

**WARSZAWA
WRZESIEŃ 2025**



**WPŁYW PROJEKTU NOWELIZACJI USTAWY O
KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA
NA SZPITALE PUBLICZNE**

PATRONAT NAD RAPORTEM OBJĘLI:



Polskie Towarzystwo Koordynowanej
Ochrony Zdrowia



Izba Gospodarcza "Farmacja Polska"



Fundacja AI LAW TECH



Federacja Przedsiębiorców Polskich

Szanowni Państwo,

Oddajemy w Państwa ręce raport, który powstał w odpowiedzi na rosnące wyzwania stojące przed polskimi szpitalami w związku z nowelizacją ustawy o Krajowym Systemie Cyberbezpieczeństwa. Wyniki przeprowadzonych analiz jasno pokazują, że wpływ nowych regulacji na codzienne funkcjonowanie placówek medycznych będzie znaczący – zarówno pod względem finansowym, jak i organizacyjnym.

Jako osoba od lat zaangażowana w działania na rzecz zdrowia publicznego, wiem, że bezpieczeństwo cyfrowe nie jest już tylko kwestią techniczną. To warunek zapewnienia pacjentom ciągłości opieki, sprawnego zarządzania danymi i rozwoju nowoczesnych modeli, takich jak opieka koordynowana. Tymczasem raport ujawnia, że świadomość konsekwencji nowych przepisów wśród dyrekcji szpitali pozostaje niska, a potrzeba wsparcia – bardzo duża.

Moim celem było nie tylko oszacowanie kosztów, ale przede wszystkim zwrócenie uwagi na realne potrzeby szpitali i konieczność wspólnego działania. Tylko dzięki współpracy decydentów, organizacji branżowych i samych placówek możliwe będzie zbudowanie systemu ochrony zdrowia odpornego na nowe zagrożenia.

Mam nadzieję, że niniejszy raport będzie dla Państwa cennym narzędziem – inspiracją do dyskusji, źródłem wiedzy oraz punktem wyjścia do podejmowania decyzji, które zadecydują o przyszłości polskich szpitali i bezpieczeństwie pacjentów.

Z wyrazami szacunku

Urszula Szybowicz

Szanowni Państwo,

Biorąc pod uwagę obecną sytuację geopolityczną oraz rosnącą skalę ataków w cyberprzestrzeni, konieczność zapewnienia bezpieczeństwa cyfrowego Polski nie podlega dyskusji. Kluczowym wyzwaniem pozostaje jednak określenie metod podnoszenia poziomu cyberbezpieczeństwa w taki sposób, aby nie generować dodatkowych ryzyk, w szczególności związanych z zakłóceniem działalności podmiotów szpitalnych, które powinny równolegle zwiększać swoją cyberodporność.

Raport zwraca również uwagę na problem dostępności alternatyw dla rozwiązań spoza UE i NATO. Szczególnie istotne jest rozważenie skutków rezygnacji z technologii, dla których brak bezpośrednich zamienników lub w których dostępne alternatywy cechują się gorszymi parametrami. Tego rodzaju decyzje mogą bezpośrednio wpływać na jakość i ciągłość realizowanych zadań.

Analiza raportu jasno wskazuje, że projekt nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa może oddziaływać na funkcjonowanie szpitali publicznych w znacznie szerszym zakresie niż wyłącznie kwestie związane z bezpieczeństwem cyfrowym. Ocena skutków regulacji jest niezbędna, aby uniknąć obniżenia jakości świadczeń czy ryzyka przerwania ciągłości działania.

Koszty wdrożenia nowych przepisów stanowią istotny element procesu, jednak koncentrowanie się wyłącznie na aspekcie finansowym może prowadzić do pominięcia innych kluczowych wyzwań, przed którymi staną placówki medyczne. Raport podkreśla zatem potrzebę całościowego podejścia, uwzględniającego szerokie spektrum konsekwencji proponowanych zmian.

W tym kontekście niezwykle ważne jest opracowanie takich procedur implementacji wymogów cyberbezpieczeństwa, które pozwolą równocześnie podnieść jego poziom i minimalizować ryzyka w innych obszarach działalności szpitali – które to ryzyka szczegółowo opisano w niniejszym raporcie.

Z wyrazami szacunku

Ireneusz Wochlik

Szanowni Państwo,

Podmioty lecznicze w Polsce znajdują się od wielu lat pod potężną presją finansową. Wdrażanie kolejnych obowiązków, przy jednoczesnym braku kompensacji ze strony instytucji stanowiących prawo jest jednym z głównym czynników, które mogą prowadzić do destabilizacji sektora szpitalnego w Polsce.

Chociaż w debacie publicznej najczęściej w kontekście rosnących zobowiązań szpitali wskazuje się regulacje płacowe, nowe obowiązki organizacyjne czy wzrost kosztów funkcjonowania, warto spojrzeć na szeroki zakres regulacji, które przyczyniają się do pogłębienia obecnej sytuacji. Skoro obecna sytuacja finansowa systemu ochrony zdrowia pogarsza się, a całość ryzyka jest przenoszona na świadczeniodawców, to obarczanie dodatkowymi, wielomilionowymi obowiązkami szpitale wydaje się zwyczajnie ryzykowne. Kontekst uzależnienia wdrażania koordynowanej opieki zdrowotnej właśnie od nowoczesnych technologii informatycznych wskazuje jak istotne znaczenie może mieć wdrożenie ustawy o KSC. Mam nadzieję, że ten wątek zostanie poddany szerokiej debacie, a jej podstawą będą odkrycia zawarte w tym dokumencie.

Wojciech Wiśniewski

Federacja Przedsiębiorców Polskich

KLUCZOWE USTALENIA I WNIOSKI

Przeprowadzona przez Polskie Towarzystwo Koordynowanej Ochrony Zdrowia akcja ankietowa, w połączeniu z przeprowadzoną analizą pozyskanych w ten sposób danych, pokazuje, że oszacowanie potencjalnych skutków finansowych dla szpitali jest możliwe, a także mierzalne.

W przeprowadzonej akcji ankietowej wzięło udział 421 szpitali publicznych, co stanowi około 52% wszystkich podmiotów leczniczych tego typu w Polsce, tym samym uzyskane wyniki można uznać za w pełni reprezentatywne i miarodajne w zakresie całego analizowanego podsektora ochrony zdrowia.

W grupie podmiotów wypełniających ankiety znalazły się szpitale ze wszystkich województw, o prawie wszystkich stopniach referencyjności, zakładane przez każdy rodzaj podmiotów tworzących, reprezentujące każdą formę organizacyjną i zatrudniające od 101 do ponad 5000 pracowników.

Analiza informacji zawartych w ankietach wskazuje, że przedstawiciele szpitali mają niską świadomość konsekwencji i skutków finansowych wejścia w życie nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa dla prowadzenia działalności leczniczej.

Z przeprowadzonej analizy szacowania kosztów związanych z koniecznością wymiany produktów i usług pochodzących od dostawców wysokiego ryzyka, w przypadku wydania decyzji administracyjnej w pełnym zakresie, wynika, że łączna kwota dla jednego szpitala może wynieść 4,6 mln zł netto w pięcioletnim okresie, a skutek dla wszystkich szpitali publicznych w Polsce, może wynosić w ciągu pięciu lat 3,7 mld zł netto. Koszty dla całego podsektora podmiotów leczniczych będą zdecydowanie wyższe, ze względu na konieczność dokonania wydatków przez szpitale prywatne, które nie brały udziału w niniejszym badaniu.

Warto podkreślić, że analiza została rozszerzona także o zagadnienia związane z koordynowaną opieką zdrowotną (KOZ). To obszar, który w ostatnich latach zyskuje na znaczeniu jako priorytet polityki zdrowotnej, a jednocześnie staje się coraz bardziej zależny od nowoczesnych technologii informatycznych. Wdrażanie KOZ wymaga bowiem integracji systemów IT, bezpiecznej wymiany danych medycznych oraz dostępu do stabilnych narzędzi cyfrowych wspierających procesy kliniczne i administracyjne. Tym samym przepisy nowelizacji ustawy o KSC, nakładające na szpitale obowiązki w zakresie cyberbezpieczeństwa, będą miały bezpośredni wpływ na możliwości rozwoju opieki

koordynowanej. Analiza świadomości, potrzeb i barier w tym zakresie pozwala lepiej zrozumieć skalę wyzwań, przed jakimi stoją polskie szpitale.

KONTEKST SPRAWY

W kwietniu 2024 r. na stronie Rządowego Centrum Legislacji został opublikowany projekt nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa (numer z wykazu UC32). Wnioskodawcą projektu jest Minister Cyfryzacji. Wersja po uzgodnieniach w ramach Komitetu Stałego Rady Ministrów, skierowana do prac w ramach Komisji Prawniczej pochodzi z 16 września br. i w oparciu o ten dokument był analizowany kontekst sprawy. Projekt ma implementować do krajowego porządku prawnego tzw. dyrektywę NIS2, czyli dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii. Zgodnie z ogólnie dostępnymi stanowiskami i opiniami prawnymi, projekt dokonuje transpozycji postanowień NIS2 w szerszym zakresie niż wymaga tego sama dyrektywa. Polska jako jedyny kraj postanowiła w jednym akcie prawnym wdrożyć rozwiązania wynikające z dyrektywy NIS2 oraz 5G Toolbox, rozszerzając przy tym regulacje dotyczące dostawców wysokiego ryzyka (tzw. DWR) na wszystkie 18 sektorów, a nie tylko sieci 5G. Tak zdefiniowane regulacje wiązać się będą z konsekwencjami dla inwestycji i dostępności technologii, a konieczność usuwania sprzętu i usług DWR może generować znaczne obciążenia finansowe dla podmiotów zobowiązanych do dostosowania infrastruktury. Obecnie lista sektorów i podsektorów dla podmiotów kluczowych i ważnych wygląda następująco:

Podmioty kluczowe	
Sektor	Podsektor
Energia	Wydobywanie kopalin
	Energia elektryczna
	Ciepło
	Ropa i paliwa
	Gaz
	Energetyka jądrowa
	Wodór
Transport	Transport lotniczy
	Transport kolejowy
	Transport wodny

	Transport drogowy
Bankowość i infrastruktura rynków finansowych	
Ochrona zdrowia	Udzielanie świadczeń zdrowotnych i zdrowie publiczne
	Produkcja i dystrybucja substancji czynnych, produktów leczniczych i wyrobów medycznych
Zaopatrzenie w wodę pitną i jej dystrybucja	
Zbiorowe odprowadzanie ścieków	
Infrastruktura cyfrowa	Infrastruktura cyfrowa z wyłączeniem komunikacji elektronicznej
	Komunikacja elektroniczna
Zarządzanie usługami ICT	
Przestrzeń kosmiczna	
Podmioty publiczne	

Podmioty ważne	
Sektor	Podsektor
Usługi pocztowe	
Inwestycje energetyki jądrowej	
Gospodarowanie odpadami	Zbieranie odpadów
	Transport odpadów
	Przetwarzanie odpadów, w tym sortowanie, wraz z nadzorem nad wymienionymi działaniami, a także późniejsze postępowanie z miejscami unieszkodliwiania odpadów
	Działania wykonywane w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami
Produkcja, wytwarzanie i dystrybucja chemikaliów	

Produkcja, przetwarzanie i dystrybucja żywności	
Produkcja	Produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro
	Produkcja komputerów, wyrobów elektronicznych i optycznych
	Produkcja urządzeń elektrycznych
	Produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana
	Produkcja pojazdów samochodowych, przyczep i naczep
	Produkcja pozostałego sprzętu transportowego
Dostawcy usług cyfrowych	
Badania naukowe	
Podmioty publiczne ¹	

Należy także wskazać, że za podmiot kluczowy i ważny co do zasady mogą być uznane firmy będące co najmniej średnim przedsiębiorstwem². Projekt przewiduje jednak wyjątki. Chodzi m.in. o sytuację, gdy zakłócenie świadczonej usługi mogłoby mieć znaczący wpływ na porządek, bezpieczeństwo lub zdrowie publiczne. W takim przypadku regulacje ustawowe będą dotyczyć także małych i mikro przedsiębiorców. W zależności od poszczególnych decyzji, liczba podmiotów, która zostanie objęta obowiązkami regulacyjnymi, wynosi ok. 38 000.

Wśród kolejnych obszarów, gdzie regulacje zostały rozbudowane w porównaniu z unijną regulacją, znajdują się – poza wskazanym powyżej rozszerzeniem katalogu sektorów kluczowych – wprowadzenie krajowej procedury uznania firmy za DWR, zwiększenie wysokości kar finansowych, wprowadzenie mechanizmu polecenia zabezpieczającego, rozszerzenie odpowiedzialności osobistej członków władz organizacji oraz zobowiązanie CSIRT do współpracy ze służbami specjalnymi, możliwość zawieszenia koncesji lub wycofania zezwolenia czy konieczność wykonywania cyklicznych audytów.

Na szczególną uwagę zasługuje kwestia DWR. Projekt ustawy określa ich jako dostawców technologii, usług ICT, sprzętu lub oprogramowania, których działalność,

¹ Jedynie w zakresie jednostek samorządu terytorialnego.

² Średnie przedsiębiorstwo zatrudnia od 50 do 250 pracowników oraz jego roczny obrót nie przekracza 50 mln euro lub roczna suma bilansowa nie przekracza 43 mln euro.

pochozenie kapitału, powiązania z krajami spoza UE i NATO czy historia zgodności z międzynarodowymi standardami bezpieczeństwa mogą stwarzać zagrożenie dla bezpieczeństwa narodowego lub integralności systemów informatycznych.

