożliwia dostosowanie zakresu działań do zawartych w niej wymagań. Wynika to z charakteru prowadzonej działalności i warunków, w jakich jest realizowana (tzw. kontekst organizacji). Treści zawarte w normie zawierają wymagania, jakie system powinien spełnić, aby zagwarantować kontrolowany przebieg procesów istotnych ze względu na wystąpienie aspektów środowiskowych.

Struktura normy obejmuje dziesięć rozdziałów, odwołuje się do procesu ciągłego doskonalenia i oparta jest na cyklu PDCA. Takie podejście ma zagwarantować, że działania na rzecz ochrony środowiska nie są podejmowane epizodycznie, ale mają charakter systematyczny i kontrolowany. Powyższe założenie ilustrują treści zawarte w tabeli 2.7.

Tabela 2.7. Proces ciągłego doskonalenia w normie ISO 14001:2015

1. Zakres normy		
2. Powołanie normatywne		
3. Terminy i definicje		
4. Kontekst organizacji	Wymagania dotyczące systemu zarządzania środowiskowego, podejścia procesowego do zarządzania, określenia kontekstu organizacji (w tym wymagań prawnych oraz wszystkich innych stron zainteresowanych w tym organizacji ekologicznych)	PLAN
4.1. Zrozumienie organizacji i jej kontekstu		
4.2. Zrozumienie potrzeb i oczekiwań stron zainteresowanych		
4.3. Określenie zakresu systemu zarządzania środowiskowego		
4.4. System zarządzania środowiskowego		
5. Przywództwo	Wymagania w stosunku do kierownictwa przedsiębiorstwa; zaangażowanie kierownictwa, niezbędne do utrzymywania systemu zarządzania środowiskowego oraz uzyskiwania zaplanowanych rezultatów	
5.1. Przywództwo i zaangażowanie		
5.2. Polityka środowiskowa		
5.3. Role uprawnienia i odpowiedzialność w organizacji		

	środowiskowych, a także problemów i niepewności mogących przeszkodzić w ich osiągnięciu	PLAN
6.1. Działania odnoszące się do ryzyk i szans		
6.2. Cele środowiskowe i planowanie ich osiągnięcia		
7. Wsparcie	Wymagania dotyczące bieżącej realizacji procesów, zarówno w warunkach normalnych, jak i w wypadku wystąpienia awarii	DO
7.1. Zasoby		
7.2. Kompetencje		
7.3. Świadomość		
7.4. Komunikacja		
7.5. Udokumentowane informacje		
8. Działania operacyjne		
8.1. Sterowanie operacyjne		
8.2. Reagowanie na awarie		
9. Ocena efektów działania	Wymagania dotyczące prowadzenia pomiarów, analiz oraz działań doskonalących, dotyczących wyrobów, klientów, skuteczności i efektywności systemu zarządzania środowiskiem	CHECK
9.1. Monitorowanie, pomiary, analiza i oceny		
9.2. Audyt wewnętrzny		
9.3. Przegląd zarządzania		
10. Doskonalenie	Wymagania dotyczące doskonalenia systemu oraz prowadzenia działań naprawczych i korygujących dla zaistniałych niezgodności	ACT
10.1. Postanowienia ogólne		
10.2. Niezgodności i działania korygujące		
10.3. Ciągłe doskonalenie		

Źródło: opracowanie własne na podstawie PN-EN ISO 14001:2015-09.

Wdrożenie systemu zarządzania środowiskowego jest działaniem złożonym. Także w przypadku tej normy obejmuje swoim zakresem trzy etapy.

W ramach tego etapu należy podjąć decyzję, czy system będzie wdrażany przy wykorzystaniu doświadczenia konsultantów zewnętrznych, czy przez pracowników podmiotu. Dodatkowo konieczne jest powołanie zespołu osób, które będą odpowiedzialne za wykonanie i nadzorowanie poprawności przygotowanej dokumentacji. Koniecznym jest także przeprowadzenie wstępnego przeglądu środowiskowego.

Etap 2 – Opracowanie

Punktem wyjścia dla wdrożenia systemu powinny być szkolenia dla pracowników. Dzięki temu rośnie świadomość wśród kadry i możliwe jest przeprowadzenie efektywnej analizy oddziaływania organizacji na środowisko. Na tym etapie opracowywane są procedury operacyjne, polityka środowiskowa i program środowiskowy.

Etap 3 – Testowanie

Na tym etapie wdrażane są działania korygujące, których zadaniem jest weryfikacja zgodności stanu faktycznego z wymaganiami wynikającymi z normy ISO 14001:2015 oraz przeprowadzony jest przegląd zarządzania z uwzględnieniem roli najwyższego kierownictwa.

Podejmowane działania obejmują (Hamrol 2017, s. 243–244):

1. Zadeklarowanie i wdrożenie polityki środowiskowej.
2. Opracowanie planu realizacji polityki środowiskowej, uwzględniającego:
   - identyfikację aspektów środowiskowych, które mogą oddziaływać na środowisko oraz sposobów (dróg), w których to oddziaływanie się ujawnia,
   - identyfikację wymogów prawnych dotyczących środowiska,
   - cele środowiskowe dotyczące zidentyfikowanych aspektów, program i zadania prowadzące do ich osiągania.
3. Pomiar, monitorowanie i ocena prowadzonych działań środowiskowych.
4. Doskonalenie systemu zarządzania środowiskowego przez prowadzenie przeglądów, szacowanie ryzyk i wdrożenie działań korygujących.

Wdrażając normę ISO 14001:2015, jednym z pierwszych działań, jakie należy podjąć, jest opracowanie polityki środowiskowej. Polityka ta powinna zawierać treści potwierdzające, że:

- jest odpowiednia do charakteru, skali oraz wpływu działań organizacji, produktów lub usług na środowisko,

bieganie zanieczyszczeniom,
- zawiera zobowiązanie do spełnienia odpowiednich wymagań wynikających z przepisów prawa dotyczących środowiska,
- jest udokumentowana, wdrożona i utrzymywana oraz zakomunikowana wszystkim zatrudnionym,
- jest publicznie dostępna.

Dodatkowo w Polityce Środowiskowej formułowane są nadrzędne cele, które następnie są operacjonalizowane na poziomie poszczególnych komórek organizacyjnych. W przypadku podmiotu leczniczego cele zawarte w polityce środowiskowej mogą być sformułowane w następujący sposób:
- prowadzenie działań zgodnie z obowiązującymi przepisami i wymaganiami prawnymi dotyczącymi ochrony środowiska;
- angażowanie personelu w działania na rzecz ograniczenia negatywnego oddziaływania na środowisko w wyniku świadczonych usług;
- prawidłowe gospodarowanie wodą i ściekami;
- efektywne zużycie nośników energii cieplnej i elektrycznej;
- prawidłowe postępowanie z wytworzonymi odpadami;
- zmniejszenie ryzyka wystąpienia awarii środowiskowych.

W praktyce realizacja tak wyznaczonych celów wymaga nie tylko szkolenia pracowników, ale także ponoszenia nakładów na np. termomodernizację, wymianę źródeł światła na energooszczędne czy też eliminowanie cieknących kranów i toalet.

Kolejnym istotnym obszarem aktywności podejmowanej w ramach wdrożonego systemu ISO 14001:2015 jest identyfikowanie aspektów środowiskowych (rysunek 2.6). Pod pojęciem aspektów środowiskowych rozumie się działania organizacji oraz jej wyrobów i usług, które mogą oddziaływać ze środowiskiem (ISO 14001). Najczęściej spotykanymi aspektami środowiskowymi mogą być: pobór energii i wody, wytwarzanie odpadów czy emisje gazów i pyłów do powietrza. Przy ich określaniu można posłużyć się m.in. wskazaniem parametrów wejściowych i wyjściowych z procesów zarządczych, podstawowych (np. rejestracja w izbie przyjęć w trybie planowym i nagłym, hospitalizacja na oddziałach zabiegowych i zachowawczych) i pomocniczych (np. zakup sprzętu i leków, zarządzanie kadrami, serwis urządzeń, dezynfekcja sal, utrzymanie higieny, utylizacja leków, odpady medyczne).

WEJŚCIE	PROCESY	WYJŚCIA	SKUTKI DLA ŚRODOWISKA
• Surowce/materiały • Opakowania i materiały opakowaniowe • Energia elektryczna • Gaz ziemny • Woda • Środki czystości • Narzędzia i urządzenia • Materiały konserwacyjne • Odczynniki chemiczne • Paliwo do środków transportu • Materiały biurowe	• podstawowe (wytwórcze) • pomocnicze	Hałas	Szkoda na ludzkim zdrowiu
			Niszczenie fauny
		Emisja gazów oraz pozostałe emisje niezorganizowane	Zanieczyszczenie powietrza
			Ubytek ozonu
			Zakwaszenie wód i gleb
			Szkoda na ludzkim zdrowiu
		Opady	Zanieczyszczenie powietrza, wody i gleby
			Niszczenie flory i fauny
			Szkoda na ludzkim zdrowiu
		Ścieki	Zanieczyszczenie wody
			Zatrucia wody
			Niszczenie flory i fauny
			Bioakumulacja
		Zanieczyszczenie gleb	Zanieczyszczenie gleby
			Zanieczyszczenie wód gruntowych
			Niszczenie fauny i flory
		Pożar/wybuch	Zanieczyszczenie środowiska
			Skażenie środowiska
			Szkoda na ludzkim zdrowiu

Źródło: Hamrol 2017, s. 244.

2.4.2. Korzyści i bariery wdrażania normy ISO 1400:2015 do podmiotów leczniczych

W trakcie wdrażania i późniejszego utrzymania systemu zarządzania środowiskowego należy skoncentrować się na tzw. istotnych aspektach środowiskowych. Do takich zalicza się te, które:
- generują ryzyko ponoszenia wysokich kosztów,
- mogą stanowić źródło znaczących konsekwencji prawnych,

- w znacznym stopniu wpływają na zanieczyszczenie środowiska naturalnego.

Weryfikacja powyższych zagadnień ma odzwierciedlenie w korzyściach, które można odnotować po wdrożeniu wymagań normy 14001:2015. Są nimi:

- Zidentyfikowanie aspektów środowiskowych przy uwzględnieniu takich kryteriów, jak: obowiązujące akty prawne, zasięg oddziaływania, prawdopodobieństwo wystąpienia oraz skutek wystąpienia (niewielkie, średnie, znaczne). W praktyce przygotowane są zestawienia tabelaryczne, które pozwalają te parametry szacować.
- Redukcja kosztów oraz oszczędności energii – wdrożenie w podmiocie leczniczym wymagań normy ISO 14001:2015 pozwala dyrektorom w znacznym stopniom obniżyć koszty zużycia wody i energii elektrycznej. Dodatkowo za sprawą przeprowadzonej termomodernizacji istnieje możliwość obniżenia kosztów ogrzewania budynków.
- Optymalizowanie wytwarzania odpadów.
- Budowanie wizerunku organizacji zorientowanej na ochronę środowiska. Dowodem rosnącej świadomości środowiskowej wśród społeczeństwa, w tym osób zarządzających może być wzrost ilości przeprowadzonych certyfikacji ISO 14001:2015.
- Zwiększenie osiągnięć przedsiębiorstwa poprzez wzrost zaufania klientów oraz poprawę wyników środowiskowych przedsiębiorstwa.
- Zapewnienie zrównoważonego rozwoju podmiotu przy ciągle rosnących wymaganiach środowiskowych – zapewnienie zgodności z przepisami prawa z zakresu ochrony środowiska.

