



Raport z badania

przeprowadzonego wśród przedsiębiorców telekomunikacyjnych
w zakresie kosztów wymiany sprzętu i oprogramowania
dostawców spoza UE i NATO w przypadku zastosowania
mechanizmu dostawcy wysokiego ryzyka

STRUKTURA OPRACOWANIA

WSTĘP	03
I. KLUCZOWE USTALENIA I WNIOSKI	04
II. KONTEKST SPRAWY	04
III. CELE ANALIZY	08
IV. MATERIAŁY ŹRÓDŁOWE	08
V. WYNIKI ANALIZY	08
VI. SZCZEGÓŁOWE WNIOSKI I PODSUMOWANIE KOŃCOWE	20

O IZBIE

Krajowa Izba Komunikacji Ethernetowej (KIKE) istnieje od 2008 roku, kiedy grupa lokalnych operatorów z całej Polski postanowiła zawiązać formalną współpracę pod postacią izby gospodarczej.

Celem KIKE jest wspieranie rodzimego rynku telekomunikacyjnego w sektorze mikro, małych i średnich przedsiębiorców.

Zrzeszamy polskich lokalnych operatorów telekomunikacyjnych, którzy dostarczają przewodowy internet szerokopasmowy konsumentom, przedsiębiorcom, instytucjom publicznym, głównie na wschodzie i południu kraju.





Krajowa Izba Komunikacji Ethernetowej (KIKE) z dużym zaangażowaniem śledzi i stara się wspierać prace nad kolejnymi wersjami nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (KSC).

Od początku tych prac członkowie KIKE są zaniepokojeni możliwymi finansowymi skutkami regulacji, w szczególności w zakresie tzw. dostawcy wysokiego ryzyka (DWR). Decyzja DWR wiąże się bowiem z nakazem wycofania z użytkowania sprzętu wskazanego w takiej decyzji w ciągu 4 lub 7 lat od daty jej wydania, bez odszkodowania.

Szacowanie możliwych skutków takiej decyzji nie zostało dokonane przez projektodawcę na etapie prac nad projektem nowelizacji. Z kolei procedura wydawania decyzji DWR nie przewiduje obowiązku analizy tej kwestii przez organ z urzędu.

Niepokój ma zatem oczywistą przyczynę: nakaz wycofania z użytkowania sprzętu i oprogramowania, gdy odbywa się bez odszkodowania i to przed upływem okresu amortyzacji (dla urządzeń aktywnych w telekomunikacji okres ten wynosi 10 lat), stanowi kosztowną ingerencję w swobodę działalności gospodarczej. Co więcej, w opinii przygotowanej na zlecenie KIKE, prof. Ryszard Piotrowski (WPIA UW) wskazał m.in. że

„[...] regulacja nie przewiduje przyznania odszkodowania z tytułu usunięcia sprzętu lub oprogramowania, co jest równoznaczne z pozbawieniem własności przysługującej podmiotom zobowiązanym na mocy ustawy, a więc z wywłaszczeniem na cele publiczne. Jest to niezgodne z art. 21 ust. 2 Konstytucji, w myśl którego wywłaszczenie jest dopuszczalne, jedynie wówczas, gdy jest dokonywane na cele publiczne i za słusznym odszkodowaniem¹.”

Profesor stwierdził również, że rozwiązanie DWR narusza zakaz nadmiernej ingerencji wbrew zasadzie proporcjonalności stanowiących ograniczeń.

W związku z powyższym, bardzo ważne jest budowanie świadomości wśród przedstawicieli administracji publicznej oraz przedsiębiorców na temat skali skutków finansowych potencjalnego nakazu usuwania sprzętu i oprogramowania.

Nie znamy zakresu sprzętu i oprogramowania, który może być w przyszłości objęty nakazem, ani listy dostawców, którzy być może zostaną uznani za DWR. Nie wiemy również, jakie podmioty odczułyby faktyczne skutki decyzji DWR. Ten katalog może być szerszy niż tylko podmioty formalnie zobowiązane do usuwania sprzętu i oprogramowania, ponieważ sieci telekomunikacyjne i – szerzej – rynek telekomunikacyjny – stanowią system naczyń połączonych. Szacowanie skali problemu jest jednak możliwe.