Zaliczenie dostawcy do tej kategorii w ramach procedury określonej w nowelizacji opiera się na ocenie ryzyka, dokonywanej przez ministra cyfryzacji oraz opinii kolegium do spraw cyberbezpieczeństwa. Kryteria obejmują aspekty techniczne (m.in. historia incydentów bezpieczeństwa czy zidentyfikowanych podatności) i nietechniczne (zagrożenia ekonomiczne, wywiadowcze, terrorystyczne, wpływ państw spoza UE i NATO, ochrona danych osobowych oraz powiązania z podmiotami objętymi sankcjami międzynarodowymi). Fundamentalny dla celów niniejszej analizy jest przepis ustawy, który stanowi, że po zaliczeniu dostawcy do grona DWR, podmioty kluczowe i ważne muszą zaprzestać użytkowania dostarczanych przez niego określonych w decyzji produktów, usług i procesów ICT w ciągu 4 lat (duzi operatorzy telekomunikacyjni) lub 7 lat (pozostałe podmioty). To z kolei będzie prowadzić do poniesienia przez podmioty znacznych nakładów finansowych na zakup nowych produktów i usług oraz ich wdrożenie w swojej organizacji.

Odnosząc się do sektora ochrony zdrowia, to opracowana przez Ministerstwo Cyfryzacji Ocena Skutków Regulacji wskazuje, że nowelizacja ustawy będzie miała wpływ łącznie na 1248 podmiotów. OSR nie precyzuje ile z tej liczby dotyczy podmiotów z podsektora udzielanie świadczeń zdrowotnych i zdrowie publiczne, a ile z podsektora produkcja i dystrybucja substancji czynnych, produktów leczniczych i wyrobów medycznych. Według danych Polskiego Towarzystwa Koordynowanej Ochrony Zdrowia samych szpitali publicznych jest w Polsce obecnie około 800 i taką liczbę przyjęto do dalszych analiz skutków finansowych. Uzasadnieniem dla takiego podejścia jest wprowadzona w projekcie nowelizacji KSC reguła wskazująca, że podmiot leczniczy, który nie jest przedsiębiorcą (w tej grupie znajdują się właśnie szpitale publiczne) jest uznawany za podmiot ważny, jeżeli zatrudnia od 50 do 249 osób, a za podmiot kluczowy jeżeli zatrudnia co najmniej 250.

OSR – w kontekście skutków finansowych – prezentuje jedynie wpływ na sektor finansów publicznych. Znajduje się tam także stwierdzenie, że wszystkie skutki finansowe z tytułu realizacji projektowanej ustawy w części 46 – *Zdrowie* sfinansowane zostaną w ramach środków na ochronę zdrowia, w tym w ramach ustalonego funduszu wynagrodzeń (niezwiększonego z tytułu tej ustawy), bez możliwości ubiegania się o dodatkowe środki ponad te kwoty. W tym kontekście istotne jest także pismo Ministra Zdrowia z 1 września br. skierowane do Sekretarza Stałego Komitetu Rady Ministrów, w którym wskazano, że brak możliwości ubiegania się o dodatkowe środki oznacza realny brak możliwości

zwiększenia wydatków na wynagrodzenia osobowe, w tym dla osób realizujących w ministerstwie oraz Centrum e-Zdrowia zadania wynikające z projektowanej ustawy w ramach działalności sektorowego zespołu cyberbezpieczeństwa – CSiRT Centrum e-Zdrowia.

Z załącznika nr 4 do OSR, zawierającego szczegółowe wyliczenia planowanych wydatków wprost wynika, że projektodawca określił jedynie skutki finansowe z części budżetowej 46 na zadania dotyczące funkcjonowania CSIRT, wynagrodzeń dla dodatkowych pracowników, w tym składek na ubezpieczenia społeczne, Fundusz Pracy, Fundusz Solidarnościowy, PPK, koszty stanowiska pracy oraz koszty zakupu licencji do norm technicznych i innych dokumentów standaryzacyjnych z zakresu cyberbezpieczeństwa. Całkowicie zostały pominięte koszty związane z koniecznością wycofania sprzętu lub oprogramowania od dostawców wysokiego ryzyka i zastąpienia ich nowymi produktami. To z kolei prowadzi do wniosku, że koszty te będą musiały ponosić szpitale ze środków własnych lub ze środków własnych organów tworzących.

W sekcji pn. „Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe” tabela dotycząca skutków w ujęciu pieniężnym nie została wypełniona, ale jednocześnie projektodawca przyznaje, że wejście przepisów w życie będzie się wiązać ze wzrostem nakładów finansowych jednak Ministerstwo Cyfryzacji przyznało, że na tym etapie nie jest możliwe oszacowanie kosztów dostosowawczych po stronie przedsiębiorców w zależności od ich rodzajów z uwagi na brak danych.

Projektodawca stwierdził, że koszty związane z wycofaniem sprzętu lub oprogramowania od dostawców wysokiego ryzyka są niemierzalne. Nowelizacja przewiduje kompetencję dla ministra właściwego do spraw informatyzacji do wydania decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, co zdaniem Ministerstwa Cyfryzacji, prowadzi do niemożności wskazania kosztów jakie poniosą podmioty kluczowe i podmioty ważne w związku z wycofaniem produktów ICT, usług ICT i procesów ICT pochodzących od dostawców wysokiego ryzyka, ponieważ nie można w tej chwili przewidzieć jaką decyzję wyda minister i w związku z tym jakie koszty poniosą podmioty zobowiązane do wycofania sprzętu.

CELE ANALIZY

W związku z tym, że projektodawca nie przygotował na potrzeby OSR nawet szacunkowych danych dotyczących kosztów niezbędnych do poniesienia przez podmioty lecznicze w celu dostosowania się do nowych wymogów regulacyjnych, w tym potencjalnych kosztów wymiany produktów ICT, usług ICT i procesów ICT pochodzących od dostawców wysokiego ryzyka, celem analizy jest przeprowadzenie oszacowania takich skutków w oparciu o dane ze szpitali publicznych pozyskane przez Polskie Towarzystwo Koordynowanej Ochrony Zdrowia.

Dodatkowymi celami analizy są: określenie świadomości kierownictwa szpitali na temat konsekwencji finansowych i organizacyjnych wejścia w życie nowych przepisów oraz czy w ich ocenie istnieje realna alternatywa zastąpienia sprzętu i usług dostawców wysokiego ryzyka produktami dostawców pochodzących wyłącznie z terenu UE oraz NATO.

Ponadto analizie zostaną poddane odpowiedzi na pytania dotyczące koordynowanej ochrony zdrowia, w tym jej organizacji, wykorzystywanych technologii i bezpieczeństwa cyfrowego, a także wyzwań i potrzeb poszczególnych szpitali.

MATERIAŁY ŹRÓDŁOWE

Do analizy wykorzystano informacje przekazane przez szpitale. Dane te zostały pozyskane poprzez opracowanie ankiety, umieszczonej na dedykowanej podstronie Polskiego Towarzystwa Koordynowanej Ochrony Zdrowia. Okres ankietowania trwał od 1 do 31 sierpnia 2025 r. Dane do analizy zostały przekazane w postaci pliku .xls. Ankiety na potrzeby tej analizy zostały wypełnione przez 421 szpitali publicznych, co stanowi ponad 50% wszystkich podmiotów leczniczych z tej grupy. W grupie podmiotów wypełniających ankietę były szpitale ze wszystkich województw, prawie wszystkich poziomów (I, II, III poziom, ogólnopolskie, pediatryczne, psychiatryczne oraz pulmonologiczne i onkologiczne), placówki wszystkich podmiotów tworzących (jednostki samorządu terytorialnego – miasta na prawach powiatu, starostwa powiatowe, województwa, ale też wojewodowie, Ministerstwo Obrony Narodowej, Ministerstwo Spraw Wewnętrznych i Administracji oraz państwowe uczelnie medyczne), szpitale reprezentujące każdą formę organizacyjną (SPZOZ, spółki samorządowe, szpitale resortowe i uniwersyteckie), zatrudniające od 101 do ponad 5000 pracowników, co zgodnie z projektem nowelizacji KSC oznacza, że wszystkie te szpitale mają status podmiotów kluczowych lub ważnych.

Dodatkowo do analizy wykorzystano projekt nowelizacji ustawy KSC w wersji z dnia 16 września 2025 r., w szczególności informacje znajdujące się w Ocenie Skutków Regulacji i uzasadnieniu, a także informacje ogólnodostępne w źródłach otwartych.

WYNIKI ANALIZY

W ramach ankiety sformułowano 29 następujących pytań:

1. W którym województwie znajduje się szpital?
2. Jaki jest poziom szpitala?
3. Jaki był organ tworzący szpital?
4. Jaka jest forma organizacyjna?
5. Jaka jest liczba zatrudnionych pracowników?
6. Jaka była wielkość kontraktu z NFZ w 2024 r.?
7. Czy znane są Pani/Panu konsekwencje dla szpitali wprowadzenia ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa przedstawionego przez Ministerstwo Cyfryzacji?
8. Ile w zasobach Pani/Pana szpitala znajduje się sprzętu teleinformatycznego, urządzeń elektronicznych, maszyn (komputery, serwery, routery, switchy, drukarki, skanery, monitory, kamery, rezonans magnetyczny, tomograf komputerowy, RTG, USG, kardiomonitor, ciśnieniomierze, pompy infuzyjne, wyposażenie OIT itp.) od producentów pochodzących spoza państw Unii Europejskiej i NATO?
9. Czy Pani/Pana zdaniem istnieje realna możliwość wymiany powyższego sprzętu teleinformatycznego, urządzeń elektronicznych, maszyn i zastąpienie ich wyłącznie urządzeniami produkowanymi przez firmy z państw Unii Europejskiej i NATO?
10. Jeżeli TAK to: czy Pani/Pana zdaniem koszt netto wymiany sprzętu teleinformatycznego, urządzeń elektronicznych, maszyn (koszt wymiany jest rozumiany jako zakup nowych urządzeń, utylizacja wymienianych oraz usługa demontażu i instalacji nowych urządzeń) będzie na poziomie:?
11. Jaka jest procentowa wartość wykorzystywanego oprogramowania (w tym programów komputerowych, aplikacji, sterowników, silników bazodanowych etc., niezależnie od formy posiadania – własność produktów, licencje, subskrypcje itp.) pochodzącego od producentów z państw spoza Unii Europejskiej i NATO w stosunku do całego posiadanego oprogramowania?

12. Czy Pani/Pana zdaniem istnieje realna możliwość wymiany powyższego oprogramowania i zastąpienie go wyłącznie oprogramowaniem od producentów pochodzących z państw Unii Europejskiej i NATO?
13. Jeżeli TAK to: czy Pani/Pana zdaniem koszt netto wymiany oprogramowania (koszt wymiany jest rozumiany jako zakup nowego oprogramowania oraz usługi deinstalacji oraz instalacji, konfiguracji i wdrożenia nowego, a także migracji danych z wycofywanych systemów do nowych systemów IT) będzie na poziomie:?
14. Czy zna Pani/Pan roczne koszty serwisu i wsparcia technicznego posiadanego sprzętu teleinformatycznego, urządzeń elektronicznych, maszyn od producentów pochodzących spoza państw Unii Europejskiej i NATO?
15. Jeżeli TAK to: jest to kwota netto na poziomie:?
16. Czy zna Pani/Pan roczne koszty serwisu i wsparcia technicznego dla posiadanego oprogramowania pochodzącego od producentów spoza państw Unii Europejskiej i NATO?
17. Jeżeli TAK to: jest to kwota netto na poziomie:?
18. Czy Pani/Pana zdaniem wymiana posiadanego sprzętu teleinformatycznego, urządzeń elektronicznych, maszyn na sprzęt pochodzący wyłącznie z państw Unii Europejskiej i NATO będzie wiązała się z większymi kosztami serwisu i wsparcia technicznego?
19. Jeżeli TAK to: będzie to kwota netto na poziomie:?
20. Czy Pani/Pana zdaniem wymiana posiadanego oprogramowania na oprogramowanie pochodzące wyłącznie z państw Unii Europejskiej i NATO będzie wiązała się z większymi kosztami serwisu i wsparcia technicznego?
21. Jeżeli TAK to: będzie to kwota netto na poziomie:?
22. Czy szpital realizuje opiekę koordynowaną w ramach umowy z NFZ?
23. Jakie elementy opieki koordynowanej są obecnie realizowane przez szpital?
24. Czy szpital korzysta z systemu IT wspierającego opiekę koordynowaną (np. integracja EHR, system kolejkowy, zarządzanie terapią)?
25. Czy systemy wspierające KOZ są zgodne z wymaganiami cyberbezpieczeństwa przewidzianymi w nowelizacji ustawy o KSC?
26. Czy szpital przeprowadził analizę ryzyk w zakresie cyberbezpieczeństwa systemów wykorzystywanych w opiece koordynowanej?
27. Jakie bariery utrudniają Państwa szpitalowi skuteczne wdrażanie opieki koordynowanej?
28. Czy szpital planuje rozszerzenie zakresu opieki koordynowanej w ciągu najbliższych 12 miesięcy?

29. Jakie wsparcie byłoby najbardziej pomocne przy wdrażaniu/rozwoju OKZ?

Pierwsze sześć pytań miało charakter techniczno-organizacyjny, gdyż na ich podstawie dokonano weryfikacji grupy podmiotów leczniczych spełniających kryteria zawarte w projekcie nowelizacji ustawy KSC dla podmiotów ważnych i kluczowych, a także określenia czy mamy do czynienia ze szpitalami publicznymi czy prywatnymi.

Poniżej zaprezentowano kilka podstawowych danych liczbowych, wskazujących na reprezentatywny rozkład podmiotów leczniczych, biorących udział w procesie ankietowania.