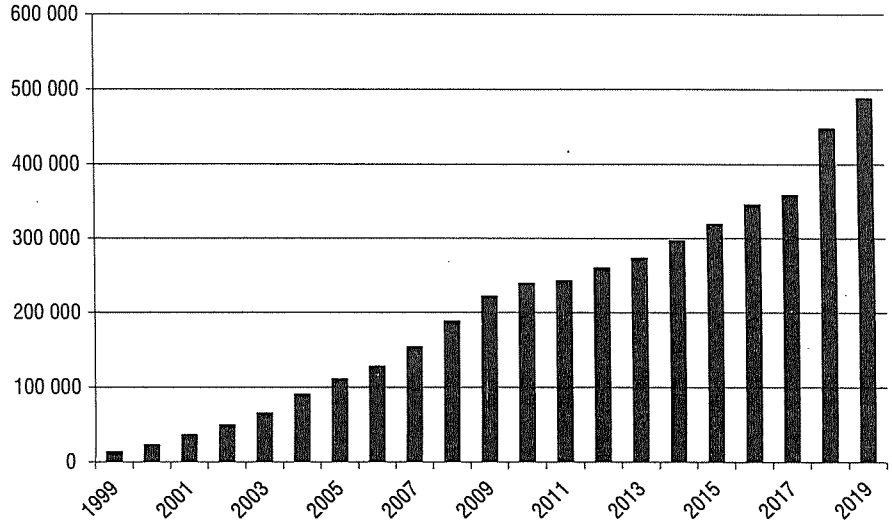
Tendencję wrażliwości na konsekwencje środowiskowe wynikające z prowadzonej działalności można zaobserwować dokonując analizy liczny wydanych certyfikatów (wykres 2.3).

Trudno jednak w ramach przedstawionej statystyki podać liczbę podmiotów leczniczych, które wdrożyły system ISO 14001:2015. Wynika to z:

1. Braku możliwości wygenerowania danych z dostępnej bazy rejestrowej. Poszukiwania informacji na temat systemów należy rozpocząć od Rejestru Podmiotów Wykonujących Działalność Leczniczą. Wprawdzie przy rekordzie danego zakładu informacja na temat wdrożonych systemów jest możliwa do odnalezienia, to jednak system nie pozwala na agregacje danych z konkretnego obszaru (województwo, kraj).

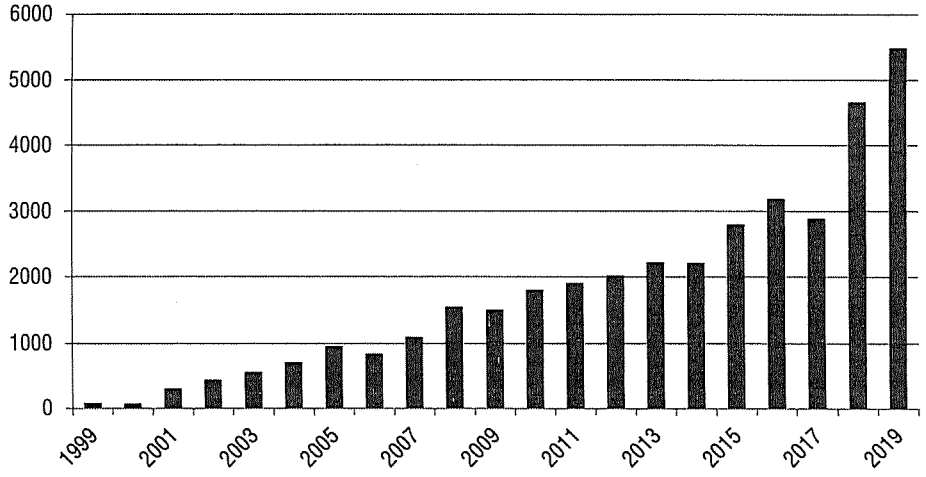
badań mogłaby zbierać dane rynkowe, pozyskując je z firm certyfikujących dotyczących wdrożenia.

Wykres 2.3. Liczba wydanych certyfikatów ISO 14001 na świecie



Źródło: https://www.kaiso.pl/statystyki-iso-2019 (dostęp: 17.12.2021).

Wykres 2.4. Liczba wydanych certyfikatów ISO 14001 w Polsce



Źródło: https://www.kaiso.pl/statystyki-iso-2019 (dostęp: 17.12.2021).

?func=ll&objId=18808772&objAction=browse&viewType=1) została przedstawiona liczba certyfikatów dla działu *Health and social work* – 120 certyfikatów. To w niej lokują się podmioty medyczne, co daje orientacyjny pogląd.

Przedstawiając aspekty wdrożeniowe, nie sposób pominąć trudności w zakresie wdrożenia systemu. Można tutaj wskazać:

- brak świadomości korzyści wdrożenia systemu;
- brak przygotowanych analiz oszczędności kosztowych po wdrożeniu systemu;
- zbyt małe zaangażowanie w procesy wdrożeniowe kadry kierowniczej;
- niechęć pracowników do wdrażania zmian – brak motywacji i wiedzy w zakresie dostosowania się do przygotowanych procesów;
- wzrost kosztów w zakresie utrzymania systemu – koszty przygotowania i utrzymania systemu, koszty usług firm doradczych, koszty certyfikacji;
- obowiązek stałego monitorowania i doskonalenia systemu – element, który powinien być korzyścią dla wdrażanych systemów, staje się dla części organizacji problematyczny. Przynajmniej trzy razy w roku przerywana jest praca w celu przygotowania się do audytów: audyt trzeciej strony, audyt wewnętrzny oraz przegląd zarządzania. Powoduje to nie tylko konieczność przeglądu dokumentacji. Bardzo często wiąże się z intensywną pracą nad usunięciem wszelkich niezgodności systemowych;
- przy wadliwie wdrożonym systemie można zaobserwować wzrost biurokracji w przedsiębiorstwie.

2.5. System zarządzania bezpieczeństwem informacji zgodnym z ISO 27001:2017

Jednym z najbardziej mobilizujących argumentów za wdrożeniem systemu zarządzania bezpieczeństwem informacji jest Rozporządzenie Ministra Zdrowia z dnia 5 sierpnia 2016 roku (Dz. U. z dnia 5 sierpnia 2016, poz. 1372 ze zm.) w sprawie szczegółowych kryteriów wyboru ofert w postępowaniu w sprawie zawarcia umów o udzielanie świadczeń opieki zdrowotnej.

udzielających świadczeń opieki zdrowotnej

Lp.	Przedmiot postępowania	Punktacja
1.	**Świadczenia nocnej i świątecznej opieki zdrowotnej na obszarze zabezpieczenia do 50 tys. świadczeniobiorców**	
	Certyfikat ISO 9001 systemu zarządzania jakością	2
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	2
2.	**Świadczenia nocnej i świątecznej opieki zdrowotnej na obszarze zabezpieczenia powyżej 50 tys. świadczeniobiorców**	
	Certyfikat ISO 9001 systemu zarządzania jakością	2
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	2
3.	**Ambulatoryjna Opieka Specjalistyczna (AOS)**	
	Certyfikat ISO 9001 systemu zarządzania jakością	1
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	1
4.	**Opieka psychiatryczna i leczenie uzależnień**	
	Certyfikat ISO 9001 systemu zarządzania jakością	0,5
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	0,5
5.	**Rehabilitacja lecznicza**	
	Certyfikat ISO 9001 systemu zarządzania jakością	1
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	1
6.	**Świadczenia pielęgnacyjne i opiekuńcze w ramach opieki długoterminowej**	
	Certyfikat ISO 9001 systemu zarządzania jakością	2
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	2
7.	**Zakład opiekuńczo-leczniczy dla świadczeniobiorców wentylowanych mechanicznie lub zakład pielęgnacyjno-opiekuńczy dla świadczeniobiorców wentylowanych mechaniczni**	
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	2
8.	**Zakład pielęgnacyjno-opiekuńczy dla dzieci i młodzieży lub zakład opiekuńczo-leczniczy dla dzieci i młodzieży**	
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	2

9.	**Zakład opiekuńczo-leczniczy dla dzieci i młodzieży wentylowanych mechanicznie lub zakład pielęgnacyjno-opiekuńczy dla dzieci i młodzieży wentylowanych mechanicznie**	
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	2
10.	**Leczenie szpitalne**	
	Certyfikat ISO 9001 systemu zarządzania jakością	1,5
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	0,5
11.	**Leczenie szpitalne – hospitalizacja planowa**	
	Certyfikat ISO 9001 systemu zarządzania jakością	1,5
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	0,5
12.	**Leczenie szpitalne – leczenie jednego dnia** • Alergologia/alergologia dla dzieci • Angiologia • Choroby płuc/choroby płuc dla dzieci • Choroby wewnętrzne • Dermatologia i wenerologia/dermatologia i wenerologia dla dzieci • Diabetologia/diabetologia dla dzieci • Endokrynologia/endokrynologia dla dzieci • Gastroenterologia/gastroenterologia dla dzieci • Geriatria • Neurologia/neurologia dla dzieci • Pediatria • Reumatologia/reumatologia dla dzieci	
	Certyfikat ISO 9001 systemu zarządzania jakością	1,5
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	0,5
13.	**Ratownictwo medyczne**	
	Certyfikat ISO 9001 systemu zarządzania jakością	3
14.	**Leczenie stomatologiczne**	
	Certyfikat ISO 9001 systemu zarządzania jakością	1
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	1
15.	**Lecznictwo uzdrowiskowe**	
	Certyfikat ISO 9001 systemu zarządzania jakością	1
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	1
16.	**Świadczenia zdrowotne kontraktowane odrębnie**	
	Certyfikat ISO 9001 systemu zarządzania jakością	1
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	1
17.	**Opieka paliatywna i hospicyjna**	
	Certyfikat ISO 9001 systemu zarządzania jakością	1
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	1
18.	**Poradnia medycyny paliatywnej**	
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	1
19.	**Leczenie szpitalne – świadczenia wysoko specjalistyczne**	
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	0,5
20.	**Programy zdrowotne**	
	Certyfikat ISO 9001 systemu zarządzania jakością	2
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	2
21.	**Leczenie szpitalne – programy lekowe**	
	Certyfikat ISO 9001 systemu zarządzania jakością	1
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	1
22.	**Leczenie szpitalne – chemioterapia**	
	Certyfikat ISO 9001 systemu zarządzania jakością	1
	Certyfikat ISO 27001 systemu zarządzania bezpieczeństwem informacji	1
23.	**Pomoc doraźna i transport sanitarny**	
	Certyfikat ISO 9001 systemu zarządzania jakością	10

Źródło: opracowanie własne na podstawie DZ.U. 2016, poz. 1372.

Wzrost skali gromadzenia danych oraz rozwój technologii informatycznych zwiększa się także ryzyko wystąpienia cyberzagrożeń. Potwierdzeniem skali zagrożeń mogą być kolejne raporty o stanie bezpieczeństwa cyberprzestrzeni RP. Zdaniem ekspertów z Rządowego Zespołu Reagowania na Incydenty Komputerowe rośnie liczba incydentów związanych z cyberzagrożeniami, które stają się coraz bardziej niebezpieczne. Znaczną grupę stanowią ataki wykonywane przez tzw. botnety – sieci komputerowe zawirusowane przez złośliwe oprogramowanie. Zadaniem botnetów jest wykonywanie poleceń cyberprzestępców. Z publikowanych raportów działającego przy ABW Zespołu Reagowania na Incydenty

ataków, z czego większość stanowiły ataki wykonane przez botnety, o tyle w 2019 roku miało miejsce 12405 incydentów cybernetycznych[29].

Konsekwencją tego typu incydentów jest nie tylko zakłócenie funkcjonowania instytucji spowodowany zablokowaniem dostępu do danych, ale także zagrożenie dla zdrowia i życia obywateli w przypadku instytucji wchodzących w skład tzw. infrastruktury krytycznej, do której należy zaliczyć podmioty lecznicze. Tym samym należałoby przyjąć, że zagwarantowanie bezpieczeństwa informacji powinno być uwzględniane wśród celów o charakterze strategicznym w każdej organizacji, a zwłaszcza takiej, która dysponuje danymi o charakterze sensytywnym (stan zdrowia, przebyte choroby, preferencje polityczne, preferencje seksualne, karalność). Na przestrzeni ostatnich lat, zwłaszcza po wejściu w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO), świadomość dotycząca znaczenia informacji i konieczności ich ochrony wzrosła. Można jednak odnieść wrażenie, że świadomość skali zagrożeń jest niewystarczająca. O tym, jak ważna jest ochrona informacji przed szkodliwym oprogramowaniem, może świadczyć różnorodność zagrożeń (tabela 2.9).

Tabela 2.9. Rodzaje szkodliwego oprogramowania

Rodzaj oprogramowania	Definicja
Wirus	Program lub fragment szkodliwego kodu, który dołącza się, nadpisuje lub zamienia inny program w celu reprodukcji samego siebie bez zgody użytkownika.
Robak	Złośliwe oprogramowanie podobne do wirusów, rozmnażające się tylko przez sieć. W przeciwieństwie do wirusów nie potrzebują programu „żywiciela". Często powielają się pocztą elektroniczną.
Trojan	Nie rozmnaża się jak wirus, ale jego działanie jest równie szkodliwe. Ukrywa się pod nazwą lub w części pliku, który użytkownikowi wydaje się pomocny. Oprócz właściwego działania pliku zgodnego z jego nazwą, trojan wykonuje w tle operacje szkodliwe dla użytkownika, np. pozwala dokonać ataku włamywacza (hakera).
Programy szpiegujące	Oprogramowanie zbierające informacje o osobie fizycznej lub prawnej bez jej zgody (np. informacje o odwiedzanych witrynach, hasła dostępowe itp.).
Exploit	Kod umożliwiający bezpośrednie włamanie do komputera użytkownika, dokonanie zmian lub przejęcie kontroli. Exploit wykorzystuje lukę w oprogramowaniu zainstalowanym na atakowanym komputerze.
Rootkit	Ogólna zasada działania opiera się na maskowaniu obecności pewnych uruchomionych programów lub procesów systemowych (zwykle służących hakerowi do administrowania zaatakowanym systemem). Rootkit zostaje wkompilowany w istotne procedury systemowe. Zwykle jest trudny do wykrycia z racji tego, że nie występuje jako osobna aplikacja.
Dialery	Programy łączące się z siecią przez inny numer dostępowy niż wybrany przez użytkownika. Dialery szkodzą posiadaczom modemów telefonicznych (analogowych i cyfrowych ISDN).

Źródło: Skolnik, Miciuła, Kubiński 2018, s. 33–34.

Wzrost skali cyberprzestępczości wymaga metodycznego podejścia do kwestii zapewnienia bezpieczeństwa informacji. Osoby zarządzające organizacjami, w tym podmiotami leczniczymi, powinny uznać informacje za zasób równie istotny jak pozostałe, którymi dysponuje, mianowicie zasobami kadrowymi, lokalowymi, finansowymi i sprzętowymi (Beskosty 2017, s. 163–164).

2.5.1. Wymagania i znaczenie normy ISO 27001:2017

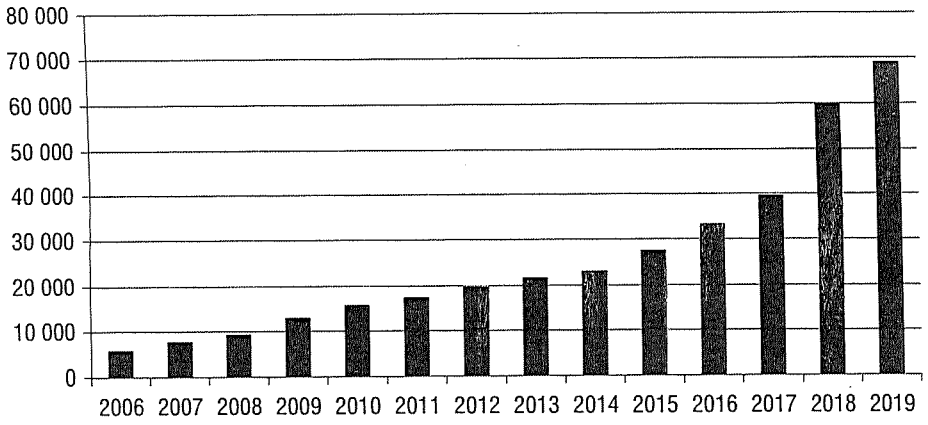
Norma ISO 27001 podlega jak inne normy procesowi nowelizacji. Obecnie obowiązująca norma PN-EN ISO 27001:2017-06 zastąpiła wcześniejszą PN-EN ISO 27001:2014-12. Normy te zostały opracowane na podstawie wypracowanych wcześniej zabezpieczeń w przemyśle. Za początek systemowego zabezpieczenia informacji można uznać opublikowany w 1992 roku przez Departament Handlu i Przemysłu Wielkiej Brytanii raport *A Code of Practice for Information Security Management*. Dokument ten po trzech latach został ujęty w ramy brytyjskiej normy BS 7799. Po czterech latach, w roku 1999 przeprowadzono pierwszą nowelizację tego standardu, a rok później w ramach tzw. szybkiej ścieżki opublikowano międzynarodową normę ISO/IEC 17799:2000

[29] https://www.avlab.pl/raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-rp-w-2018-roku (dostęp: 17.12.2021); https://www.wnp.pl/finanse/raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-w-2019-roku (dostęp: 17.12.2021).

czenia organizacji i systemów informatycznych ujęte w różnych obszarach zabezpieczeń. W 2001 roku British Standards Institution (BSI – nazwa krajowego organu normalizacyjnego Zjednoczonego Królestwa) wydał drugi arkusz normy BS 7799. W arkuszu tym określono konstrukcję systemu zarządzania bezpieczeństwem informacji, która była spójna m.in. z normą ISO 9001:2000. W ten sposób doprowadzono do opublikowania normy ISO/IEC 27001:2005.

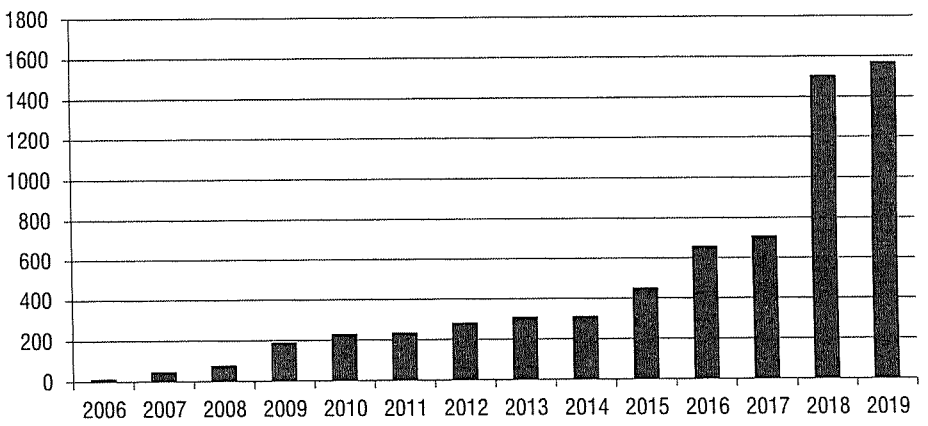
W Polsce, podobnie jak i na całym świecie, można zaobserwować wyraźny wzrost zainteresowania normą ISO 27001. Wynika to z tego, że menadżerowie zdają sobie sprawę z faktu, że model SZBI, stanowiąc zbiór dobrych praktyk, pozwala systemowo chronić informacje. Należy zauważyć, że liczba wydawanych na świecie certyfikatów ISO 27001 od roku 2006 sukcesywnie rośnie, przy czym duży wzrost dynamiki można zaobserwować od 2018 roku. Można przypuszczać, że jest to konsekwencją wejścia w życie 28.05.2018 wymagań wynikających z rozporządzenia o ochronie danych osobowych (wykres 2.5).

Wykres 2.5. Wydane na świecie certyfikaty ISO 27001



Źródło: The ISO Survey of Management System Standard Certifications za lata 2007 do 2019

Dla porównania w Polsce dynamika wydawanych certyfikatów wydaje się być wyższa niż na świecie. Dotyczy to zwłaszcza sytuacji z 2018 roku, kiedy liczba ta uległa podwojeniu w porównaniu do sytuacji z 2017 roku (por. wykres 2.6).



Źródło: The ISO Survey of Management System Standard Certifications za lata 2007–2019.

Warto zauważyć, że certyfikacja tego systemu nie jest obligatoryjna i część organizacji może wdrożyć wymagania wynikające z normy, niepoddając się zewnętrznej ocenie. Ważniejsze wydaje się systemowe podejście do ochrony informacji. W normie ISO 27001:2017 wskazano trzy aspekty dotyczące informacji, które muszą podlegać ochronie:

- poufność,
- integralność,
- dostępność.

Zagwarantowanie poufności oznacza zapewnienie dostępu do informacji wyłącznie osobom upoważnionym. Zachowanie integralności wiąże się z dokładnością oraz kompletnością informacji, także w trakcie jej przetwarzania. W praktyce oznacza to konieczność weryfikacji wiarygodności źródła informacji oraz kontrolę nad wprowadzonymi zmianami. Dostępność z kolei wymaga zagwarantowania upoważnionym osobom korzystanie z danych, gdy tego będą potrzebowały.

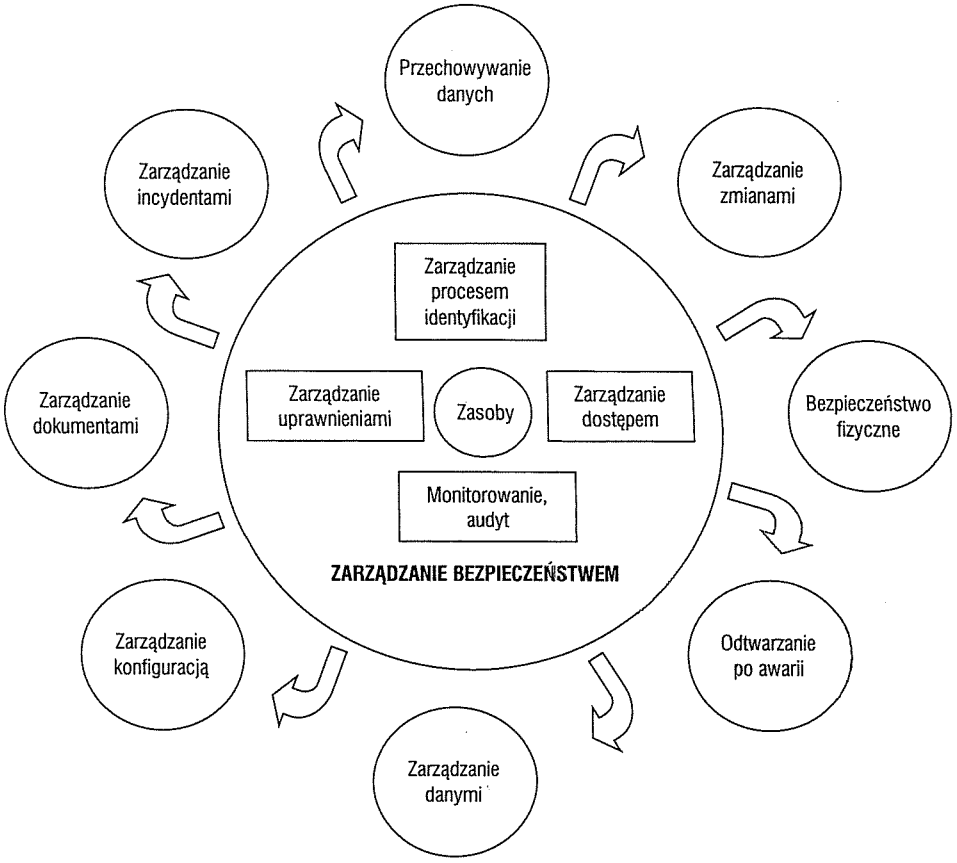
Bezpieczeństwo informacji, jak zauważa A. Hamrol (2017, s. 221–222), może być zagrożone ze względu na brak lub niejednoznaczność obowiązujących procedur bądź niedoskonałość człowieka. Źródła zagrożeń mogą tkwić w zarządzaniu, sprzęcie, oprogramowaniu i w samej informacji. Zagrożenia mogą zatem pochodzić (tamże):

- od człowieka, np. omyłkowe skasowanie pliku, włamanie do systemu, w tym kradzież danych (obserwacje wskazują że większość problemów dotyczących bezprawnego dostępu do informacji wiąże się z niewiedzą pracowników);

- od sprzętu (awaria, niewłaściwe skonfigurowanie).