Tabela nr 1 – Liczba szpitali w podziale na województwa

województwo	liczba
dolnośląskie	42
kujawsko-pomorskie	31
lubelskie	24
lubuskie	17
łódzkie	31
małopolskie	33
mazowieckie	56
opolskie	14
podkarpackie	22
podlaskie	12
pomorskie	22
śląskie	45
świętokrzyskie	16
warmińsko-mazurskie	17
wielkopolskie	24
zachodniopomorskie	15

Tabela nr 2 – Liczba szpitali w podziale na poziomy (stopnie referencyjności)

poziom	liczba
I poziom	166
II poziom	98
III poziom	67
ogólnopolski	37
pediatryczny	8
psychiatryczny	21
pulmonologiczny/onkologiczny	24

Tabela nr 3 – Liczba szpitali w podziale na organ tworzący

organ tworzący	liczba
JST-powiat	186
JST-miasto	72
JST-województwo	23
wojewoda	109
MON	7
MSWiA	9
uczelnia medyczna	15

Tabela nr 4 – Liczba szpitali w podziale na formę organizacyjną

forma organizacyjna	liczba
spółka samorządowa	41
SPZOZ	349
szpital resortowy	16
szpital uniwersytecki	15

Tabela nr 5 – Liczba szpitali w podziale na liczbę pracowników

liczba zatrudnionych	liczba
101-250	12
251-500	273
501-1000	74
1001-5000	60
ponad 5000	2

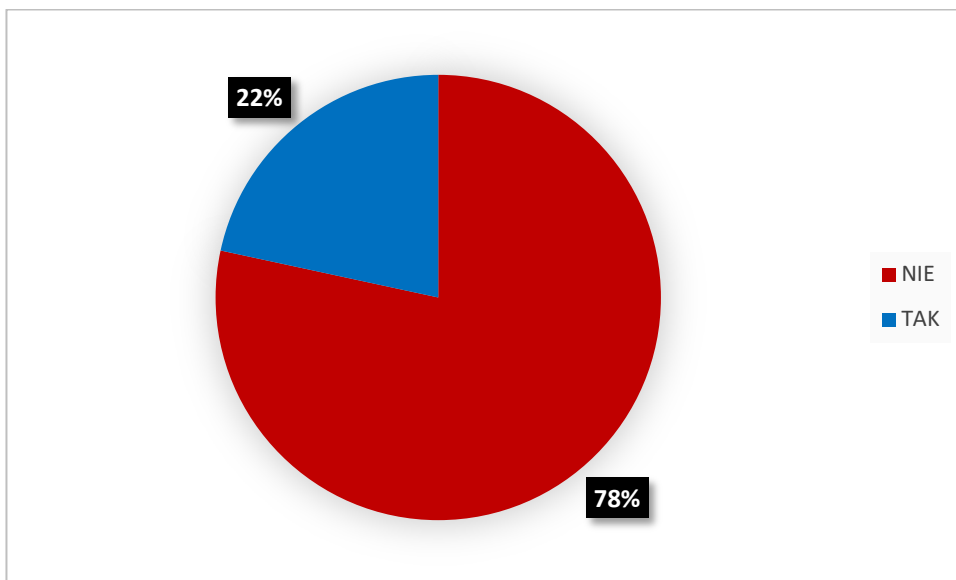
Jak zostało wspomniane na wstępie, powyższe statystyki wskazują na pełną referencyjność danych, a także kompleksową reprezentację podmiotów biorących udział w ankiecie. Istotne jest przede wszystkim to, że wszystkie szpitale biorące udział w ankiecie zostaną objęte regulacjami nowelizacji ustawy KSC, a 97% z nich posiada status podmiotu kluczowego, co oznacza, że będą musiały realizować wszystkie obowiązki ustawowe. W kwestii posiadanego kontraktu z NFZ w 2024 r., należy ocenić, że jego wysokość jest sprawą indywidualną, natomiast przedział w przypadku ankietowanych szpitali wynosi od 5 mln zł do 1,8 mld zł.

Kolejny zestaw 15 pytań oraz zależności między poszczególnymi pytaniami stwarzają podstawę do udzielania odpowiedzi na pytania wskazane w podstawowych celach

analizy. Ostatnie 8 pytań odwołuje się do zagadnień z obszaru koordynowanej ochrony zdrowia.

Pierwszym celem analizy było określenie poziomu świadomości podmiotów leczniczych, jaki wpływ na ten podsektor ochrony zdrowia będą mieć przepisy nowelizacji ustawy KSC. Zagadnienie zostało zaadresowane pytaniem nr 7. Spośród 421 odpowiedzi, w 330 przypadkach ankietowani wskazali odpowiedź „NIE”. Stanowi to 78% wszystkich odpowiedzi, co prowadzi do wniosku, że kierownictwo szpitali posiada bardzo mały stan wiedzy na temat konsekwencji wejścia przepisów w życie na prowadzenie działalności leczniczej – zarówno w wymiarze organizacyjnym jak i finansowym.

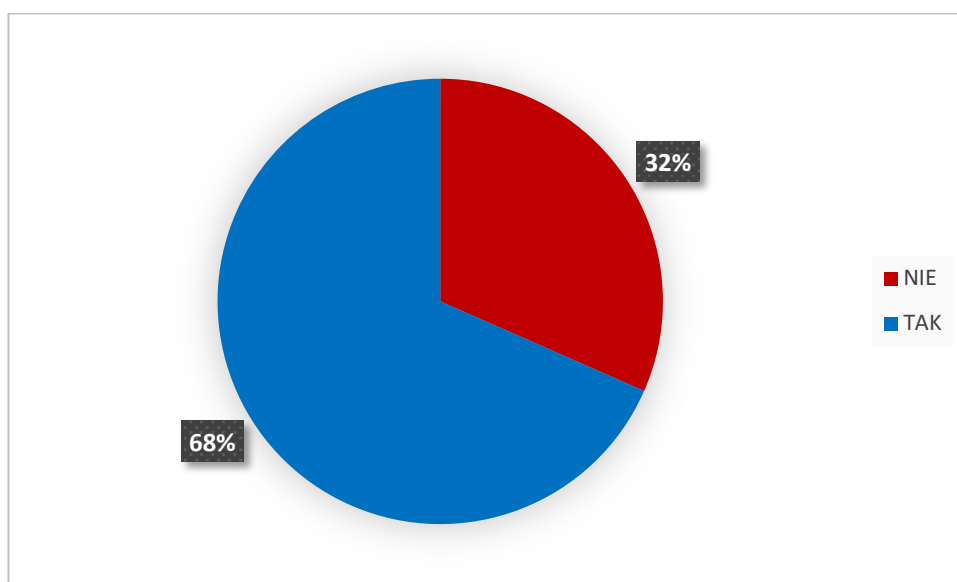
Wykres nr 1 – Odpowiedzi udzielone na pytanie: Czy znane są Pani/Panu konsekwencje dla szpitali wprowadzenia ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa przedstawionego przez Ministerstwo Cyfryzacji?



Kolejnym celem była próba ustalenia, czy dla sprzętu i oprogramowania podmiotów uznanych za dostawców wysokiego ryzyka istnieje realna alternatywa w postaci produktów dostarczanych przez firmy z UE lub NATO. Ten aspekt jest niezwykle istotny dla bezpieczeństwa państwa. Jeżeli podmioty ważne i kluczowe zostaną zobowiązane do wycofania z użytkowania określonego sprzętu i oprogramowania, a nie będzie dla nich zamienników w wymiarze funkcjonalnym (aspekt kosztowy zostanie omówiony w dalszej części raportu), może to doprowadzić do zatrzymania lub znaczącego spowolnienia procesów i produkcji w tych organizacjach, które działają w sektorach uznanych przez projektodawcę za fundamentalne dla bezpieczeństwa wewnętrznego i stabilności państwa.

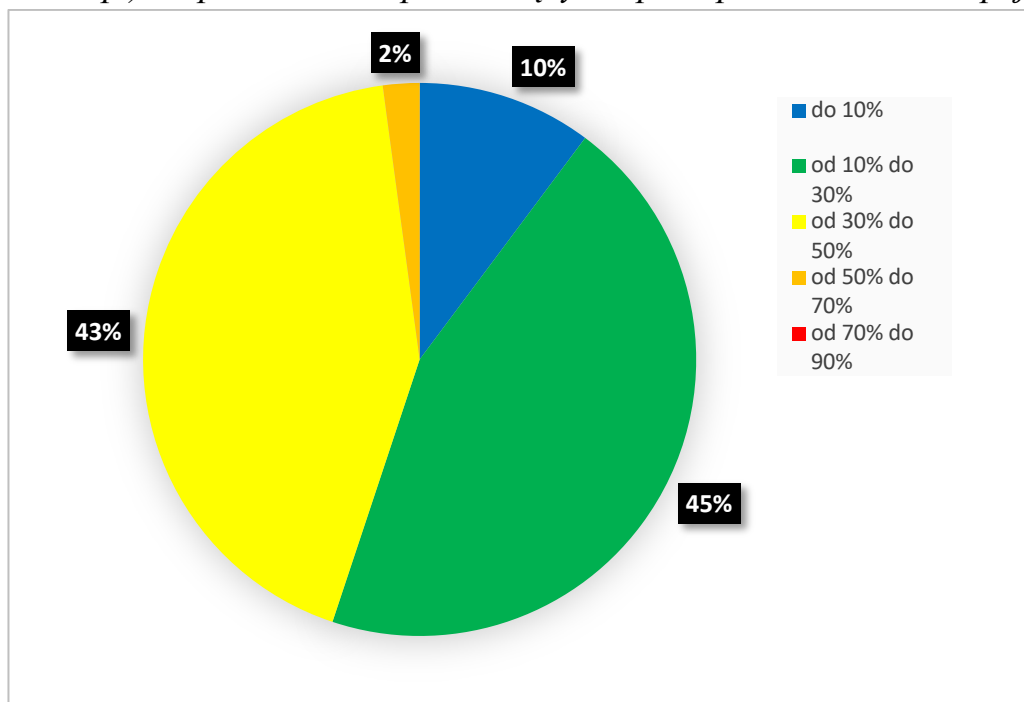
W przypadku możliwości wymiany sprzętu 133 z 421 ankietowanych stwierdziło, że taka opcja nie istnieje. Stanowi to 32% wszystkich odpowiedzi.

Wykres nr 2 – Odpowiedzi udzielone na pytanie: Czy Pani/Pana zdaniem istnieje realna możliwość wymiany powyższego sprzętu teleinformatycznego, urządzeń elektronicznych, maszyn i zastąpienie ich urządzeniami produkowanymi przez firmy z państw Unii Europejskiej i NATO?



W celu oceny na ile ewentualna decyzja decydentów o konieczności wymiany produktów podmiotu uznanego za dostawcę wysokiego ryzyka może być problematyczna i w praktyce doprowadzić do zatrzymania lub utrudnienia realizacji świadczeń medycznych i tym samym zaburzenia prowadzenia działalności leczniczej, należy także ocenić jaki udział sprzętu producentów spoza UE i NATO znajduje się w zasobach ankietowanych szpitali. Taki właśnie cel miało pytanie nr 8 ankiety. Poniżej zostały przedstawione dane w ujęciu procentowym prezentujące ten podział.

Wykres nr 3 – Odpowiedzi udzielone na pytanie: Ile w zasobach Pani/Pana szpitala znajduje się sprzętu teleinformatycznego, urządzeń elektronicznych, maszyn (komputery, serwery, routery, switchy, drukarki, skanery, monitory, kamery, rezonans magnetyczny, tomograf komputerowy, RTG, USG, kardiomonitor, ciśnieniomierze, pompy infuzyjne, wyposażenie OIT itp.) od producentów pochodzących spoza państw Unii Europejskiej i NATO?

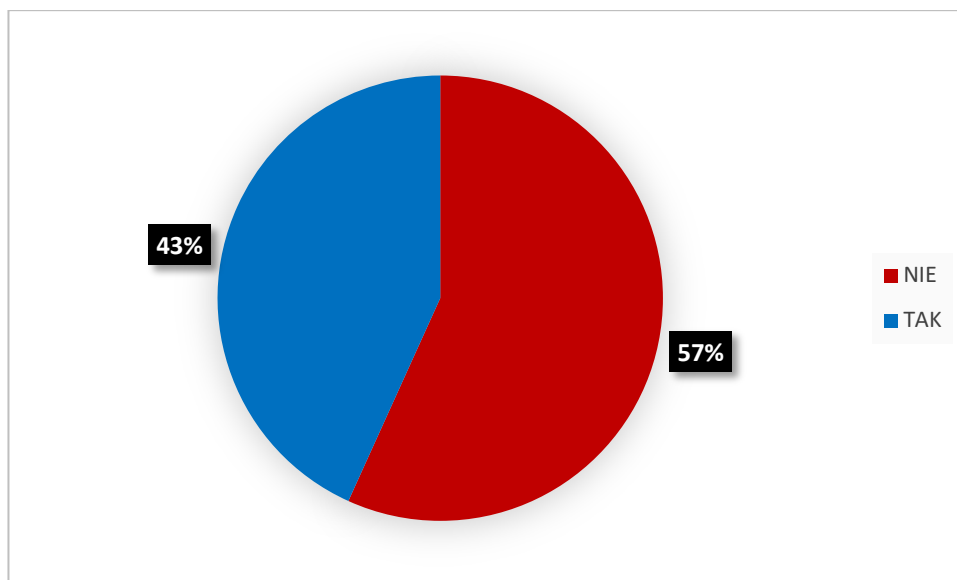


Z przedstawionych wyników wynika, że w praktyce tylko 2% szpitali może doświadczyć ryzyka zatrzymania realizacji świadczeń medycznych. Jest to grupa oznaczona kolorem szarym, w której ponad połowa sprzętu pochodzi spoza UE i NATO. Z kolei 43% szpitali może mieć problem z utrzymaniem niezakłóconej ciągłości prowadzenia działalności leczniczej, gdyż w tej grupie sprzęt spoza UE i NATO stanowi między 30% a 50% zasobów.

Podsumowując, można założyć, że w przypadku uznania producentów sprzętu pochodzącego z państwa spoza UE i NATO za dostawców wysokiego ryzyka, 45% szpitali może borykać się z różnej skali problemami utrzymania efektywności i liczby świadczonych procedur medycznych na poziomie sprzed wydania takiej decyzji.

Odmienne wygląda natomiast sytuacja w przypadku oprogramowania dostarczanego przez podmioty spoza UE i NATO. Z wyników przeprowadzonej ankiety wynika, że 57% szpitali nie widzi możliwości wymiany i zastąpienia go wyłącznie oprogramowaniem firm z państw UE i NATO.

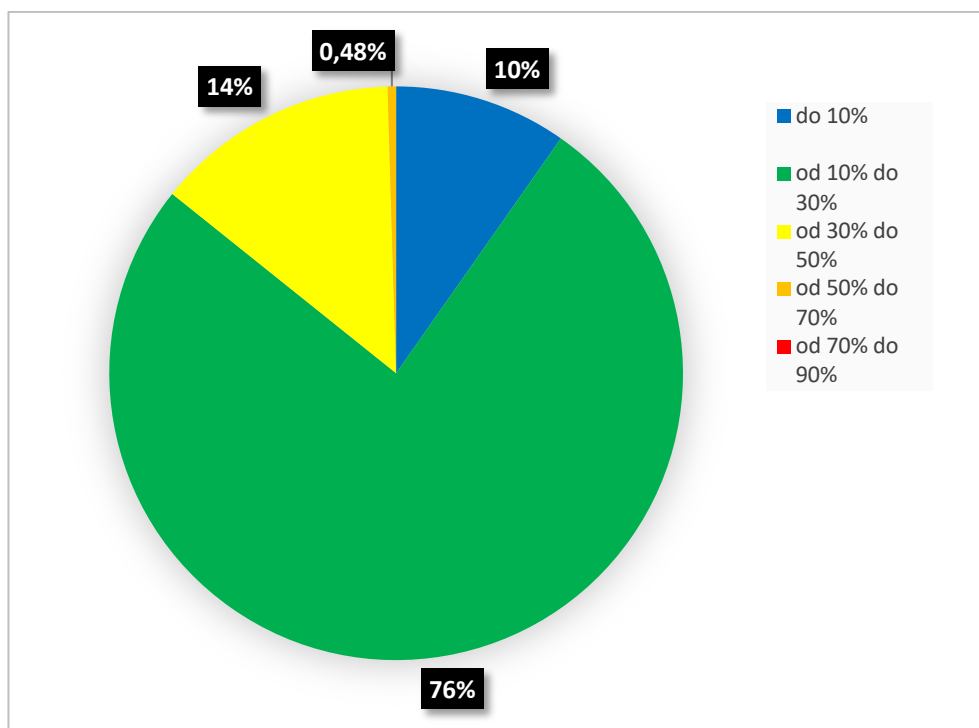
Wykres nr 4 – Odpowiedzi udzielone na pytanie: Czy Pani/Pana zdaniem istnieje realna możliwość wymiany powyższego oprogramowania i zastąpienie go wyłącznie oprogramowaniem od producentów pochodzących z państw Unii Europejskiej i NATO?



Wskaźnik na poziomie blisko 60% należy uznać za obiektywnie wysoki, jednak najprawdopodobniej nie wywoła bardzo dużego wpływu organizacyjnego na szpitale, ponieważ jedynie 0,5% ankietowanych wskazało, że w swoich zasobach informatycznych posiada powyżej 50% oprogramowania³ dostawców spoza UE i NATO, a 86% stwierdziło, że takie oprogramowanie nie stanowi więcej niż 30% całości takich zasobów. Szczegółowe dane z podziałem procentowym zostały zaprezentowane na poniższym wykresie.

³ W ujęciu wartości wykorzystywanego oprogramowania spoza UE i NATO w stosunku do całego posiadanego oprogramowania.

Wykres nr 5 – Odpowiedzi udzielone na pytanie: Jaka jest procentowa wartość wykorzystanego oprogramowania (w tym programów komputerowych, aplikacji, sterowników, silników bazodanowych etc., niezależnie od formy posiadania – własność produktów, licencje, subskrypcje itp.) pochodzącego od producentów z państw spoza Unii Europejskiej i NATO w stosunku do całego posiadanego oprogramowania?



Z powyższych danych wynika, że w przypadku decyzji o uznaniu producentów oprogramowania pochodzących spoza UE i NATO za dostawców wysokiego ryzyka, konieczność jego wymiany nie powinna negatywnie wpłynąć na realizowane procesy i procedury medyczne. Jedynie dla około 0,5% podmiotów, może wywołać to realne zakłócenie w prowadzeniu działalności leczniczej.

Podstawowym celem analizy była próba udzielenia odpowiedzi na pytanie w jaki sposób wejście w życie nowelizacji ustawy KSC wpłynie na aspekt finansowy prowadzonej przez szpitale działalności leczniczej, precyzując – czy nastąpi wzrost kosztów, a jeżeli tak, to szacunkowo o jaką kwotę. Ze względu, że dane podlegające analizie opierają się na pytaniach ankietowych, poza procesem szacowania kosztów pozostają inne czynniki kosztotwórcze zawarte w projekcie ustawy, m.in. wprowadzenie odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych⁴. Raport skupia się wyłącznie

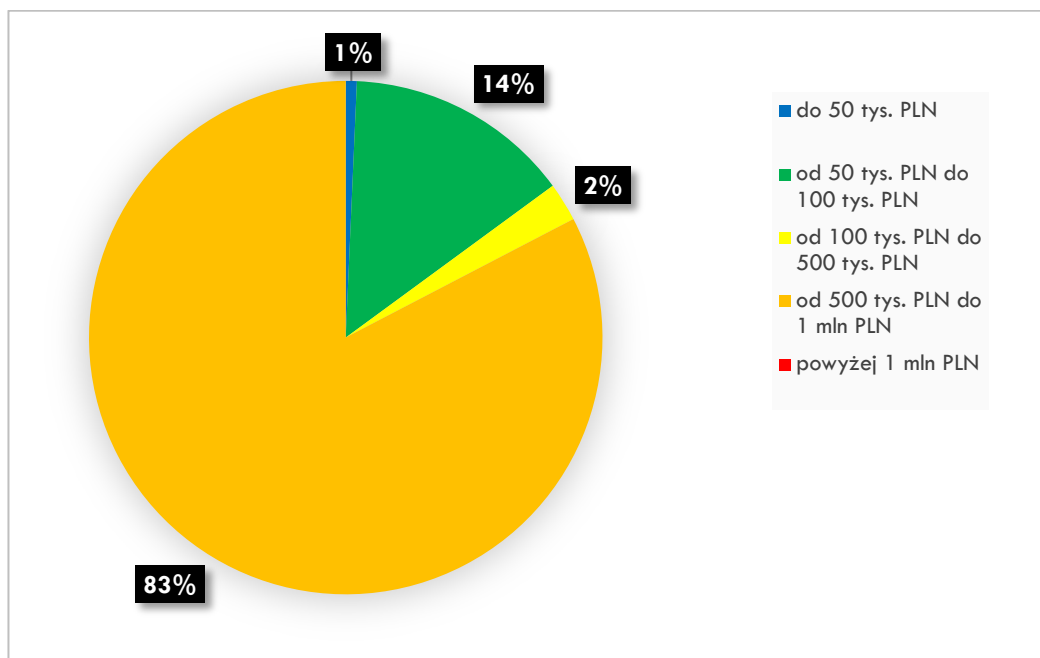
⁴ Obejmują one m.in.: politykę analizy ryzyka i bezpieczeństwa systemów informatycznych, zarządzanie incydentami, opracowanie planu ciągłości działania oraz zarządzania kryzysowego, bezpieczeństwo łańcucha dostaw,

na oszacowaniu kosztów, które będą ponosić szpitale w związku z ewentualnymi decyzjami ministra właściwego ds. informatyzacji w przedmiocie uznania producentów sprzętu i oprogramowania za dostawców wysokiego ryzyka, co w konsekwencji będzie prowadziło do konieczności wycofania ich produktów z organizacji i zastąpienia ich nowymi rozwiązaniami.

Analiza ww. kosztów, ze względu na inną specyfikę produktową, składa się z dwóch elementów, badanych niezależnie od siebie – szacowanych kosztów wymiany sprzętu oraz kosztów wymiany oprogramowania. Ponadto dla obu elementów przeanalizowano koszty serwisu i wsparcia technicznego, gdyż tego typu usługi również objęte są różnymi politykami sprzedażowymi, często powiązanymi z praktykami stosowanymi w kraju producenta.

Z udzielonych przez ankietowane szpitale odpowiedzi wynika, że 83% z nich uważa, iż koszt wymiany sprzętu będzie w przedziale od 500 tys. PLN do 1 mln PLN, a 14% twierdzi, że będzie to kwota w przedziale od 50 tys. PLN do 100 tys. PLN. Pełne dane prezentuje poniższy wykres.

Wykres nr 6 – Odpowiedzi udzielone na pytanie: Jeżeli TAK to: czy Pani/Pana zdaniem koszt netto wymiany sprzętu teleinformatycznego, urządzeń elektronicznych, maszyn (koszt wymiany jest rozumiany jako zakup nowych urządzeń, utylizacja wymienianych oraz usługa demontażu i instalacji nowych urządzeń) będzie na poziomie?



W toku procesu analitycznego, podjęto decyzję, aby zaprezentowane na powyższym wykresie dane przeliczyć z wykorzystaniem funkcji średniej ważonej, co umożliwi uzyskanie reprezentatywnej kwoty z tego badania. Proces obliczenia średniej ważonej dla prezentowanych na wykresie danych rozpoczęto od wyliczenia średniej arytmetycznej dla wszystkich pięciu przedziałów kwotowych. Poniższa tabela zawiera wyniki przeliczenia.

Tabela nr 6 – Wyniki średniej arytmetycznej dla przedziałów kwotowych z pytania nr 10

przedział kwotowy z pytania nr 7	średnia arytmetyczna
do 50 tys. PLN	25000 PLN
od 50 tys. PLN do 100 tys. PLN	75000 PLN
od 100 tys. PLN do 500 tys. PLN	300000 PLN
od 500 tys. PLN do 1 mln PLN	750000 PLN
powyżej 1 mln PLN	1100000 PLN ⁵

Następnie podanym w tabeli uśrednionym kwotom przypisano wagę odpowiadającą wartościom procentowym dla odpowiedniego przedziału kwotowego z wykresu nr 6. W ostatnim etapie tak przygotowane dane, ułożone w tabeli, przeliczono z wykorzystaniem formuły w programie MS Excel⁶. W ten sposób otrzymano średnią ważoną, którą należy interpretować przez pryzmat celów analizy, czyli jako szacunkowy koszt wymiany sprzętu. W poniższej tabeli zaprezentowano wyniki obliczenia średniej ważonej.

Tabela nr 7 – Wyniki średniej ważonej dla kosztów wymiany sprzętu

przedział kwotowy z pytania nr 10 ⁷	Waga - procent udzielonych odpowiedzi	średnia kwota w PLN
do 50 tys. PLN	1%	25000
od 50 tys. PLN do 100 tys. PLN	14%	75000
od 100 tys. PLN do 500 tys. PLN	2%	300000
od 500 tys. PLN do 1 mln PLN	83%	750000
średnia arytmetyczna		287500
średnia ważona		639250

⁵ Dla przedziału powyżej 1 mln tys. PLN nie da się utworzyć średniej ze względu na brak określonej kwoty „do”.

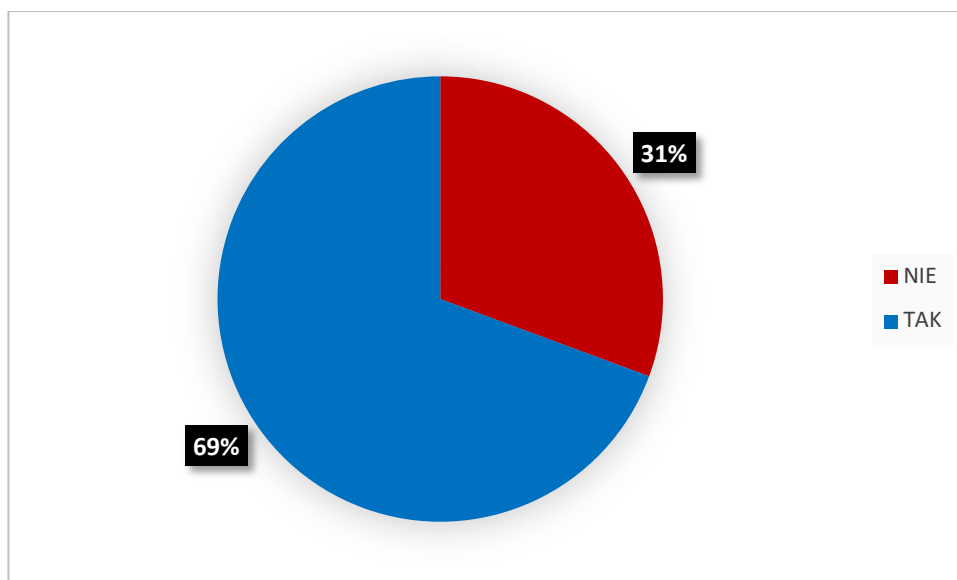
Tym samym przyjęto ostrożnościowy współczynnik dla dalszego procesu szacowania.

⁶ Formuła dla tej tabeli to =SUMA.ILOCZYNÓW(C2:C5;B2:B5)/SUMA(B2:B5)

⁷ W tabeli pominięto przedział powyżej 1 mln PLN, gdyż w pytaniu nr 10 liczba odpowiedzi dla tego przedziału wynosiła 0.