Celem działań w zakresie eliminacji pojawiających się zagrożeń zarówno w przedsiębiorstwie, jak i podmiocie leczniczym jest osiągnięcie poziomu organizacyjnego oraz technicznego, który pozwoli wypracować mechanizmy ciągłego nadzoru z możliwością ich procesowego doskonalenia (rysunek 2.7).

Rysunek 2.7. Procesowe zapewnienie bezpieczeństwa informacji



Źródło: Olkiewicz 2016, s. 91.

Jak zauważa M. Wiśniewska (2009, s. 80), organizacje, które chcą w sposób skuteczny chronić swoje informacje, powinny zastosować podejście systemowe, polegające na holistycznym zarządzaniu własnymi zasobami informacyjnymi, pieczeństwem informacji. Tym samym wiele organizacji decyduje się na wdrożenie kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji.

Działania podejmowane w ramach systemu zarządzania bezpieczeństwem informacji powinny być ukierunkowane nie tyle na reagowanie na incydenty bezpieczeństwa informacji, ile na prewencję. Należy zatem zadbać o odpowiedni poziom świadomości w podmiocie leczniczym, który wydaje się wyjątkowo narażony na tego typu zagrożenia ze względu na dużą liczbę personelu pracującego pod presją czasu i niekiedy w silnym stresie. Dodatkowo, szczególnie w przypadku publicznych podmiotów, niebagatelny wpływ na możliwość wdrożenia rozwiązań mają ograniczenia finansowe wynikające z poziomu kontraktowania i znikomego niekiedy zaangażowania organów założycielskich. Wdrażając rozwiązania dotyczące ochrony danych, należy także mieć na uwadze fakt, że dotyczy to zarówno dokumentacji prowadzonej w formie papierowej, jak i elektronicznej.

Tabela 2.10. Wymagania normy ISO 27001:2015

1. Zakres normy	
2. Powołanie normatywne	
3. Terminy i definicje	
4. Kontekst organizacji	PLAN
4.1. Zrozumienie organizacji i jej kontekstu	
4.2. Zrozumienie potrzeb i oczekiwań stron zainteresowanych	
4.3. Określenie zakresu systemu zarządzania bezpieczeństwem informacji	
4.4. System zarządzania bezpieczeństwem informacji	
5. Przywództwo	
5.1. Przywództwo i zaangażowanie	
5.2. Polityka	
5.3. Role, odpowiedzialność i uprawnienia w organizacji	
6. Planowanie	
6.1. Działania odnoszące się do ryzyk i szans	
6.2. Cele ochrony informacji i planowanie ich osiągnięcia	

7.1. Zasoby	DO
7.2. Kompetencje	
7.3. Świadomość	
7.4. Komunikacja	
7.5. Udokumentowane informacje	
8. Działania operacyjne	
8.1. Planowanie i nadzór nad działaniami operacyjnymi	
8.2. Ocena ryzyka bezpieczeństwa informacji	
8.3. Szacowanie ryzyka bezpieczeństwa informacji	
9. Ocena efektów działania	CHECK
9.1. Monitorowanie, pomiary, analiza i oceny	
9.2. Audyt wewnętrzny	
9.3. Przegląd zarządzania	
10. Doskonalenie	ACT
10.1. Niezgodności i działania korygujące	
10.2. Ciągłe doskonalenie	

Źródło: opracowanie własne.

W podmiotach leczniczych zagadnieniami o największym ryzyku utraty informacji są rozwiązania dotyczące dostępu do pomieszczeń, dokumentacji i systemów informatycznych. W związku z powyższym można wyróżnić w podmiotach świadczących usługi medyczne następujące obszary bezpieczeństwa:

1. Bezpieczeństwo prawno-organizacyjne.
2. Bezpieczeństwo fizyczne.
3. Bezpieczeństwo teleinformatyczne.

Ad. 1. W odniesieniu do zagadnień dotyczących zasad postępowania z informacjami należy określić, jakie informacje są najbardziej wartościowe dla jednostki medycznej i kto odpowiada za określenie tej wartości. Koniecznym jest także opracowanie zasad przetwarzania informacji w kontekście ich oznaczenia, przechowywania, niszczenia, kopiowania i udostępniania na zewnątrz. W świetle tów bezpieczeństwa, które należy rozumieć jako niepożądane zdarzenie będące naruszeniem bezpieczeństwa informacji. Personel musi mieć świadomość, że incydenty mogą się zdarzyć w każdej organizacji, a ich zgłaszanie i analizowanie ma uchronić podmiot leczniczy przed podobnymi lub poważniejszymi sytuacjami w przyszłości. Zagwarantowanie bezpieczeństwa prawno-organizacyjnego wymaga także podpisania stosownych umów z dostawcami, w tym tak zwanych umów powierzenia. Jest to o tyle ważne, że przepisy RODO zakładają tzw. odpowiedzialność solidarną i w razie wycieku np. danych osobowych niezawinionego przez podmiot leczniczy mogą go narazić na poważne konsekwencje finansowe. W podmiocie leczniczym należy ponadto zadbać, aby personel korzystał wyłącznie z legalnego oprogramowania i nie instalował żadnego we własnym zakresie, także takiego, które można bezpłatnie pobrać z Internetu.

Ad. 2. Podnosząc kwestie dotyczące bezpieczeństwa fizycznego, kluczową kwestią wydaje się zagwarantowanie zabezpieczenia terenu, obiektu i pomieszczeń. Uzasadnionym wydaje się ogrodzenie terenu, zamontowanie elektronicznego systemu monitoringu, zamontowanie w pomieszczeniach, np. na parterze, folii antywłamaniowej, zapewnienie ochrony obiektu. Odrębną kwestią jest odpowiednie zorganizowanie recepcji lub stanowiska w izbie przyjęć. Konieczne wydaje się zapewnienie odpowiedniego dystansu pomiędzy osobą obsługiwaną a oczekującą w kolejce. Dodatkowo należy pamiętać, aby treści wyświetlane na ekranie monitora jak i wprowadzane do dokumentacji nie były widoczne dla osób do tego nieuprawnionych. W pomieszczeniach należy przestrzegać zasady tzw. czystego biurka (nie zostawiać dokumentów zawierających dane osobowe, kiedy osoba upoważniona nie ma nad nim kontroli). W pokojach muszą być szafy zamykane (na dokumenty), a dostęp do nich musi się wiązać formalnym nadaniem uprawnień (polityka kluczy). W przypadku osób odwiedzających, np. pacjentów, musi być prowadzony ich rejestr lub przynajmniej nadzór elektroniczny (monitoring). Uzasadnionym jest także wydzielenie strefy odwiedzin, która zagwarantuje, że osoby postronne nie będą widziały, kto oprócz ich bliskich jest w danej chwili hospitalizowany. Zagwarantowanie odpowiedniego poziomu bezpieczeństwa fizycznego wymaga także nadzorowania dostępu do archiwum, w przypadku którego należy prowadzić rejestr wejść, wyjść i pobrań. Dokumentacja w archiwum musi być uporządkowana, np. w opisanych segregatorach. W pomieszczeniach należy monitorować temperaturę i wilgotność.

Kolejnym aspektem związanym z tym obszarem bezpieczeństwa jest także nadzór nad pracą urządzeń (komputery, serwery itp.). W pierwszej kolejności należy uniemożliwić do nich dostęp osobom nieupoważnionym (polityka

uszkodzeniem (np. otwarte okno podczas burzy, sprzęt usytuowany w pobliżu klimatyzatora). W podmiocie leczniczym należy zabezpieczyć się na wypadek przerwy w dopływie energii elektrycznej poprzez zwielokrotnione linie, generator prądu oraz UPS. Pomieszczenie serwerowni powinno być klimatyzowane, żeby uchronić serwery przed przegrzaniem w upalne dni. Cała infrastruktura informatyczna musi ponadto być systematycznie serwisowana.

Ad. 3. Analizując zagadnienie dotyczące bezpieczeństwa teleinformatycznego należy zwrócić uwagę na prowadzenie polityki haseł. Zmiana haseł powinna być wymuszana przez administratora, przy czym nie ma potrzeby jej zbyt częstego zmieniania, ponieważ przyjęcie takiej zasady może skutkować ich osłabieniem (autorzy haseł ustalają jeden moduł hasła stały, a część zmieniając, np. wprowadzając liczbę stosowną do kolejnego miesiąca lub roku, np. stokrotka/01 w styczniu i stokrotka/03 w marcu). Z poziomu administratora systemu informatycznego powinna być określona liczba prób logowania (loginy nie mogą być współdzielone) oraz zagwarantowane oprogramowanie antywirusowe. Istotne są szkolenia personelu w zakresie bezpiecznego korzystania z zasobów Internetu oraz ewentualne odłączenie od niego tych komputerów, na dyskach których są zapisane szczególnie cenne informacje. W ramach tego typu zagrożeń trzeba także wprowadzić rozwiązania gwarantujące tworzenie z odpowiednią częstotliwością kopii bezpieczeństwa oraz określić zasady korzystania z nośników zewnętrznych, których stosowanie powinno być ograniczone lub sprowadzać się do korzystania tylko z takich, które są rejestrowane (każdy fakt kopiowania danych jest widoczny w systemie). Dodatkowo koniecznym jest spełnienie określonych zasad dotyczących niszczenia nośników danych i sposobu ich usuwania (zasada np. nadpisywania danych na dyskach komputerów).

W zarządzaniu podmiotem nie można bowiem oddzielić sfery bezpieczeństwa informacji od sfery zarządzania. Istotne stają się takie aspekty, jak (Oliewicz 2016, s. 94):

- stały monitoring jakości informacji (kontrolę, analizę i doskonalenie danych uzyskiwanych, przetwarzanych oraz przekazywanych);
- przejrzyste, skuteczne i zrozumiałe procedury postępowania zwiększające rolę jakości informacji (wzmocnienie znaczenia pracowników, akredytację bezpieczeństwa dostępności itd.);
- wzmocnienie czynnika jakości informacji w biznesowej sferze organizacji (monitorowanie i eliminowanie ryzyka, kreowanie odpowiedniej polityki IT oraz bezpieczeństwa informacji);
- rantujących właściwe postępowanie ukierunkowane na kształtowanie jakości informacji.

Warto podkreślić, iż także w normie ISO 27001:2017 wykorzystany jest opisany wcześniej model Deminga (PDCA), który powinien być stosowany do wszystkich elementów SZBI. Podejście procesowe zakłada, że wszystkimi obszarami należy tak zarządzać, aby przekształcać wejścia w wyjścia.

Podejście procesowe do zarządzania bezpieczeństwem informacji zapewnione w normie zwraca uwagę na identyfikację, interakcję i zarządzanie procesami, czyli[30]:

- zrozumienie wymagań bezpieczeństwa informacji w organizacji oraz określenie zasad i celów bezpieczeństwa informacji;
- wdrożenie i eksploatację zabezpieczeń w celu zarządzania ryzykiem bezpieczeństwa informacji w kontekście całkowitego ryzyka biznesowego organizacji;
- monitorowanie i przegląd wydajności oraz skuteczności SZBI;
- ciągłe doskonalenie na podstawie obiektywnego pomiaru.

Norma ISO 27001:2017 składa się z dwóch części.

Część zasadnicza zawiera wymagania, w których zwiększono nacisk na realne funkcjonowanie organizacji wdrażających system. Wyraża się to m.in. w powiązaniu planowania z oceną ryzyka (rozdział 6 normy) oraz wprowadzeniu kontekstu organizacji, co wymusza niejako na osobach zarządzających podmiotami leczniczymi prowadzenia analizy otoczenia z uwzględnieniem metod analizy strategicznej, tak w zakresie mikro-, jak i makrootoczenia.

W zakresie wymagań norma ISO 27001 kładzie szczególny nacisk na komunikację. Konieczne jest uwzględnienie rodzaju przekazywanych informacji, adresatów przekazu oraz osoby odpowiedzialnej za jej realizację. Istotnym wymaganiem jest również szacowanie ryzyka wystąpienia wycieku danych. Przykładowy arkusz został zaprezentowany w tabeli 2.11, w której identyfikuje się ryzyko w ramach realizowanych procesów, następnie wskazuje się jego skutki, określa prawdopodobieństwo wystąpienia i na końcu określa się w wyniku przeprowadzonej oceny, czy poziom ryzyka jest akceptowalny czy nie. W przypadku ryzyk nieakceptowalnych wskazanym jest zaproponowanie działań, które pozwolą obniżyć prawdopodobieństwo wystąpienia albo ewentualne skutki.

---

[30] Norma PN-ISO/IEC 27001:2017.

Lp.	Proces	Opis zagrożenia	Skutek wystąpienia zagrożenia (S) Skala 1–3	Prawdopodobieństwo wystąpienia zagrożenia (P) Skala 1–3	Ryzyko wystąpienia zagrożenia R=SxP	Poziom ryzyka	Uwagi
	Obsługa w Izbie Przyjęć	Wyciek danych	3	3	9	Poziom nieakceptowalny	Szkolenie z RODO

Źródło: opracowanie własne.

Dodatkowo w przypadku ryzyk określonych jako nieakceptowalne można zdecydować się na wprowadzenie kolejnych działań (tabela 2.12), które pozwolą dookreślić rekomendacje doskonalenia.

Tabela 2.12. Plan postępowania z ryzykiem nieakceptowalnym

Lp.	Kategoria ryzyka	Opis zagrożenia	Sugerowane działania korygujące	Osoba nadzorująca realizację	Termin realizacji	Wymagane koszty	Daty monitorowania realizacji	Analiza skuteczności działań

Źródło: opracowanie własne.

Bardzo istotną częścią normy ISO 27001:2017 jest załącznik A, w którym przedstawiono obszary w zakresie wymaganych zabezpieczeń.

Tabela 2.13. Cele stosowania zabezpieczeń i zabezpieczenia

Odniesienie do rozdziału	ISO 27001:2017
A5.	Polityki bezpieczeństwa informacji
A6.	Organizacja bezpieczeństwa informacji
A7.	Bezpieczeństwo zasobów ludzkich
A8.	Zarządzanie aktywami
A9.	Kontrola dostępu
A10.	Kryptografia
A11.	Bezpieczeństwo fizyczne i środowiskowe
A12.	Bezpieczna eksploatacja
A13.	Bezpieczeństwo komunikacji
A14.	Pozyskiwanie, rozwój i utrzymanie systemu
A15.	Relacje z dostawcami
A16.	Zarządzanie incydentami związanymi z bezpieczeństwem informacji
A17.	Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania
A18.	Zgodność

Źródło: opracowanie na podstawie normy PN-ISO/ICE 27001:2017.

Proces wdrażania systemu zarządzania bezpieczeństwem informacji zgodnego z PN-ISO/IEC 27001:2017 można podzielić na następujące etapy:

Etap 1 – Przygotowanie

Decydując się na wdrożenie wymagań normy należy w pierwszej kolejności określić zakres systemu. Oznacza to w praktyce podjęcie decyzji, czy wdrożenie powinno dotyczyć całego podmiotu, czy tylko wybranych działów zakładu. Najkorzystniejszym podejściem ze względu na skalę ewentualnych zagrożeń wydaje się podjęcie decyzji o wdrożeniu w całej organizacji. Proces wdrożenia jest złożony i obejmuje wiele etapów, które powinny zostać właściwie przeprowadzone, aby można było mówić o jego skutecznym wdrożeniu (Wiśniewska 2009, s. 82):

- audyt wstępny,
- klasyfikacja aktywów,
- opracowanie metody i przeprowadzenie analizy ryzyka,
- wdrożenie zabezpieczeń,
- opracowanie i wdrożenie dokumentacji SZBI,
- szkolenie dla pracowników,
- audyt wewnętrzny oraz przegląd SZBI.

Audyt wstępny może być przeprowadzony przez pracownika podmiotu leczniczego i przez konsultanta z firmy doradczej. Zaangażowanie osoby z zewnątrz wydaje się o tyle zasadne, że taka osoba, mając doświadczenie z innych organizacji, będzie potrafiła dostrzec problemy, których może nie zauważyć pracownik,

powinien obejmować wszystkie obszary bezpieczeństwa uwzględniane w wymaganiach normy ISO 27001:2017. Wynik takiego audytu ma duże znaczenie w ustaleniu zakresu prac, jakie będzie należało wykonać przygotowując podmiot do certyfikacji. W trakcie audytu należy uwzględnić szerokie spektrum źródeł informacji, takie jak analiza dokumentacji, rozmowy z pracownikami oraz obserwacje. Szczególnie istotne wydają się obserwacje i rozmowy, ponieważ dzięki temu możliwe będzie zweryfikowanie, jaki jest poziom świadomości personelu na temat znaczenia SZBI. Warto tym samym zaobserwować, czy pracownicy nie wprowadzają danych do systemu, korzystając z loginu współpracowników, czy przestrzegają zasady tzw. czystego biurka i czy zamykają pomieszczenia kiedy z nich wychodzą. Ponadto warto zwrócić uwagę, jak przebiega proces rejestracji na badania lub konsultacje. Istotnym źródłem informacji są oczywiście dokumenty, wśród których warto uwzględnić:

- raporty z wcześniej przeprowadzonych audytów (np. ISO 9001:2015 w obszarze punktu nadzór nad infrastrukturą);
- regulamin organizacyjny;
- zarządzenia dyrekcji w zakresie archiwizacji dokumentów i systemu informatycznego;
- dokumentację, w zakresie IT;
- dokumenty, dotyczące zasad postępowania z informacją w podmiocie (np. instrukcja kancelaryjna);
- instrukcje awaryjne (np. postępowanie na wypadek pożaru, przerwy w dopływie prądu itp.).

W trakcie audytu można także zweryfikować poziom zabezpieczenia terenu, budynków oraz systemów informatycznych.

Etap 2 – Opracowanie

Bardzo istotnym obszarem wdrożenia SZBI jest klasyfikacja aktywów (urządzeń, oprogramowania, danych, dokumentów itp.). Na wstępie należy dokonać inwentaryzacji aktywów i określić, jakie będą ewentualne konsekwencje braku dostępu lub ewentualnej utraty danego zasobu (np. jakie będą konsekwencje przerwy w dopływie prądu, braku dostępu do Internetu, wycieku danych czy awarii). W wyniku przeprowadzonej inwentaryzacji można przystąpić do kategoryzacji wyodrębniając następujące rodzaje[31]:

[31] Na podstawie: www.opensecurity.pl/polityka-bezpieczenstwa.

Za tego typu aktywa, należy uznać takie, bez których podmiot leczniczy nie może funkcjonować lub utrata których w wyniku udostępnienia dostępu osobom nieupoważnionym groziłaby znacznymi konsekwencjami. Do tej kategorii można zaliczyć:

- serwery,
- bazy danych,
- zbiory danych osobowych (np. pacjentów, pracowników),
- systemy i oprogramowanie wykorzystywane w procesie obsługi pacjentów oraz sprawozdawczości do NFZ.

2. Aktywa ważne
   Ten rodzaj aktywów obejmuje urządzenia i systemy, których zadania mogą być wykonane innymi środkami, ale przy dodatkowym nakładzie sił i kosztów lub których krótkotrwała niedostępność nie powoduje poważnych konsekwencji:
   - urządzenia sieciowe,
   - urządzenia i systemy do backupu i archiwizacji,
   - urządzenia wspomagające pracę serwerowni (klimatyzatory, VPS-y[32]),
   - systemy alarmowe,
   - systemy kontroli dostępu.
3. Aktywa zasadnicze
   Zadania tych aktywów przy relatywnie małym nakładzie sił i środków mogą być wykonane ręcznie. Do tego typu aktywów można zaliczyć:
   - komputery stacjonarne,
   - laptopy,
   - telefony.

   Bardzo istotnym aspektem związanym z klasyfikacją aktywów jest przeprowadzenie analogicznej kategoryzacji informacji. W związku z powyższym można wyodrębnić *informacje poufne*, do których dostęp ma wąskie grono osób upoważnionych. Do tego typu informacji należy zaliczyć np. informacje na temat stanu zdrowia pacjentów (wyniki badań, przebyte choroby itp.). Kolejnym rodzajem informacji byłyby *informacje wewnętrzne*, do których dostęp również mają określone osoby, ale jest to krąg szerszy i związany z bieżącą działalnością. Tego typu informacjami mogą być dane dotyczące np. zrealizowanych procedur medycznych wykonywane w ramach sprawozdawczości do NFZ.

[32] VPS (*Virtual Private Serwer*) – sposób podziału fizycznej maszyny na części, z której każda imituje oddzielny serwer fizyczny.

charakter publiczny. Do tego typu zaliczyć można treści udostępniane na stronach www (rodzaj i zakres udzielanych świadczeń, kadra zatrudniona na oddziałach) oraz w materiałach informacyjnych, takich jak katalogi czy broszury. Ponadto warto także wskazać miejsca przechowywania danych z uwzględnieniem okresowych i docelowych. W przypadku dokumentacji medycznej pacjentów, takiej np. historia choroby, początkowo jest przechowywana na oddziale, na którym pacjent jest hospitalizowany, a po jej zamknięciu przekazywana do archiwum jako miejsca docelowego. Wiąże się to oczywiście z określeniem odpowiednich zasad jej zabezpieczenia (w tym ograniczenia dostępu) i przekazywania (w tym czasie, w jakim to powinno nastąpić).

Przeprowadzenie czynności związanych z klasyfikacją aktywów pozwala na:

- usprawnienie przepływu informacji,
- zabezpieczenie się na wypadek ryzyka udostępnienia danych osobom nieupoważnionym w tym kradzieży danych,
- identyfikację ewentualnych przyczyn awarii mogących skutkować utratą danych.

Etap 3 – Testowanie

Bardzo istotnym etapem wdrożenia wymagań normy ISO 27001:2017 jest przeprowadzenie analizy ryzyka. Rzetelna ocena ryzyk wymaga czasu i zaangażowania całego zespołu. Szacowanie ryzyk zakłada ocenę skutków, poziom ewentualnych szkód, jakie mogą wystąpić w podmiocie leczniczym i prawdopodobieństwa wystąpienia. Należy tym samym określić, w kontekście kategoryzacji ryzyk konsekwencje związane z naruszeniem poufności danych, dostępem do nich jak i zachowaniem integralności.

Kolejnym etapem wdrożenia jest ocena poziomu zabezpieczeń w organizacji. Ten aspekt bardzo często naraża podmioty na koszty związane z zakupem zarówno odpowiedniego oprogramowania (licencje) oraz z wprowadzeniem rozwiązań organizacyjnych związanych z bezpieczeństwem fizycznym (np. ochrona, monitoring elektroniczny).