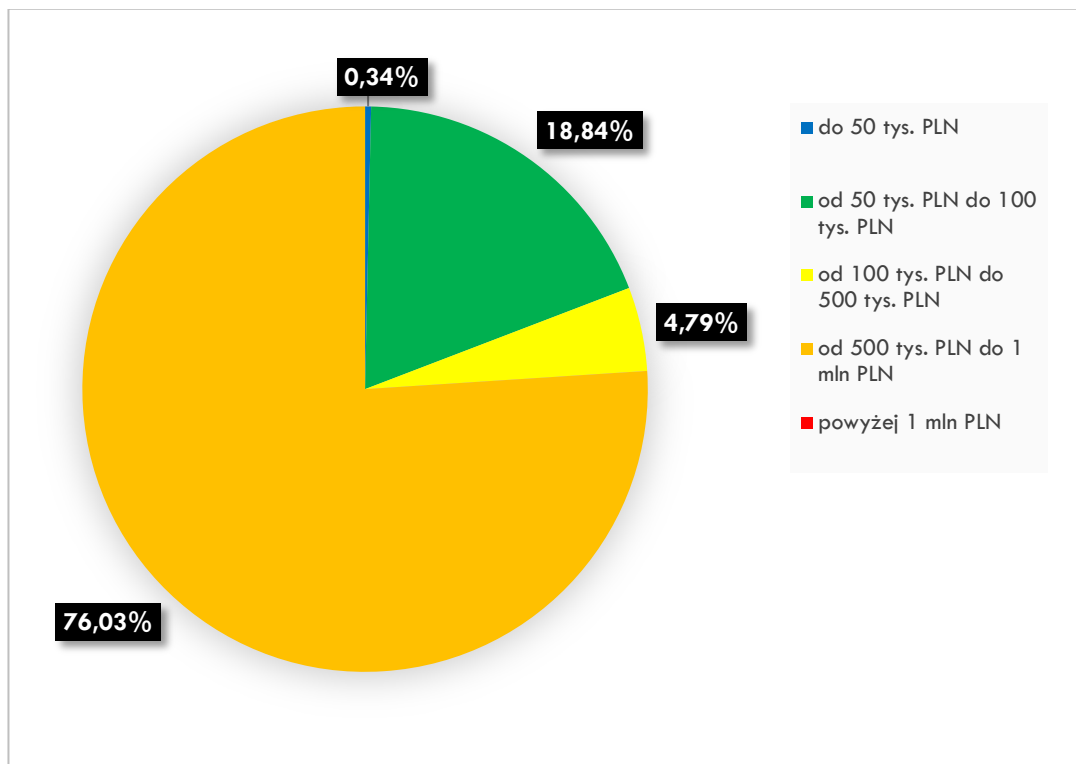
W celu oszacowania całościowych kosztów związanych z wymianą sprzętu, należało także przeanalizować koszty serwisu i wsparcia technicznego dla tych urządzeń. W tym przypadku 69% ankietowanych wskazało, że wymiana sprzętu będzie wiązać się ze wzrostem kosztów. Wyniki zapytania zostały zaprezentowane na poniższym wykresie.

Wykres nr 7 – Odpowiedzi udzielone na pytanie: Czy Pani/Pana zdaniem wymiana posiadanego sprzętu teleinformatycznego, urządzeń elektronicznych, maszyn na sprzęt pochodzący wyłącznie od producentów z państw Unii Europejskiej i NATO będzie wiązała się z większymi kosztami serwisu i wsparcia technicznego?



Z udzielonych przez ankietowane szpitale odpowiedzi wynika, że 76% z nich uważa, iż koszt serwisu i wsparcia technicznego wzrośnie w przedziale od 500 tys. PLN do 1 mln PLN, a 19% podmiotów twierdzi, że wzrost wyniesie od 50 tys. PLN do 100 tys. PLN. Pełne dane zostały zaprezentowane na poniższym wykresie.

Wykres nr 8 – Odpowiedzi udzielone na pytanie: Jeżeli TAK to: będzie to kwota netto na poziomie?



Ponownie, aby móc oszacować wzrost kosztów serwisu i wsparcia technicznego dla wymienionego sprzętu, należało wyliczyć średnią ważoną z powyższych odpowiedzi. Proces przebiegał analogicznie do opisanego szczegółowo przy kosztach wymiany sprzętu, więc w tym miejscu zostaną zaprezentowane jedynie tabelaryczne wyniki dokonywanych obliczeń.

Tabela nr 8 – Wyniki średniej arytmetycznej dla przedziałów kwotowych z pytania nr 19

przedział kwotowy z pytania nr 19	średnia arytmetyczna
do 50 tys. PLN	25000 PLN
od 50 tys. PLN do 100 tys. PLN	75000 PLN
od 100 tys. PLN do 500 tys. PLN	300000 PLN
od 500 tys. PLN do 1 mln PLN	750000 PLN
powyżej 1 mln PLN	1100000 PLN

Tabela nr 9 – Wyniki średniej ważonej dla kosztów serwisu i wsparcia technicznego sprzętu

przedział kwotowy z pytania nr 19 ⁸	Waga - procent udzielonych odpowiedzi	średnia kwota w PLN
do 50 tys. PLN	0,34%	25000
od 50 tys. PLN do 100 tys. PLN	18,84%	75000
od 100 tys. PLN do 500 tys. PLN	4,79%	300000
od 500 tys. PLN do 1 mln PLN	76,03%	750000
średnia arytmetyczna		287500
średnia ważona⁹		598810

Podsumowując, całkowite koszty związane z koniecznością wymiany sprzętu producenta uznanego za dostawcę wysokiego ryzyka w jednym szpitalu można oszacować na poziomie 1 238 060 PLN netto¹⁰ w pierwszym roku, natomiast w przeciągu 5 lat¹¹ kwota ta może wynosić 3 633 300 PLN netto¹².

Drugim elementem badania wpływu nowelizacji ustawy KSC na aspekt finansowy prowadzonej przez szpitale działalności leczniczej jest analiza kosztów związanych z wymianą oprogramowania oraz usług jego serwisu i wsparcia technicznego.

Z udzielonych przez ankietowane podmioty odpowiedzi wynika, że 69% z nich uważa, iż koszt wymiany oprogramowania będzie w przedziale od 500 tys. PLN do 1 mln PLN, a 26% twierdzi, że będzie to kwota w przedziale od 50 tys. PLN do 100 tys. PLN. Pełne dane prezentuje poniższy wykres.

⁸ W tabeli pominięto przedział od 1 mln PLN, gdyż w pytaniu nr 19 liczba odpowiedzi dla tego przedziału wynosiła 0.

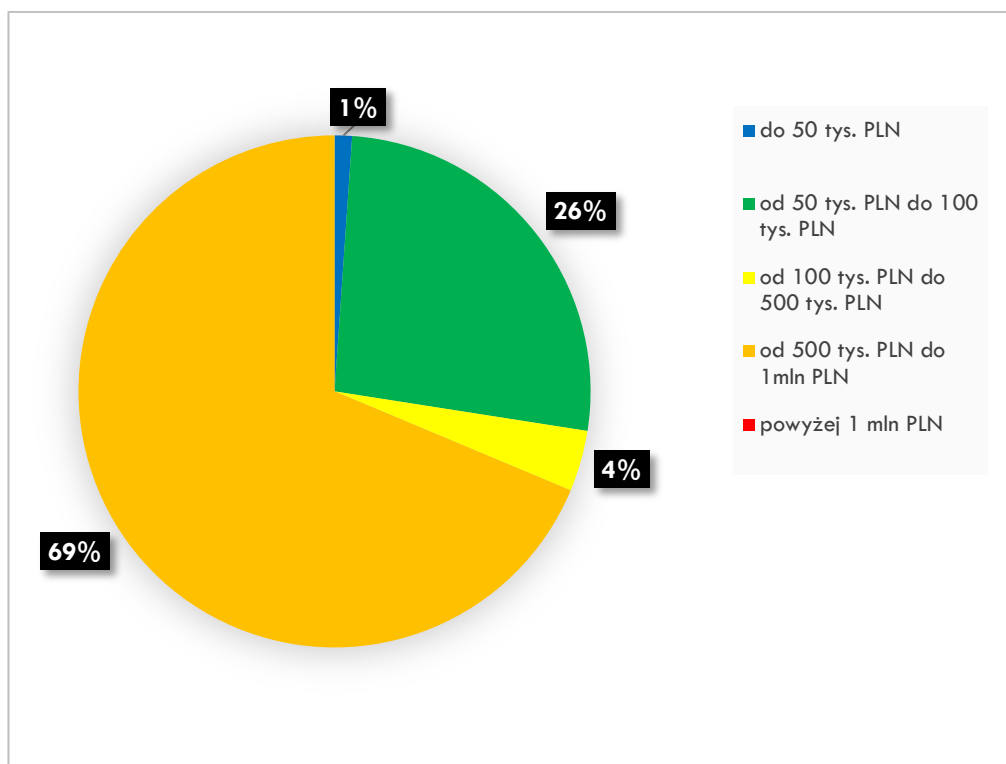
⁹ Formuła dla tej tabeli to =SUMA.ILOCZYNÓW(C2:C5;B2:B5)/SUMA(B2:B5)

¹⁰ Suma średniego kosztu wymiany sprzętu z tabeli nr 7 i średniego rocznego kosztu serwisu z tabeli nr 9.

¹¹ Przyjęto okres o połowę krótszy niż wymaga się na potrzeby szacowania kosztów w Ocenie Skutków Regulacji, gdyż w szóstym roku najprawdopodobniej pojawią się i tak pewne dodatkowe inwestycje związane z koniecznością wymiany, naprawy czy modernizacji posiadanego sprzętu. To z kolei będzie miało wpływ zarówno na koszty sprzętu jak i jego serwisu. Podobny punkt widzenia został zaprezentowany w uzasadnieniu do projektu nowelizacji. Tam autorzy wskazali, że średni cykl życia urządzenia wynosi od 5 do 10 lat.

¹² Suma średniego kosztu wymiany sprzętu z tabeli nr 7 i pięciokrotności średniego rocznego kosztu serwisu z tabeli nr 9.

Wykres nr 9 – Odpowiedzi udzielone na pytanie: Jeżeli TAK to: czy Pani/Pana zdaniem koszt netto wymiany oprogramowania (koszt wymiany jest rozumiany jako zakup nowego oprogramowania oraz usługi deinstalacji oraz instalacji, konfiguracji i wdrożenia nowego, a także migracji danych z wycofywanych systemów do nowych systemów IT) będzie na poziomie?



Dla oszacowania kosztów wymiany oprogramowania ponownie posłużono się metodą wyliczania średniej ważonej, analogicznie jak w przypadku obliczenia kosztów wymiany sprzętu. Poniższa tabela zawiera wyniki tego przeliczenia.

Tabela nr 10 – Wyniki średniej arytmetycznej dla przedziałów kwotowych z pytania nr 13

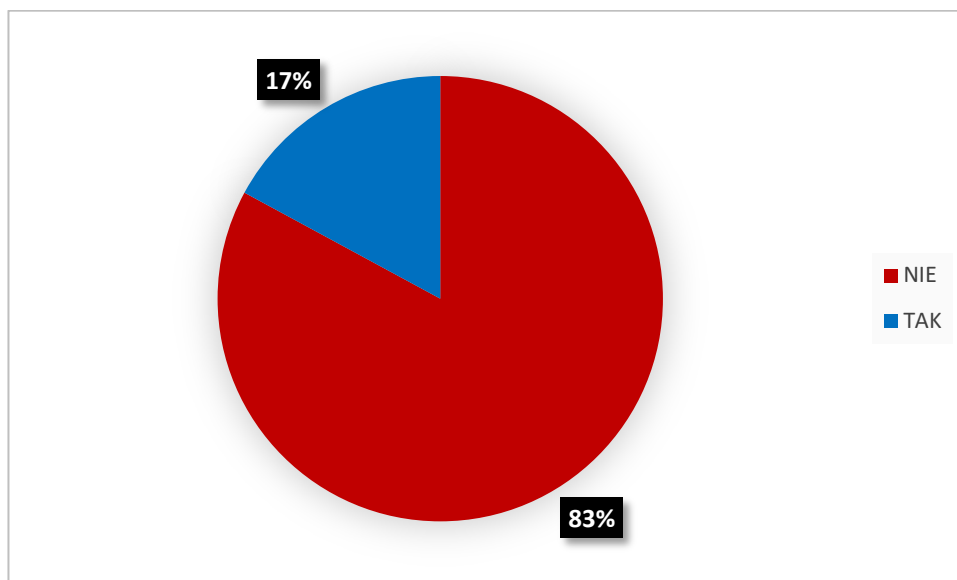
przedział kwotowy z pytania nr 13	średnia arytmetyczna
do 50 tys. PLN	25000 PLN
od 50 tys. PLN do 100 tys. PLN	75000 PLN
od 100 tys. PLN do 500 tys. PLN	300000 PLN
od 500 tys. PLN do 1 mln PLN	750000 PLN
powyżej 1 mln PLN	1100000 PLN

Tabela nr 11 – Wyniki średniej ważonej dla kosztów wymiany oprogramowania

przedział kwotowy z pytania nr 13 ¹³	Waga - procent udzielonych odpowiedzi	średnia kwota w PLN
do 50 tys. PLN	1%	25000
od 50 tys. PLN do 100 tys. PLN	26%	75000
od 100 tys. PLN do 500 tys. PLN	4%	300000
od 500 tys. PLN do 1 mln PLN	69%	750000
średnia arytmetyczna		287500
średnia ważona¹⁴		549250

Następnie powtórzono proces analityczny dla oszacowania wzrostu kosztów związanych z usługą serwisu i wsparcia technicznego oprogramowania. W tym przypadku 17% ankietowanych stwierdziło, że według nich taki wzrost nastąpi.

Wykres nr 10 – Odpowiedzi udzielone na pytanie: Czy Pani/Pana zdaniem wymiana posiadanego oprogramowania na oprogramowanie pochodzące wyłącznie od producentów z państw Unii Europejskiej i NATO będzie wiązała się z większymi kosztami serwisu i wsparcia technicznego?