Przystępując do tworzenia dokumentacji SZBI należy pamiętać, że poziom jej szczegółowości powinien być uzależniony od charakteru prowadzonej działalności. Niezależnie jednak od tego poziomu jej sformalizowanie musi gwarantować określenie zasad pozwalających na zabezpieczenie informacji.

Norma ISO 27001 określa następujący zakres dokumentacji:

- zakres SZBI – pkt 4.3,
- raport procesu szacowania ryzyka – pkt 6.1.2,
- cele SZBI – pkt 6.2,
- opis metody szacowania ryzyk – pkt 8.2,
- plan postępowania z ryzykiem – pkt 8.3,
- dowód kompetencji – pkt 7.2,
- dowód wyników monitorowania i pomiarów – pkt 9.1,
- dowód realizacji programu audytów i wyników audytów – pkt 9.2,
- dowód wyników przeglądu – pkt 9.3,
- dowód charakteru niezgodności i wszelkich działań podjętych w ich następstwie oraz wyniki działań korygujących – pkt 9.3.

Istotnym dokumentem do przygotowania jest deklaracja stosowania, w której należy się odnieść do 18 grup celów stosowania zabezpieczeń wymienionych w załączniku A normy ISO 27001:2017. Skuteczne wdrożenie wymagań normy ISO 27001 jest możliwe jedynie przy udziale zatrudnionego personelu. Tym samym uzasadnione jest przeprowadzenie szkoleń dedykowanych różnym grupom zawodowym. Pierwszym szkoleniem, w który powinno uczestniczyć możliwie najwięcej osób, jest ogólne szkolenie z zakresu wymagań normy. Pracownicy mogą się dzięki temu dowiedzieć, czym jest SZBI, jakie są uwarunkowania jego wdrożenia oraz jaka jest ich rola w organizacji, która go wdrożyła. Dodatkowo osoba prowadząca takie szkolenie powinna w przystępny sposób przedstawić korzyści, jakie odniesie nie tylko podmiot, ale także osoby w nim zatrudnione.

Kolejne szkolenie powinno być dedykowane reprezentantom poszczególnych komórek organizacyjnych. W trakcie tego szkolenia powinna zostać omówiona struktura dokumentacji oraz zasady jej przygotowania.

Ostatnim z cyklu szkoleń jest szkolenie dla audytorów wewnętrznych, w trakcie którego poznają oni zasady audytowania. Osoba prowadząca takie szkolenie w formie warsztatowej powinna przedstawić zasady opracowania dokumentów roboczych (np. lista pytań audytowych), przygotowania planu audytów i opracowania raportu z audytu. Pomocne może okazać się wyjaśnienie, czym są niezgodności i jak je klasyfikować. Tak przygotowani kandydaci na audytorów wewnętrznych mogą sami lub przy udziale konsultanta przystąpić do przeprowadzenia audytów wewnętrznych. Przeprowadzenie audytów oraz regularnych przeglądów SZBI (w zaplanowanych odstępach czasu pkt. 9.3) pozwala nie tylko zweryfikować skuteczność wprowadzonych rozwiązań, ale także możliwość ciągłego doskonalenia, które pozwala podwyższać poziom bezpieczeństwa informacji.

powinien być przeprowadzony w następujących obszarach:

- analizy dokumentacji;
- weryfikacji realizowanego poziomu bezpieczeństwa informacji;
- bezpieczeństwa przetwarzania informacji w kontekście obowiązującej polityki bezpieczeństwa informacji;
- systemów teleinformatycznych;
- szkoleń z zakresu bezpieczeństwa danych osobowych;
- stany infrastruktury ICT (technologii informacyjno-komunikacyjnej) oraz sieciowej;
- usług zdalnej poczty elektronicznej;
- zasadności wdrożenia elektronicznego zarządzania dokumentami.

Zwieńczeniem przeprowadzonych działań i dowodem na zgodność wprowadzonych rozwiązań z wymaganiami normy EN/SO/ICE/27001:2017 jest poddanie się ocenie jednostki certyfikującej. Pozytywny wynik audytu certyfikującego może stanowić nie tylko powód do dumy, ale także element wyróżniający podmiot leczniczy spośród innych działających na danym terenie.

2.5.2. Korzyści i bariery wdrażania normy ISO 27001:2017 w podmiotach leczniczych

System zarządzania bezpieczeństwem informacji, ma na celu zapewnienie odpowiedniego poziomu odporności na zakłócenia i zagrożenia związane z bezpieczeństwem informacji. Jak wskazuje Malon Group (www.iso,org.pl pobrano dnia 30 grudnia 2021), do podstawowych korzyści z wdrożenia i stosowania systemu zarządzania bezpieczeństwem informacji zgodnego z wymaganiami ISO 27001:2017 należą:

1) eliminacja lub redukcja ryzyka wystąpienia zdarzeń związanych z bezpieczeństwem informacji;
2) przygotowanie organizacji na zdarzenia związane z bezpieczeństwem informacji, w tym dzięki odpowiednim procedurom, skuteczne przezwyciężanie incydentów, gdy się pojawią – efektywna odpowiedź, minimalizacja ich wpływu na organizacje;
3) proaktywne podejście do zarządzania bezpieczeństwem informacji poprzez zapobieganie potencjalnym skutkom zdarzeń dotyczących bezpieczeństwa informacji, do których można zaliczyć:
   a) kary związane z niestosowaniem się do przepisów prawa lub regulacji i interesariuszy,
   b) kary związane z niestosowaniem się do przepisów prawa lub regulacji umów cywilno-prawnych,
   c) brak możliwości realizacji działalności lub poszczególnych procesów i działań,
   d) utratę zaufania pacjentów oraz interesariuszy – zły public relations, utrata reputacji podmiotu,
   e) skutki wynikające z działań sabotażowych, przeprowadzanych przez pracowników,
   f) straty materialne i niematerialne wynikające z zakłóceń ciągłości działania;
4) wdrożony system podnosi wiarygodność organizacji w oczach pacjentów;
5) poprawa efektywności procesów oraz działań poprzez uregulowanie kwestii związanych z dostępem pracowników do właściwej oraz spójnej informacji, niezbędnej z punktu widzenia wykonywanych obowiązków oraz przydzielonych odpowiedzialności;
6) zapewnienie odpowiedniego poziomu odporności organizacji na zakłócenia działalności związane z bezpieczeństwem informacji oraz skuteczne zarządzanie zdarzeniem w przypadku materializacji zagrożenia;
7) spełnienie wymagań występujących w prawodawstwie w odniesieniu do wymagań klientów, a także ubezpieczycieli;
8) zapewnienie bezpieczeństwa danych pacjentów w wyniku poprawnie funkcjonującego systemu zarządzania informacją;
9) stosowanie odpowiedniego do ryzyka poziomu jakości ochrony aktywów informacyjnych;
10) zwiększenie przewagi konkurencyjnej organizacji na rynku;
11) uporządkowanie w zakresie dostępu do spójnej i integralnej informacji oraz obiegu informacji;
12) implementację i przegląd regulacji dotyczących bezpieczeństwa danych osobowych pod kątem ich adekwatności do sytuacji organizacji, zakresu przetwarzanych danych osobowych integracja z regulacjami dotyczącymi jakości, ochrony środowiska czy BHP;
13) spełnienie wymagania normy ISO 9001:2015 (w przypadku podmiotów, które posiadają już wdrożony system) w zakresie dostosowywania organizacji do nowych wymagań.

z którymi spotykają się kierownicy zakładów:

- brak zrozumienia pracowników co do istoty systemu, brak przestrzegania zaleceń i brak stosowania się do procedur, co powoduje pojawienie się incydentów lub niepożądanych zdarzeń związanych z bezpieczeństwem informacji;
- bagatelizowanie sfery zabezpieczeń przez zarządzających i pracowników;
- brak rejestracji incydentów, co w konsekwencji prowadzi do braku wdrożenia działań korygujących powodujących utratę danych;
- brak właściwego szacowania ryzyka w zakresie np. nośnika informacji, używanego software'u, lokalizacji – miejsca występowania informacji, właściciela informacji czy użytkownika;
- brak właściwych zasobów do wprowadzenia systemu – zwiększenie kosztów skutkujących pokusą niestosowania się do zaleceń systemu.

Mimo że kwestie bezpieczeństwa nie muszą być związane z występowaniem o certyfikację systemu, to jednak standard umożliwia systematyczną pracę nad poprawą bezpieczeństwa informatycznego.

2.6. Norma ISO 45001:2018 – system zarządzania bezpieczeństwem i higieną pracy

Każda organizacja jest odpowiedzialna za bezpieczeństwo i higienę pracy swoich pracowników oraz osób, na które może mieć wpływ jej działanie. Bezpieczeństwo i higienę pracy można definiować jako stan warunków organizacji pracy oraz zachowań pracowników, które zapewnią wymagany poziom ochrony zdrowia i życia przed zagrożeniami występującymi w środowisku pracy. Odpowiedzialność ta obejmuje propagowanie i ochronę zdrowia zarówno fizycznego, jak i psychicznego. Przyjęcie w organizacji systemowego podejścia do bezpieczeństwa i higieny pracy ma umożliwić zagwarantowanie instytucji niezagrażających zdrowiu i życiu warunków pracy. Możliwe będzie tym samym wypracowanie rozwiązań zapobiegających występowaniu urazów związanych z pracą. Celem systemu zarządzania bezpieczeństwem i higieną pracy w organizacji jest:

- eliminowanie czynników mogących stanowić zagrożenie dla zdrowia i życia kadry;
- wypracowanie zasad zarządzania ryzykiem i możliwościami BHP;
- zapobieganie urazom związanym z wykonywaniem czynności zawodowych.

bezpieczeństwo pracy na przestrzeni minionych dziesięcioleci ewoluowała. Na początku XX wieku pracodawcy koncentrowali się jedynie na odpowiednim wyposażeniu stanowiska pracy oraz na stanie technicznym urządzeń. Takie podejście oczywiście nie gwarantowało skutecznego eliminowania zagrożeń. Z czasem zdano sobie sprawę ze znaczenia środków ochrony osobistej i zaczęto wyposażać kadrę w fartuchy, kaski i osłony. Takie podejście było typowe dla okresu międzywojennego. Dopiero w latach pięćdziesiątych przedsiębiorcy zaczęli zwracać uwagę na znaczenie ergonomii stanowisk pracy oraz odpowiednią budowę maszyn i urządzeń. Zaczęto wprowadzać do zakładów takie rozwiązania, które miały być bezpieczne zarówno dla obsługującego urządzenie pracownika, jak i dla innych członków załogi. Pomimo sukcesywnego zmniejszania liczby wypadków przy pracy brakowało rozwiązań ograniczających prawdopodobieństwo wystąpienia zagrożeń. Dopiero w latach siedemdziesiątych i osiemdziesiątych XX wieku zdano sobie sprawę ze znaczenia szacowania ryzyk (zob. tabela 2.14). Na podstawie analizy wcześniejszych zdarzeń zaczęto przewidywać potencjalne zagrożenie.

Tabela 2.14. Etapy rozwoju podejścia do bezpieczeństwa i higieny pracy

Okres	Kamienie milowe rozwoju zarządzania BHP
Wiek XX (początek stulecia)	Zwrócenie uwagi na wypadki
Lata 30. XX w.	Środki ochrony indywidualnej i osłony
Lata 40.–50. XX w.	Ergonomia
Lata 60. XX w.	Bezpieczeństwo techniczne
Lata 70. XX w.	Analiza ryzyka i czynnik ludzki
Lata 80. XX w.	Organizacja a bezpieczeństwo
Lata 90. XX w.	Systemy zarządzania bezpieczeństwem pracy
Wiek XXI	Kultura bezpieczeństwa pracy

Źródło: Matuszak-Flejszman 2019, s. 209.

Należy zauważyć, że dopiero na przełomie XX i XXI wieku zdano sobie sprawę ze znaczenia prewencji. Pracodawcy zaczęli podejmować kroki mające na celu eliminowanie przyczyn, które mogą stanowić źródło późniejszego zagrożenia.

W prewencji wypadkowej ważna jest potencjalna możliwość spowodowania urazu, a nie tylko rzeczywisty rezultat. Uraz jest wynikiem wypadku, a jego skutki i koszty z nim związane są uzależnione od wielu czynników. Dlatego należy zapobiegać przede wszystkim przyczynom wydarzeń mogącym powodować

muje się ratownictwo medyczne). Praktyka gospodarcza pokazuje, że wypadki są często poprzedzone incydentami oraz niezgodnościami wskazującymi na istnienie zagrożeń dla bezpieczeństwa (Ewertowski 2018, s. 21). Przyjęcie takiego założenia pokazuje jak ważne są strategie proaktywne. Tym samym chcąc zwiększyć poziom bezpieczeństwa w organizacji, w tym także w podmiocie leczniczym, należy zgłaszać, archiwizować, wymieniać między działami i analizować wszelkie informacje dotyczące incydentów bezpieczeństwa. W efekcie łatwiej będzie wdrażać rozwiązania w zakresie poprawy bezpieczeństwa.

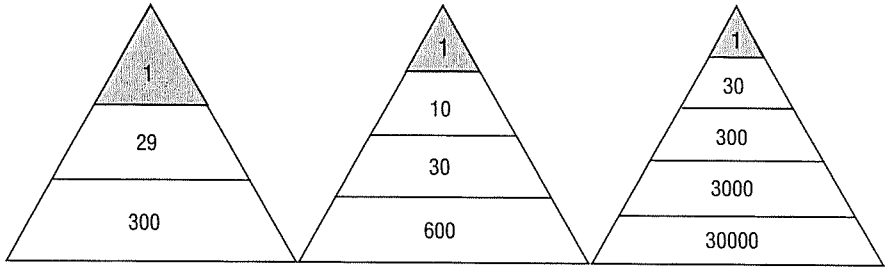
Podejście takie ilustruje tzw. trójkąt Heinricha, który jest uważany za fundament filozofii BHP. H.W. Heinrich przeprowadził w 1931 roku badania, z których wynikało, że każdy wypadek przy pracy powodujący ciężki uszczerbek na zdrowiu poprzedza wiele zdarzeń nieskutkujących urazem. Z analizy 330 zdarzeń tego samego rodzaju zdaniem H.W. Heinricha wynikało, że 300 nie powodowało uszczerbku na zdrowiu, 29 – średnie urazy, a tylko w 1 przypadku dochodziło do ciężkiego urazu. Wnioski, jakie z tych badań wyprowadził autor, podważały wcześniejsze teorie zakładające, że fundamentem działań zapobiegającym wypadkom powinny być analizy poważnych wypadków przy pracy. Według autora najcenniejsze wskazówki do ustalenia przyczyn wypadków można uzyskać biorąc pod uwagę grupę zdarzeń niepowodujących urazów lub przyczyniających się jedynie do lekkich urazów[33].

Z wynikami badań H.W. Heinricha, pomimo że miały znaczący wpływ na bezpieczeństwo pracy, podejmowano polemikę. Jednym z krytyków był W. Edwards Deming, który twierdził, że teoria Heinricha postrzegająca działania ludzi jako przyczynę większości wypadków w miejscu pracy jest błędna, ponieważ to organizacja pracy i złe systemy zarządzania doprowadzają do tego typu zdarzeń.

Tak zwany trójkąt Heinricha stał się inspiracją dla kolejnych badań przeprowadzanych przez F. Birda oraz firmę Conoco Philips Marine. Badania Birda zorganizowane w 1966 roku na próbie 1,7 mln raportów z wypadków poprawiły proporcje trójkąta i uwzględniały cztery kategorie, tj. wypadki śmiertelne, poważne wypadki, wypadki i incydenty. W 2003 roku firma Conoco Philips Marine przeprowadziła podobne badania, które ukazały znaczącą różnicę pomiędzy proporcją zdarzeń śmiertelnych a niebezpiecznych zachowań. Na każdy wypadek śmiertelny przypada co najmniej 30 000 niebezpiecznych zachowań (nieokreślonych do tamtej pory w taksonomiach zdarzeń). Zależności pokazujące proporcje Birda i Conoco Philips Marine ilustruje rysunek 2.8.

[33] www.atest.com.pl/teksty (dostęp: 20.09.2021).

Rysunek 2.8. Trójkąt Heinricha (po lewej) oraz jego modyfikacje wykonane przez Birda (w środku) i Conoco Philips Marine



Źródło: Ewertowski 2018, s. 22.

Chcąc zatem zwiększyć poziom bezpieczeństwa pracowników, należy wdrożyć rozwiązania systemowe, które pozwolą nie tylko właściwie organizować pracę, ale także nadzorować realizowane procesy.

2.6.1. Wymagania i znaczenie normy ISO 45001:2018

Analizując genezę powstania systemów zarządzania bezpieczeństwem i higieną pracy, należy cofnąć się do roku 1996 kiedy Brytyjski Instytut Normalizacyjny (BSI) opracował normę BS 8800. Norma ta miała charakter poradnika ułatwiającego skuteczne przewidywanie i zapobieganie występowaniu okoliczności narażających pracowników na utratę zdrowia lub życia oraz przeciwdziałanie chorobom zawodowym[34]. W Polsce w roku 1998 zainicjowano w Polskim Komitecie Normali-

[34] Podobne normy opracowano i ustanowiono również w innych krajach przodujących w zakresie systemowego podejścia do zarządzania BHP. Należy tu przede wszystkim wymienić normę holenderską NPR 5001 (NN1, 1996) oraz opracowaną przez australijsko-nowozelandzki komitet techniczny wspólną normę AS/NZS 4804/SA/SNZ,1997/2001). Normy i projekty norm dotyczących systemowego zarządzania BHP opracowano i opublikowano w Hiszpanii, gdzie ukazały się w postaci serii sześciu dokumentów. Dwie najważniejsze normy z tej serii to: UNE 81900 (AENOR,1996a) oraz UNE 81901 (AE-NOR,1996b). Komitet .Techniczny Międzynarodowej Organizacji ISO podjął w 1996 roku decyzję o opracowaniu międzynarodowych norm ISO serii 18001. Przeprowadzone w 1997 roku międzynarodowe konsultacje doprowadziły jednak do zaprzestania prac, które próbowano wznowić jeszcze w 1999 roku. Jednak po kolejnym międzynarodowym głosowaniu prace ponownie przerwano (Urbaniak 2004, s. 267).

w zakresie zarządzania bezpieczeństwem i higieną pracy. W strukturach PKN powołano Normalizacyjną Komisję Problemową nr 276 ds. Zarządzania BHP[35].

W normie ISO 45001:2018 zawarto wymagania dotyczące systemu zarządzania bezpieczeństwem i higieną pracy wraz z wytycznymi dotyczącymi jego stosowania w celu zapobiegania urazom przy pracy. W pkt 3.11. ISO 45000:2018 przyjęto, iż system zarządzania bezpieczeństwem i higieną pracy to część systemu zarządzania wykorzystywany do realizacji polityki BHP. Norma wskazuje, iż zamierzone wyniki to przede wszystkim zapobieganie urazom i dolegliwościom zdrowotnym pracowników oraz zapewnienie bezpiecznych i higienicznych miejsc pracy.

Przyjęto proaktywne założenia poprawy wyników w zakresie bezpieczeństwa poprzez stworzenie odpowiednich ram zarządzania ryzykiem i szansami w zakresie bezpieczeństwa i higieny pracy. Do zasadniczych celów wdrażanych rozwiązań w zakresie normy ISO 45001 można zaliczyć:

- zapobieganie wypadkom przy pracy,
- minimalizowanie ryzyka wystąpienia chorób zawodowych,
- zapewnienie bezpiecznych stanowisk pracy.

[35] Efektem prac tej komisji było opublikowanie serii norm PN-N-18000, która obejmowała następujące dokumenty:

– PN-N-18001:1999 Systemy zarządzania bezpieczeństwem i higieną pracy – Wymagania,

– PN-N-18002:2000 Systemy zarządzania bezpieczeństwem i higieną pracy – Ogólne wytyczne do oceny ryzyka zawodowego,

– PN-N-18004:2001 System zarządzania bezpieczeństwem i higieną pracy – Wytyczne.

W roku 2003 decyzją Prezesa Polskiego Komitetu Normalizacyjnego zatwierdzono nowowydane normy PN-N-18001-1999, które opublikowano w styczniu 2004 roku pod nazwą PN-N-18001:2004 System zarządzania bezpieczeństwem i higieną pracy.

Wśród obecnie obowiązujących standardów w zakresie systemowego podejścia do bezpieczeństwa i higieny pracy można wymienić następujące standardy o charakterze międzynarodowym (Matuszak-Flejszman 2019, s. 213):

– ILO-OSH 2001 Guidelines on Occupational Safety and Health Management System. Dokument opracowany przez Międzynarodowe Biuro Pracy (International Labour Organization – ILO), Genewa 2001;

– OHSAS 18001:2007 Occupational health safety management systems – Requirements, opracowany przez BSI, Londyn 2007;

– ISO 45001 Occupational health safety management systems – Requirements with guidance for use, norma opracowana przez Międzynarodową Organizację Normalizacyjną, Genewa 2018.

HLS (szerzej w pkt 2.2 pracy). Normę tworzą wymagania zawarte w rozdziałach od 4 do 10 oraz załącznik informacyjny A. Strukturę normy ISO 45001 przedstawia tabela 2.15.

Tabela 2.15. Struktura normy ISO 45001:2018

1. Zakres	
2. Powołania normatywne	
3. Terminy i definicje	
4. Kontekst organizacji	
4.1. Zrozumienie organizacji i jej kontekstu	
4.2. Zrozumienie potrzeb i oczekiwań pracowników i innych zainteresowanych	
4.3. Określenie zakresu systemu zarządzania bezpieczeństwem i higieną pracy 4.4. System zarządzania bezpieczeństwem i higieną pracy	
5. Przywództwo i zaangażowanie pracowników	
5.1. Przywództwo i zaangażowanie	
5.2. Polityka bezpieczeństwa i higieny pracy	
5.3. Role, odpowiedzialności i uprawnienia w organizacji	
5.4. Uczestnictwo i konsultacje pracowników	
6. Planowanie	**PLAN**
6.1. Działania dotyczące ryzyk i szans	
6.1.1. Wymagania ogólne	
6.1.2. Identyfikacja zagrożeń i ocena ryzyk i szans 6.1.2.1. Identyfikacja zagrożeń 6.1.2.2. Ocena ryzyka BHP i innych ryzyk dla SZBHP	
6.1.2.3. Ocena szans BHP i innych szans dla SZBHP	
6.1.3. Określenie wymagań prawnych i innych wymagań	
6.1.4. Planowanie działań	
6.2. Cele BHP i planowanie ich osiągnięcia 6.2.1. Cele BHP 6.2.2. Planowanie osiągnięcia celów BHP	

7.1. Zasoby	
7.2. Kompetencje 7.3. Świadomość	
7.4. Komunikacja 7.4.1. Wymagania ogólne 7.4.2. Komunikacja wewnętrzna 7.4.3. Komunikacja zewnętrzna	
7.5. Udokumentowane informacje 7.5.1. Wymagania ogólne 7.5.2. Opracowanie i aktualizowanie 7.5.3. Nadzór nad udokumentowanymi informacjami	DO
Działania operacyjne	
8.1. Planowanie i działania operacyjne 8.1.1. Wymagania ogólne	
8.1.2. Eliminowanie zagrożeń i zmniejszenie ryzyka BHP 8.1.3. Zarządzanie zmianami 8.1.4. Zakupy	
8.2. Gotowość na awarie	
Ocena efektów działania	
9.1. Monitorowanie, pomiary, analiza i ocena 9.1.1. Wymagania ogólne	
9.1.2. Ocena zgodności	CHECK
9.2. Audyt wewnętrzny 9.2.1.Wymagania ogólne 9.2.2. Program audytu wewnętrznego	
9.3. Przegląd zarządzania	
Doskonalenie	
10.1. Wymagania ogólne 10.2. Incydenty, niezgodności i działania korygujące	ACT
Ciągłe doskonalenie	

Źródło: na podstawie: ISO 45001:2018.