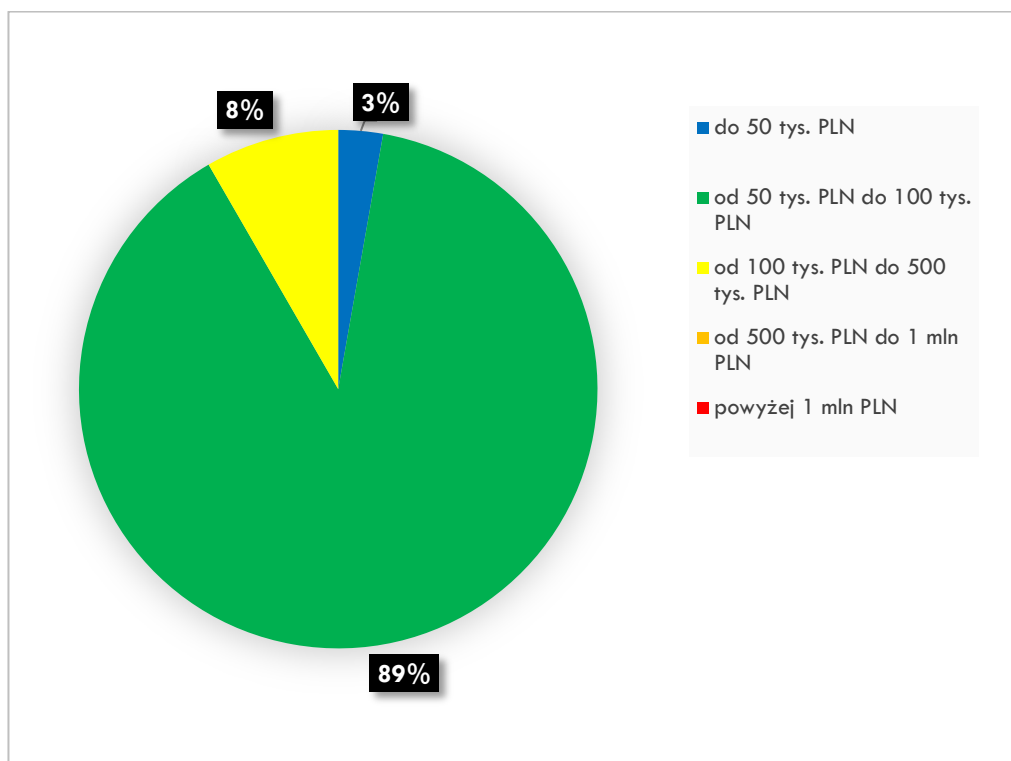
Z udzielonych przez ankietowane szpitale odpowiedzi wynika, że 89% z nich uważa, iż koszt serwisu i wsparcia technicznego oprogramowania wzrośnie w przedziale od 50

¹³ W tabeli pominięto przedział od 1 mln PLN, gdyż w pytaniu nr 13 liczba odpowiedzi dla tego przedziału wynosiła 0.

¹⁴ Formuła dla tej tabeli to =SUMA.ILOCZYNÓW(C2:C5;B2:B5)/SUMA(B2:B5)

tys. PLN do 100 tys. PLN, 8%, że będzie to w przedziale od 100 tys. PLN do 500 tys. PLN, a 3% twierdzi, że koszt nie przekroczy 50 tys. PLN.

Wykres nr 11 – Odpowiedzi udzielone na pytanie: Jeżeli TAK to: będzie to kwota netto na poziomie?



Do oszacowania kosztów serwisu i wsparcia technicznego dla wymienionego oprogramowania, wykorzystano formułę wyliczenia średniej ważonej z powyższych odpowiedzi. Poniżej zaprezentowano tabelaryczne wyniki wykonanych obliczeń.

Tabela nr 12 – Wyniki średniej arytmetycznej dla przedziałów kwotowych z pytania nr 21

przedział kwotowy z pytania nr 21	średnia arytmetyczna
do 50 tys. PLN	25000 PLN
od 50 tys. PLN do 100 tys. PLN	75000 PLN
od 100 tys. PLN do 500 tys. PLN	300000 PLN
od 500 tys. PLN do 1 mln PLN	750000 PLN
powyżej 1 mln PLN	1100000 PLN

Tabela nr 13 – Wyniki średniej ważonej dla kosztów serwisu i wsparcia technicznego oprogramowania

przedział kwotowy z pytania nr 21 ¹⁵	Waga - procent udzielonych odpowiedzi	średnia kwota w PLN
do 50 tys. PLN	3%	25000
od 50 tys. PLN do 100 tys. PLN	89%	75000
od 100 tys. PLN do 500 tys. PLN	8%	300000
średnia arytmetyczna		133333
średnia ważona¹⁶		91500

Podsumowując, całkowite koszty związane z koniecznością wymiany oprogramowania producenta uznanego za dostawcę wysokiego ryzyka w jednym szpitalu można oszacować na poziomie 640 750 PLN netto¹⁷ w pierwszym roku, natomiast w przeciągu 5 lat kwota ta może wynosić 1 006 750 PLN netto¹⁸.

Z przeprowadzonej analizy szacowania kosztów związanych z koniecznością wymiany produktów i usług pochodzących od dostawców wysokiego ryzyka, w przypadku wydania decyzji administracyjnej w pełnym zakresie, wynika, że łączna kwota dla jednego szpitala w pięcioletnim okresie może wynieść **4 640 050 PLN netto**.

Ostatni blok pytań ankietowych dotyczył koordynowanej ochrony zdrowia. Odpowiedzi były udzielane przez wszystkie 421 szpitali biorących udział w badaniu. Celem pierwszego pytania było ustalenie skali realizowanej przez szpitale opieki koordynowanej w ramach umowy z NFZ. Szczegółowe dane w ujęciu liczbowym prezentuje poniższy wykres.

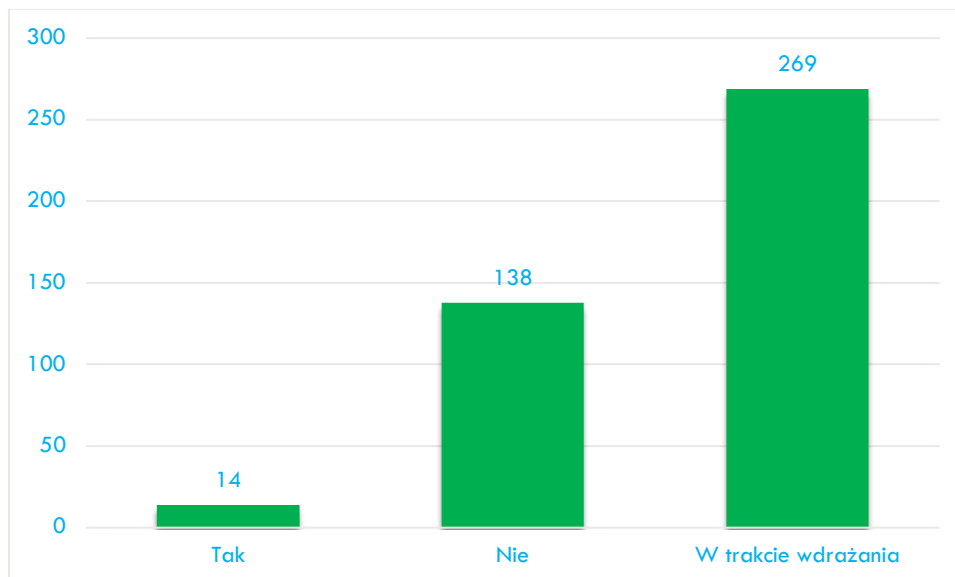
¹⁵ W tabeli pominięto przedziały od 500 tys. PLN do 1 mln PLN oraz od 1 mln PLN, gdyż w pytaniu nr 21 liczba odpowiedzi dla tych przedziałów wynosiła 0.

¹⁶ Formuła dla tej tabeli to =SUMA.ILOCZYNÓW(C2:C4;B2:B4)/SUMA(B2:B4)

¹⁷ Suma średniego kosztu wymiany oprogramowania z tabeli nr 11 i średniego rocznego kosztu serwisu z tabeli nr 13.

¹⁸ Suma średniego kosztu wymiany sprzętu z tabeli nr 11 i pięciokrotności średniego rocznego kosztu serwisu z tabeli nr 13.

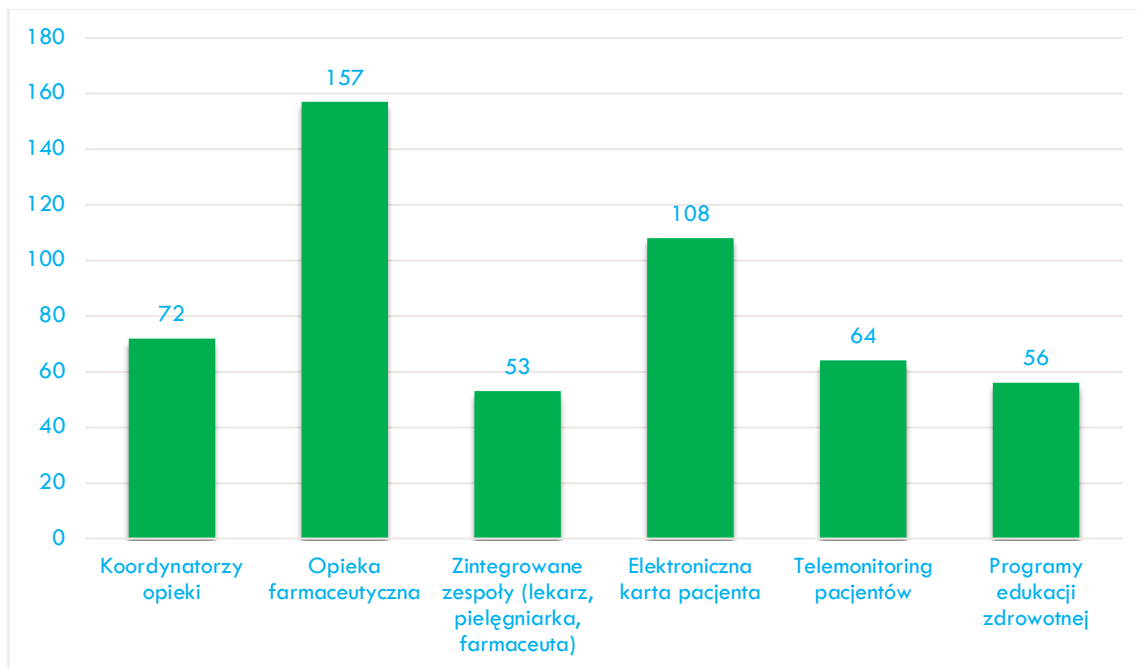
Wykres nr 12 – Odpowiedzi udzielone na pytanie: Czy szpital realizuje opiekę koordynowaną w ramach umowy z NFZ?



Uzyskane wyniki mogą budzić pewien niepokój, gdyż jedynie 3% szpitali realizuje tego typu opiekę, a 63% jest dopiero w fazie jej wdrażania.

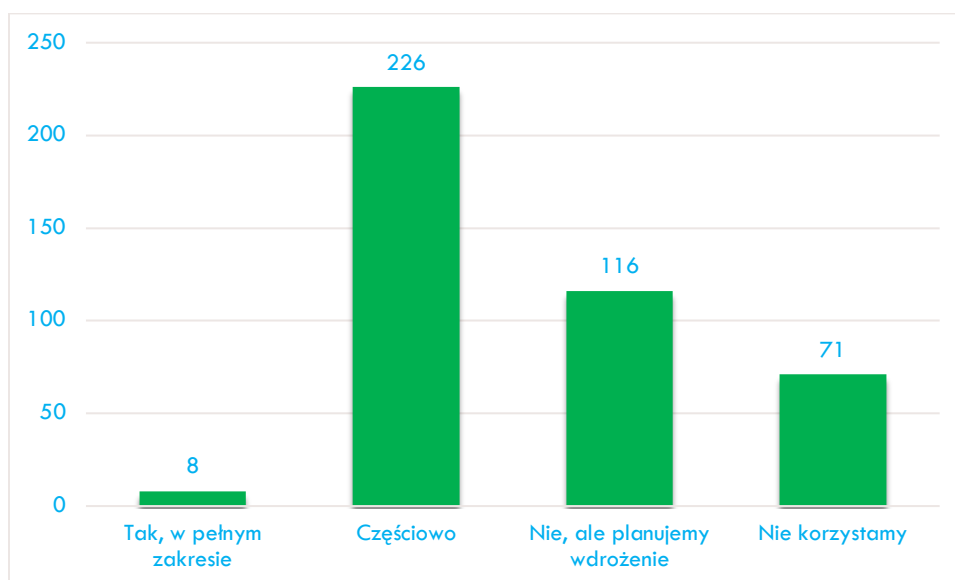
Kolejne pytanie miało za zadanie ustalić jakie konkretnie rodzaje opieki koordynowanej realizowane są przez szpitale. Było to pytanie wielokrotnego wyboru, tak aby umożliwić podmiotom leczniczym wybór dowolnego zestawu odpowiedzi, tym samym poszczególne szpitale wskazywały od 1 do 6 elementów opieki obecnie realizowanych. Istotne jest także to, że z grupy 421 szpitali aż 134 wskazały, że to pytanie ich nie dotyczy. Poniżej zostały zaprezentowane pełne dane liczbowe.

Wykres nr 13 – Odpowiedzi udzielone na pytanie: Jakie elementy opieki koordynowanej są obecnie realizowane przez szpital?