- zasadę ciągłego doskonalenia zgodne z cyklem PDCA (podobnie jak nowych wydaniach norm ISO 9001:2015, 14001:2015, 27001:2017);
- konieczność określenia kontekstu organizacji (przy wykorzystaniu metod analizy strategicznej);
- obowiązek określenia potrzeb i oczekiwań stron zainteresowanych (interesariuszy wewnętrznych i zewnętrznych);
- konieczność identyfikacji zagrożeń;
- obowiązek wprowadzenia analizy ryzyk;
- uwypuklono zapobieganie chorobom zawodowym i zdarzeniom potencjalnie wypadkowym oraz wypadkom;
- wprowadzono pojęcie udokumentowania informacji (zastąpienia podziału na dokumenty i zapisy);
- uwzględniono w systemie nadzoru nad dostawcami, w tym obszarami działań realizowanych w ramach outsourcingu.

W przypadku normy ISO 45001 istotnym **wymaganiem** jest konieczność identyfikacji zagrożeń i ocena ryzyka zawodowego. W tym celu powinny być zidentyfikowane wszystkie zagrożenia, jakie mogą wystąpić w organizacji, w tym w podmiocie leczniczym. Następnie zagrożenia należy przypisać do stanowisk wynikających ze struktury organizacyjnej i wprowadzić system oceny. Ocenia się prawdopodobieństwo wystąpienia zagrożenia oraz jego następstwa. W efekcie można wyodrębnić zagrożenia małe, średnie i duże (zob. tabela 2.16).

Tabela 2.16. Schemat oceny ryzyka zawodowego

Wyszczególnienie	Ciężkość/waga/powaga następstwa		
	Mała	Średnia	Duża
Zdarzenie mało prawdopodobne	Małe 1	Małe 1	Średnie 2
Zdarzenie prawdopodobne	Małe 1	Średnie 2	Duże 3
Zdarzenie wysoce prawdopodobne	Średnie 2	Duże 3	Duże 3

Źródło: na podstawie normy ISO 18002:2011.

czynników zwiększających ryzyko wystąpienia zagrożeń na stanowisku pracy. Można do nich zaliczyć:

- pracę w polu elektromagnetycznym,
- pracę z urządzeniami ciśnieniowymi,
- pracę ze szkodliwymi odczynnikami (np. cytostatyki),
- pracę z materiałem potencjalnie zakaźnym (ryzyko zakłucia),
- pracę z pacjentem (pacjenci pobudzeni).

Uwzględnienie powyższych ryzyk powinno skłonić dyrekcję podmiotów leczniczych do sumiennego podejścia do opracowania kart ryzyka zawodowego, w których będą identyfikowane zagrożenia oraz określane prawdopodobieństwo ich wystąpienia oraz ich ewentualne skutki. W efekcie możliwe będzie określenie w przypadku których ryzyk ich poziom można uznać za akceptowalny, a których za nieakceptowalny. W przypadku ryzyk, których poziom uznaje się za nieakceptowalny, koniecznym jest wprowadzenie określonych działań mających na celu obniżenie prawdopodobieństwa ich wystąpienia lub zniwelowanie skutków (zob. tabela 2.17).

Tabela 2.17. Arkusz szacowania ryzyka zawodowego

Proces	Opis zagrożenia	Skutek wystąpienia zagrożenia (S) Skala 1–3	Prawdopodobieństwo wystąpienia zagrożenia (P) Skala 1–3	Ryzyko wystąpienia zagrożenia R=SxP	Poziom ryzyka	Uwagi
zabieg operacyjny	zakłucie	3	2	6	nieakceptowalny	szkolenie personelu zakup sprzętu bezpiecznego (np. skalpele)

Źródło: opracowanie własne.

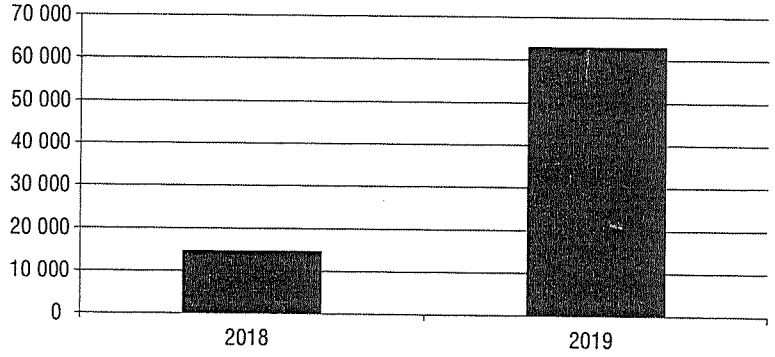
Wdrażając wymagania normy ISO 45001:2018 – System zarządzania bezpieczeństwem i higieną pracy, należy opracować wiele udokumentowanych informacji w tym politykę BHP i cele jej osiągnięcia. Zawarte w polityce zobowiązania najwyższego kierownictwa dotyczące zapewnienia zdrowych i bezpiecznych warunków pracy ma pozwolić na zapobieganie urazom i pogarszaniu stanu zdrowia personelu. Wykaz wymaganych w normie udokumentowanych informacji (tzn. takich, których opracowanie jest obligatoryjne, zawiera tabela 2.18).

Udokumentowane informacje	
4.3.	Zakres SZBHP
5.2.	Polityka BHP
5.3.	Obowiązki i uprawnienia dla odpowiednich ról w SZBHP przypisywane i przekazywane na wszystkich poziomach w organizacji
6.1.1.	Ryzyka i szanse związane z BHP
6.1.2.2.	Procesy i działania niezbędne do określenia i odniesienia się do ryzyk i szans w zakresie niezbędnym do uzyskania pewności, że są przeprowadzone zgodnie z planem
6.1.3.	Metodyka i kryteria oceny ryzyka związanego z bezpieczeństwem i higieną pracy Wymagania prawne i inne wymagania oraz ich aktualizacja w celu odzwierciedlenia wszelkich zmian
6.2.2.	Cele BHP i plany ich osiągnięcia
Udokumentowane informacje	
7.2.	Dowód kompetencji
7.5.3.	Dokumenty pochodzące z zewnątrz niezbędne do planowania i działania SZBHP
7.4.1.	Dowód komunikacji
8.1.1.	Zapewniające, że procesy zostały przeprowadzone zgodnie planem Dotyczące procesu(-ów) i planów reagowania na potencjalne sytuacje awaryjne
8.2.	Dowody wyników monitorowania, pomiaru, analizy i oceny działania
9.1.1.	Dowody konserwacji, kalibracji lub weryfikacji pomiaru urządzenia
9.1.2.	Wyniki oceny zgodności
10.2.	Charakter incydentów lub niezgodności oraz wszelkich podjętych działań Wyniki wszelkich działań i działań korygujących, w tym ocena ich skuteczności
9.2.2.	Dowód realizacji programu audytu i wyników kontroli
9.3.	Dowód wyników przeglądów zarządzania
10.3.	Dowód wyników ciągłego doskonalenia

Źródło: na podstawie: PN ISO 45001:2018.

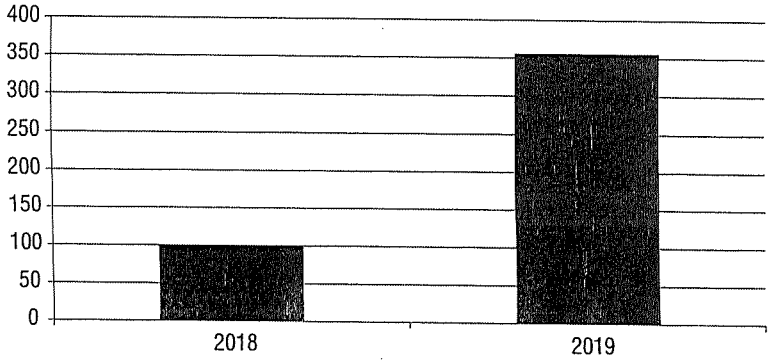
2.6.2. Korzyści i bariery wdrażania normy do podmiotów leczniczych

System ISO 45001:2018 cieszy się rosnącym zainteresowaniem na arenie międzynarodowej, czego dowodem może być rosnąca od momentu opublikowania normy liczba wydanych na świecie certyfikatów (por. wykres 2.7).



Źródło: https://www.kaiso.pl/statystyki-iso-2019 (dostęp: 17.12.2021).

Wykres 2.8. Wydane w Polsce certyfikaty ISO 45001:2018



Źródło: https://www.kaiso.pl/statystyki-iso-2019 (dostęp: 17.12.2021).

Podobnie jak w skali światowej tak i w Polsce można było zaobserwować znaczny poziom aprobaty wśród osób zarządzających organizacjami dla systemowego podejścia do bezpieczeństwa i higieny pracy. Świadczy to niewątpliwie o wysokim poziomie świadomości w zakresie ewentualnych zagrożeń, jakie mogą występować na poszczególnych stanowiskach pracy. Można wysunąć tezę, że jest to związane z chęcią wdrożenia przez osoby zarządzające proaktywnego podejścia do kwestii bezpieczeństwa.

Korzyści z wdrożenia normy ISO 45001:2018 mogą być następujące:

- zmniejszenie absencji chorobowej wśród pracowników;
- lepsza identyfikacja ryzyka – wprowadzenie standaryzacji w zakresie przyjmowania do pracy nowych pracowników obejmujące badania lekarskie (zdolność okresowe, zapoznanie z topografią podmiotu, przedstawienie obowiązujących na danym stanowisku standardów, przedstawienie do wglądu i podpisania karty ryzyka zawodowego pozwoli nie tylko obniżyć ryzyko wypadku, ale także zabezpieczyć podmiot na wypadek ewentualnych roszczeń personelu;
- redukcja kosztów ubezpieczenia – wdrożenie normy ISO 45001 w przypadku współpracy z niektórymi towarzystwami ubezpieczeniowymi pozwala także negocjować niższe składki (np. składka NNW – następstw nieszczęśliwych wypadków);
- budowanie wizerunku bezpiecznego pracodawcy;
- zmniejszenie liczby wypadków przy pracy;
- motywacja i zwiększenie zaangażowania pracowników;
- optymalizacja kosztów wypadków.

Wśród najczęstszych problemów pojawiających się w trakcie wdrożenia systemu można wymienić:

- wdrożenie systemu dla celów marketingowych – PR-owskich powoduje, że wprawdzie organizacja chwali się certyfikatem, ale nie procesy i monitorowanie przedsiębiorstwa są wirtualne;
- brak powiązania normy z celami danego podmiotu – brak koordynacji i konsultacji w zakresie procesów inwestycyjnych pomiędzy osobą odpowiedzialną za system a osoba nadzorującą prace wdrożeniowe/inwestycyjne zakładu;
- brak zaangażowania pracowników i bariery komunikacyjne – wynikają często z trybu nakazowego, który powoduje bariery mentalnościowe u pracowników;
- brak zaangażowania najwyższego kierownictwa w procesy wdrożeniowe – częste łamanie procedur ustanowionych dla pracowników, brak dobrego przykładu;
- brak zaangażowania i współudziału w tworzeniu procedur przez związki zawodowe;
- brak rozwijania u pracowników kompetencji w zakresie bezpieczeństwa i higieny pracy;
- brak warunków czy też właściwej procedury komunikacji sprzyjającej zgłaszanie incydentów;
- brak wprowadzanych programów modyfikacji zachowań niebezpiecznych i brak wyciągania rzeczywistych wniosków z audytów bezpieczeństwa.