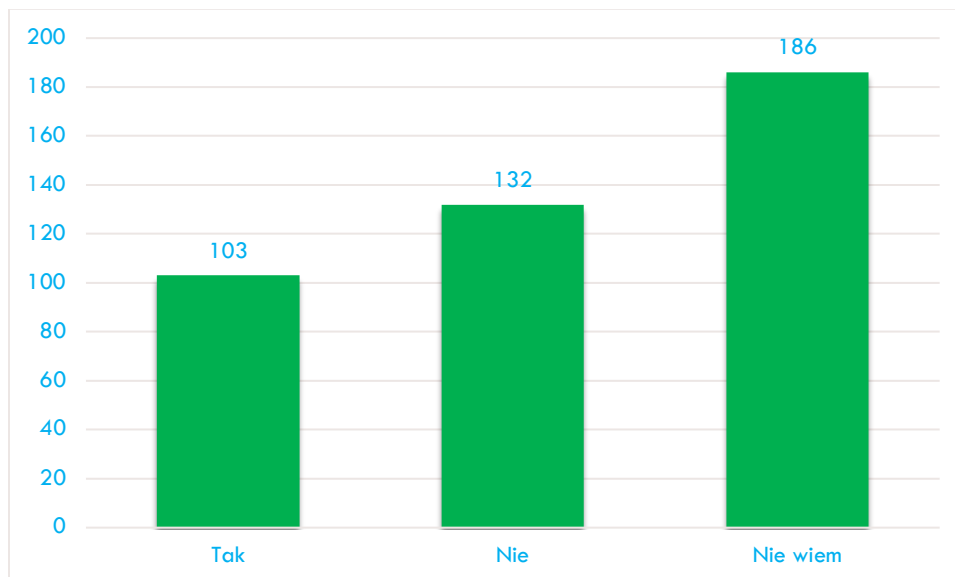


W ramach obszaru Technologia i bezpieczeństwo cyfrowe, zostały sformułowane trzy pytania jednokrotnego wyboru. Poniżej zostały przygotowane wykresy prezentujące udzielone odpowiedzi w ujęciu liczbowym.

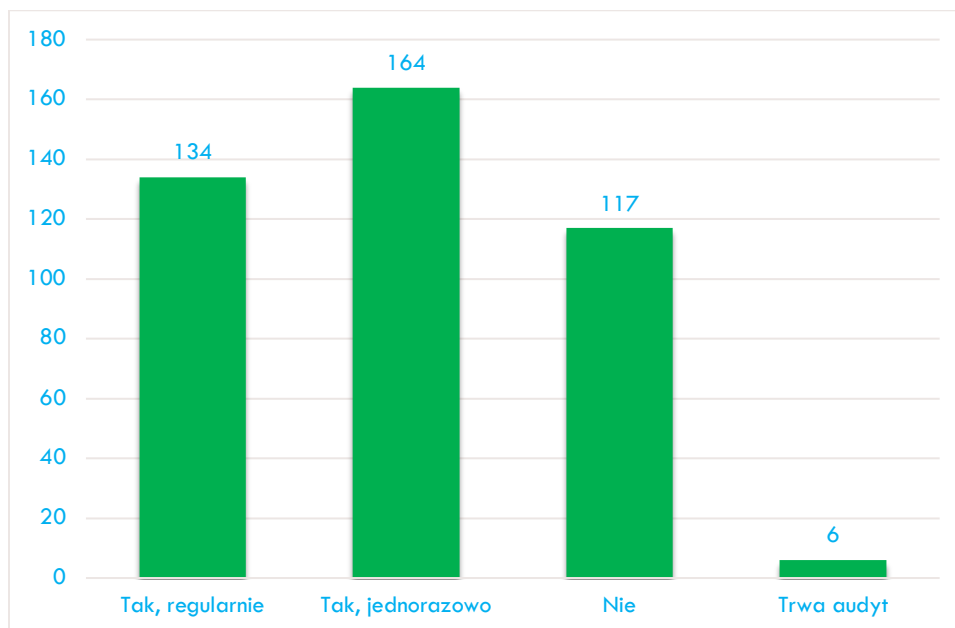
Wykres nr 14 – Odpowiedzi udzielone na pytanie: Czy szpital korzysta z systemu IT wspierającego opiekę koordynowaną (np. integracja EHR, system kolejkowy, zarządzanie terapią)?



Wykres nr 15 – Odpowiedzi udzielone na pytanie: Czy systemy wspierające KOZ są zgodne z wymaganiami cyberbezpieczeństwa przewidzianymi w nowelizacji ustawy o KSC?



Wykres nr 16 – Odpowiedzi udzielone na pytanie: Czy szpital przeprowadził analizę ryzyk w zakresie cyberbezpieczeństwa systemów wykorzystywanych w opiece koordynowanej?

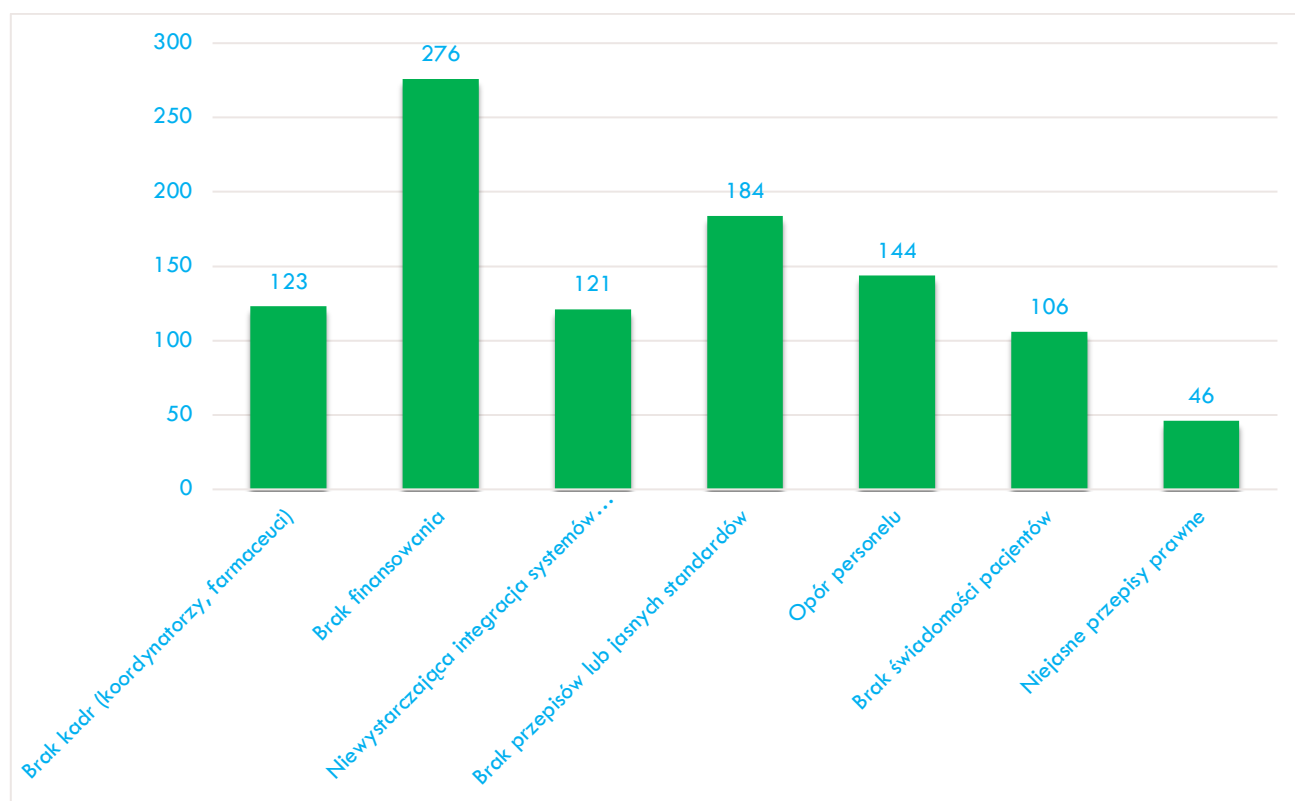


Powyższe dwa pytania mają bezpośrednie połączenie z pierwszą częścią raportu dotyczącą wpływu nowelizacji KSC na szpitale w Polsce. W tym kontekście 24% pozytywnych odpowiedzi udzielonych na pytanie dotyczące zgodności systemów KOZ

z wymaganiami cyberbezpieczeństwa przewidzianymi w nowelizacji KSC wzmacnia sformułowane wnioski o niskiej świadomości szpitali wpływu tej nowelizacji na bieżącą działalność podmiotów leczniczych. Z danych wynika również, że jedynie 31% szpitali przeprowadza regularnie analizę ryzyk w zakresie cyberbezpieczeństwa. To wprost wskazuje na zakres prac i wyzwań stojących przed szpitalami, po wejściu w życie omawianej nowelizacji KSC.

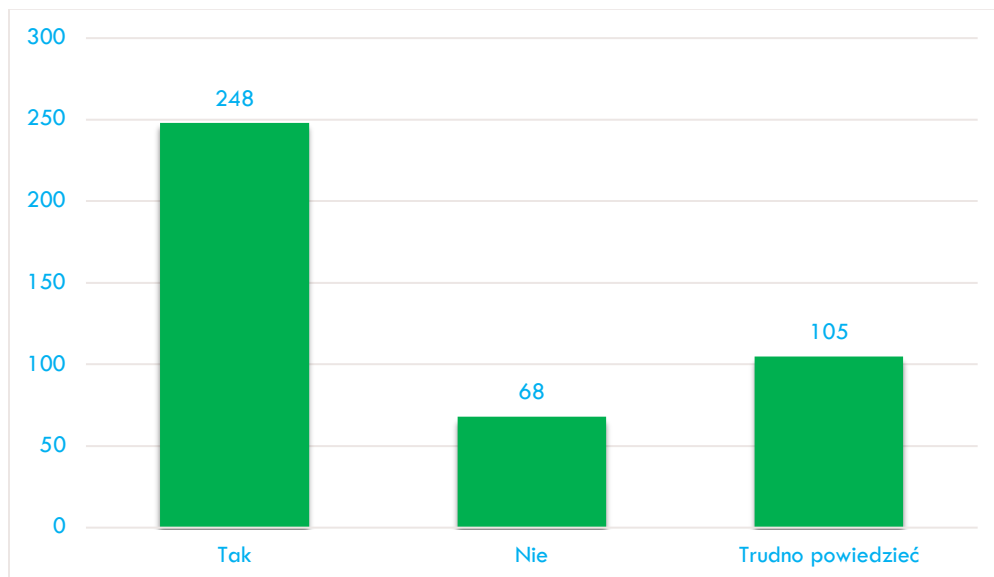
Ostatnie trzy pytania dotyczyły obszaru wyzwań i potrzeb szpitali objętych badaniem ankietowym. W pierwszym z nich odnoszącym się do barier utrudniających wdrażanie opieki koordynowanej przygotowano zestaw siedmiu możliwych odpowiedzi. Ponownie możliwe było dokonanie wielokrotnego wyboru. Szczegółowe dane prezentuje poniższy wykres.

Wykres nr 17 – Odpowiedzi udzielone na pytanie: Jakie bariery utrudniają Państwa szpitalowi skuteczne wdrażanie opieki koordynowanej?

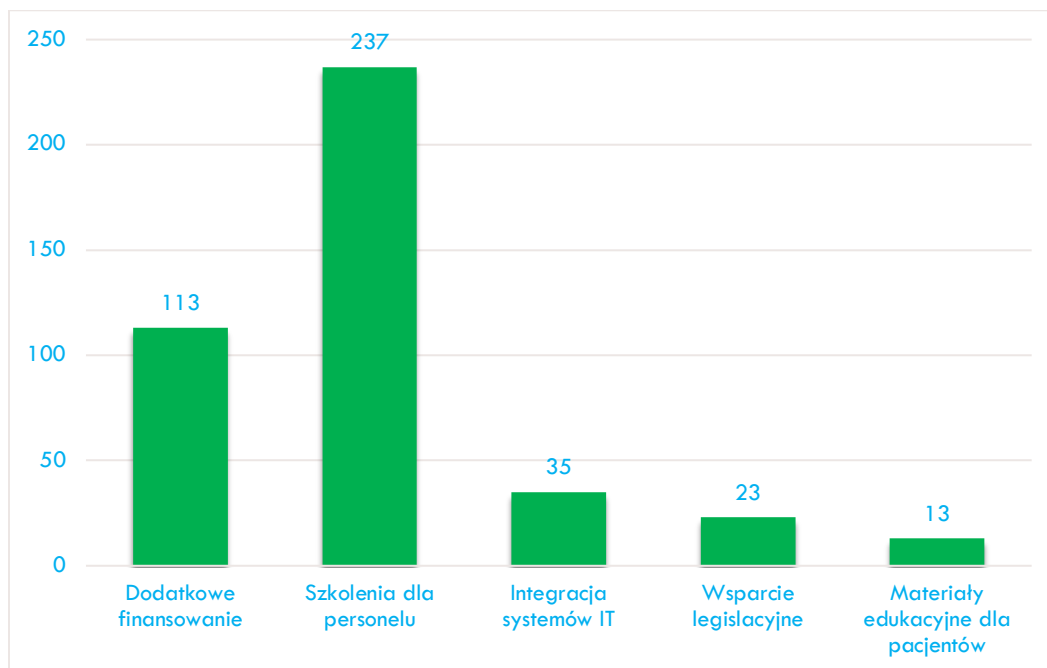


Pozostałe dwa pytania zawierały zestawy odpowiedzi jednokrotnego wyboru. Wykresy prezentują udzielone odpowiedzi w ujęciu liczbowym.

Wykres nr 18 – Odpowiedzi udzielone na pytanie: Czy szpital planuje rozszerzenie zakresu opieki koordynowanej w ciągu najbliższych 12 miesięcy?



Wykres nr 19 – Odpowiedzi udzielone na pytanie: Jakie wsparcie byłoby najbardziej pomocne przy wdrażaniu/rozwoju KOZ?



Jak widać z powyższego wykresu przeważająca większość udzielonych odpowiedzi dotyczy szkoleń dla personelu. Takiego wsparcia oczekuje aż 56% wszystkich szpitali.

Wsparcie finansowe jest dopiero na drugim miejscu. Takie oczekiwania posiada około 27% podmiotów leczniczych.

OPIEKA KOORDYNOWANA W SZPITALACH PUBLICZNYCH

Obok analizy skutków finansowych i organizacyjnych nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa, istotnym elementem przeprowadzonych badań była ocena stanu wdrożenia opieki koordynowanej (KOZ) w polskich szpitalach publicznych. Ten model organizacji świadczeń zdrowotnych, wpisany w strategię rozwoju systemu ochrony zdrowia w Polsce, ma kluczowe znaczenie dla poprawy jakości leczenia pacjentów, zapewnienia ciągłości terapii i efektywnego wykorzystania zasobów.

Rozwój KOZ wymaga jednak nie tylko odpowiednich zmian organizacyjnych i finansowych, ale również wdrożenia zaawansowanych systemów informatycznych oraz zapewnienia im wysokiego poziomu cyberbezpieczeństwa. Wyniki ankiety przeprowadzonej wśród 421 szpitali pozwalają szczegółowo określić aktualny stan wdrożeń KOZ, główne bariery rozwojowe oraz oczekiwania placówek wobec systemu ochrony zdrowia.

Skala wdrożenia KOZ

Zdecydowana większość placówek – **63%** – była w fazie wdrażania elementów KOZ, natomiast aż **34%** nie prowadziło żadnych działań w tym obszarze.

Tak niski poziom zaawansowania w pełnym wdrożeniu KOZ wskazuje na znaczące opóźnienia względem założeń systemowych oraz potwierdza, że transformacja organizacyjna szpitali wymaga znacznie szerszego wsparcia niż obecnie.

Zakres realizowanych elementów KOZ

Placówki, które realizują KOZ, wdrażają zazwyczaj wybrane elementy tego modelu, rzadziej pełny pakiet rozwiązań. Najczęściej stosowane są:

- koordynacja leczenia pacjentów przewlekłe chorych,
- prowadzenie programów profilaktycznych,
- organizacja ścieżki pacjenta z uwzględnieniem zarządzania kolejkami i integracji z systemem EHR.

Zauważalna jest jednak duża różnorodność – od placówek implementujących pojedyncze rozwiązania, po te, które wprowadzają kompleksowe modele, często pilotażowo lub w ramach ograniczonej grupy pacjentów.

Technologie wspierające KOZ

Technologia jest fundamentem koordynowanej opieki zdrowotnej, jednak raport wskazuje na poważne niedostatki w tym zakresie. Tylko **24% szpitali** zadeklarowało, że ich systemy IT wspierające KOZ spełniają wymagania cyberbezpieczeństwa określone w projekcie nowelizacji ustawy o KSC.

Jeszcze bardziej niepokojący jest fakt, że zaledwie **31% szpitali** przeprowadza regularne analizy ryzyk związanych z bezpieczeństwem systemów informatycznych wykorzystywanych w KOZ. Oznacza to, że większość placówek wdraża rozwiązania technologiczne bez właściwej oceny zagrożeń, co w kontekście ochrony danych medycznych pacjentów i ciągłości świadczeń jest poważnym problemem.

Bariery we wdrażaniu KOZ

Szpitale jednoznacznie wskazują, że największą przeszkodą w rozwoju opieki koordynowanej jest **brak odpowiedniego przeszkolenia personelu** – problem ten zidentyfikowało **56% ankietowanych placówek**. Drugą kluczową barierą jest **niewystarczające finansowanie**, które wymienia **27% szpitali**.

Pozostałe bariery dotyczą m.in. braku interoperacyjnych systemów IT, trudności organizacyjnych, a także ograniczeń związanych z integracją procesów klinicznych. Wyniki te potwierdzają, że KOZ jest nie tylko wyzwaniem technologicznym i budżetowym, ale przede wszystkim organizacyjnym i kompetencyjnym.

Oczekiwane wsparcie

Na pytanie o to, jaka forma wsparcia byłaby najbardziej pomocna przy wdrażaniu i rozwoju KOZ, szpitale najczęściej wskazywały **szkolenia dla personelu** – tę odpowiedź wybrało **56% placówek**. Na drugim miejscu znalazło się **wsparcie finansowe** (27%). Mniej wskazań dotyczyło doradztwa organizacyjnego czy wsparcia w zakresie infrastruktury IT.

Wynik ten pokazuje, że dyrekcje szpitali postrzegają rozwój KOZ przede wszystkim jako wyzwanie związane z kompetencjami i kulturą organizacyjną, a dopiero w drugiej kolejności jako problem stricte finansowy.

SZCZEGÓŁOWE WNIOSKI I PODSUMOWANIE KOŃCOWE

1. Koszty nadregulacji wynikającej z nowelizacji ustawy KSC nie zostały odpowiednio zwymiarowane w aspekcie finansowym. W Ocenie Skutków Regulacji można jedynie odnaleźć potwierdzenie, że projektodawca ma świadomość zwiększenia nakładów finansowych, które będą musiały ponosić szpitale, jednak nie podjął trudu ich pełnego oszacowania. Przewidziano jedynie wpływ na jednostki sektora finansów publicznych w zakresie kosztów funkcjonowania CSIRT, wynagrodzeń dla dodatkowych pracowników, w tym składek na ubezpieczenia społeczne, Fundusz Pracy, Fundusz Solidarnościowy, PPK, kosztów stanowisk pracy oraz kosztów zakupu licencji do norm technicznych i innych dokumentów standaryzacyjnych z zakresu cyberbezpieczeństwa. Przeprowadzona analiza pokazuje jednak, że oszacowanie potencjalnych skutków finansowych dla szpitali jest możliwe, a także mieralne.
2. Większość szpitali, na które bezpośrednio będą oddziaływać przepisy nowelizacji KSC nie posiada takiej świadomości. Potwierdza to także wynik przeprowadzonej ankiety, w której 78% podmiotów wskazało, że nie są mu znane konsekwencje związane w wejściem w życie tej nowelizacji.
3. W przypadku podmiotów leczniczych, nowelizacja ustawy KSC przewiduje, że za podmioty kluczowe i ważne zostaną uznane te placówki, które zatrudniają co najmniej 50 pracowników. Z tego powodu należy przyjąć, że wszystkie szpitale w Polsce będą mieć taki status i zostaną objęte nowoprojektowanymi regulacjami.
4. Na podstawie wyników ankiety można przyjąć założenie, że decyzja o uznaniu za dostawcę wysokiego ryzyka podmiotów spoza UE i NATO, które zajmują się produkcją sprzętu ICT nie powinna spowodować w skali ogólnopolskiej znaczących problemów z utrzymaniem bieżącej działalności przez podmioty lecznicze. 68% ankietowanych stwierdziło, że istnieje możliwość wymiany tych urządzeń na sprzęt pochodzący wyłącznie z państw UE i NATO.
5. W oparciu o zebrane na podstawie ankiet dane dotyczące potencjalnych kosztów wymiany sprzętu i oprogramowania pochodzącego od dostawców wysokiego ryzyka, a także kosztów związanych z serwisem i wsparciem technicznym dla nowo zakupionych produktów pochodzących od firm z terenu UE i NATO można przyjąć, że szacunkowa kwota dla jednego szpitala publicznego może wynieść 4,6 mln PLN netto w pięcioletniej perspektywie. W tej kwocie zawarty jest szacunkowy koszt zakupu nowych produktów, koszt deinstalacji starych i instalacji nowych urządzeń, koszt

utylicacji zdemontowanego sprzętu oraz koszty pięcioletniej usługi serwisu i wsparcia technicznego. Należy także zaznaczyć, że oszacowana kwota ma zastosowanie wyłącznie w przypadku kumulatywnego zbiegu decyzji administracyjnych o uznaniu za dostawców wysokiego ryzyka wszystkich producentów sprzętu i oprogramowania, których produkty są wykorzystywane przez poszczególne szpitale.

6. W oparciu o wyliczoną szacunkową kwotę kosztów jakie może ponieść pojedynczy podmiot leczniczy, można także oszacować przybliżony skutek finansowy dla wszystkich szpitali publicznych. Według danych Polskiego Towarzystwa Koordynowanej Ochrony Zdrowia w Polsce jest obecnie około 800 szpitali publicznych, co po przemnożeniu przez wartość finansową skutku dla jednego podmiotu daje kwotę około 3,7 mld PLN netto w pięcioletniej perspektywie.
7. Należy pamiętać, że przedmiotem analizy była jedynie próba oszacowania wzrostu kosztów dla szpitali publicznych wynikających z możliwych decyzji administracyjnych ministra właściwego ds. informatyzacji w przedmiocie dostawców wysokiego ryzyka. Tym samym poza badaniem kosztów pozostały potencjalne wydatki szpitali prywatnych, a także inne obciążenia i obowiązki wynikające z ustawy, takie jak obowiązek wprowadzenia systemu zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych, czy wykonywanie okresowych audytów. To będzie mieć również bezpośredni wpływ na organizację pracy i koszty funkcjonowania podmiotów leczniczych.
8. Analiza danych ankietowych pokazuje, że poziom wdrożenia opieki koordynowanej w polskich szpitalach publicznych jest obecnie bardzo niski. Zdecydowana większość, bo aż 63%, jest dopiero w fazie wdrażania. Tak niski odsetek wdrożeń w pełnym zakresie wskazuje, że pomimo strategicznego znaczenia KOZ w polityce zdrowotnej, w praktyce jej implementacja napotyka na liczne bariery organizacyjne, technologiczne i finansowe.
9. Szczegółowa analiza barier ujawniła, że największym wyzwaniem jest niedostateczne przygotowanie personelu – aż 56% szpitali wskazało na potrzebę szkoleń jako kluczowy warunek skutecznego wdrożenia KOZ. Na drugim miejscu znalazł się brak odpowiedniego finansowania (27%), co potwierdza, że nawet najlepiej przygotowany personel nie będzie w stanie wdrożyć nowych standardów bez zapewnienia stabilnych źródeł finansowania. Pozostałe bariery dotyczyły głównie ograniczeń infrastrukturalnych i problemów organizacyjnych, co łączy się bezpośrednio z wyzwaniami w obszarze technologii i cyberbezpieczeństwa.

10. W kontekście narzędzi IT wspierających opiekę koordynowaną sytuacja również wymaga poprawy. Zaledwie 24% systemów stosowanych w szpitalach spełnia wymogi cyberbezpieczeństwa określone w nowelizacji ustawy o KSC. Co więcej, tylko 31% szpitali przeprowadza regularne analizy ryzyk w obszarze systemów informatycznych wykorzystywanych do KOZ. Dane te jednoznacznie wskazują, że większość placówek nie jest przygotowana ani technicznie, ani organizacyjnie do prowadzenia koordynowanej opieki w zgodzie z nowymi standardami prawnymi.
11. Szpitale mają jasno sprecyzowane oczekiwania wobec wsparcia zewnętrznego. Najczęściej wskazywaną potrzebą są szkolenia dla personelu – aż 56% placówek oczekuje takiej formy pomocy. Dopiero na drugim miejscu znalazło się wsparcie finansowe (27%). Ten wynik pokazuje, że problem wdrażania KOZ ma charakter przede wszystkim kompetencyjny i organizacyjny, a nie wyłącznie budżetowy.
12. Pełna realizacja KOZ dotyczy jedynie marginalnego odsetka placówek (3%), co oznacza, że cele systemowe w tym zakresie są dalekie od osiągnięcia i tym samym widać wyraźne opóźnienia we wdrożeniach.
13. Najczęściej wskazywaną przeszkodą są braki w przygotowaniu personelu. Jest to problem systemowy, który wymaga rozwiązań ogólnokrajowych.
14. Systemy IT wspierające KOZ są w większości niezgodne z wymaganiami cyberbezpieczeństwa, a brak analiz ryzyk naraża szpitale na potencjalne incydenty.
15. Wyniki ankiet pokazują, że kompetencje personelu są uznawane za kluczowy czynnik sukcesu. Z tego też powodu szpitale wskazują szkolenia jako najczęściej oczekiwaną formę wsparcia.
16. Opieka koordynowana w polskich szpitalach jest wciąż na bardzo wczesnym etapie rozwoju. Wyniki ankiety wskazują, że placówki mają świadomość jej znaczenia, ale borykają się z poważnymi ograniczeniami organizacyjnymi i kompetencyjnymi. Największym wyzwaniem okazuje się brak przygotowanego personelu i brak wiedzy o tym, jak KOZ wdrażać w praktyce. Jest to szczególnie istotne w kontekście równoległych wymogów wynikających z nowelizacji ustawy o KSC. Bez zapewnienia cyberbezpieczeństwa systemów IT wspierających KOZ i bez inwestycji w kompetencje kadry, rozwój tego modelu będzie nie tylko opóźniony, ale i obciążony poważnymi ryzykami organizacyjnymi.
17. Wdrożenie opieki koordynowanej w Polsce stoi przed trzema równoległymi wyzwaniami:

- a. Kompetencyjnym – brak wystarczającego przeszkolenia personelu stanowi największą barierę rozwoju KOZ
- b. Technologicznym – systemy IT w większości nie spełniają wymogów bezpieczeństwa i nie wspierają w pełni procesów koordynacji.
- c. Finansowym – choć nie jest to bariera numer jeden, brak dedykowanych środków budżetowych znacząco ogranicza tempo wdrożeń.

18. Raport pokazuje wyraźnie, że aby koordynowana opieka zdrowotna mogła stać się realnym filarem systemu, konieczne są: szkolenia, inwestycje w cyfryzację, poprawa bezpieczeństwa IT oraz dedykowane wsparcie finansowe. Tylko wtedy KOZ będzie mogła spełnić swoją rolę – poprawić ciągłość leczenia, zwiększyć efektywność terapii i zapewnić pacjentom poczucie bezpieczeństwa.

19. Bez kompleksowego programu wsparcia – obejmującego szkolenia, inwestycje w infrastrukturę cyfrową oraz dopasowane mechanizmy finansowania – szpitale publiczne nie będą w stanie skutecznie rozwijać koordynowanej opieki zdrowotnej. To z kolei przełoży się na ograniczoną możliwość realizacji strategicznych celów systemu ochrony zdrowia, takich jak poprawa ciągłości leczenia, efektywności terapii oraz satysfakcji pacjenta.



URSZULA SZYBOWICZ
IRENEUSZ WOCHLIK