Z konstrukcji przepisów nowelizacji KSC wynika, że próg usunięcia sprzętu dostawców spoza UE i NATO będzie niższy niż w przypadku pozostałych dostawców. W przypadku dostawców spoza UE i NATO projekt zawiera więcej przesłanek - w porównaniu z dostawcami z UE i NATO - które mogą pozwolić na uznanie ich za DWR. W związku z powyższym postanowiliśmy zbadać stopień wykorzystania sprzętu i oprogramowania tej właśnie kategorii dostawców przez przedsiębiorców, których zrzeszamy, czyli mikro, małych i średnich przedsiębiorców telekomunikacyjnych. W ramach wypełniania ankiet na potrzeby naszego badania, przedsiębiorcy zostali również zapytani, czy w ich ocenie istnieje realna alternatywa dla sprzętu i oprogramowania pochodzących od dostawców spoza UE oraz NATO.

Niniejsze opracowanie przedstawia wyniki naszej analizy.

Karol Skupień



Prezes Krajowej Izby Komunikacji Ethernetowej

1. Dr hab. Ryszard Piotrowski (Wydział Prawa i Administracji Uniwersytetu Warszawskiego) Opinia o zgodności wybranych przepisów projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych ustaw z Konstytucją RP, Warszawa 12 czerwca 2025 r. <https://kike.pl/2025/06/prof-piotrowski-przepisy-dwr-niezgodne-z-konstytucja/>

I. KLUCZOWE USTALENIA I WNIOSKI

Przeprowadzone przez Krajową Izbę Komunikacji Ethernetowej badanie ankietowe, w połączeniu z analizą pozyskanych w ten sposób danych, pokazuje, że oszacowanie skali potencjalnych skutków finansowych nakazu usuwania sprzętu i oprogramowania przez firmy z branży komunikacji elektronicznej jest możliwe, a także mierzalne.

W przeprowadzonej akcji ankietowej wzięło udział 152 przedsiębiorców należących do segmentu mikro, małych i średnich (MŚP) przedsiębiorców telekomunikacyjnych. Z Oceny Skutków Regulacji, opracowanej i dołączonej przez Ministerstwo Cyfryzacji do projektu nowelizacji KSC wynika, że projekt ten będzie miał wpływ na 3332 podmioty wpisane do rejestru przedsiębiorców telekomunikacyjnych. Tym samym uzyskane wyniki można uznać za reprezentatywne i miarodajne dla przedsiębiorców telekomunikacyjnych, należących do podsektora komunikacji elektronicznej.

Analiza informacji zawartych w ankietach wskazuje, że przedstawiciele branży mają nadal niską świadomość konsekwencji i skutków finansowych wejścia w życie projektowanej nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa dla prowadzenia działalności gospodarczej i świadczenia usług.

Z przeprowadzonej analizy szacowania kosztów wymiany sprzętu i oprogramowania pochodzących od dostawców spoza UE i NATO wynika, że łączne koszty takiej wymiany dla jednego przedsiębiorcy mogą wynieść 4,3 mln zł netto w pięcioletnim okresie. Koszty dla wszystkich przedsiębiorców telekomunikacyjnych mogłyby zatem wynieść 14,4 mld zł netto w ciągu pięciu lat.

W związku z tym, że obecnie ponad 80% badanych przedsiębiorców telekomunikacyjnych posiada w swoich zasobach infrastrukturalnych ponad 50% sprzętu pochodzącego od dostawców spoza UE i NATO, ewentualna konieczność usunięcia całego takiego sprzętu i oprogramowania, mogłaby prowadzić do zaburzenia lub w skrajnym przypadku zatrzymania ciągłości świadczonych usług przez tę grupę przedsiębiorców.

II. KONTEKST SPRAWY

Analiza została wykonana w oparciu o projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (KSC) (druk sejmowy nr 1955), po I czytaniu w Sejmie RP, które odbyło się 5 grudnia 2025 r. Przygotowany przez Ministerstwo Cyfryzacji projekt transponuje do krajowego porządku prawnego tzw. dyrektywę NIS2, czyli dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148. Ponadto, wdraża on również rozwiązania wynikające z wytycznych ujętych w dokumencie 5G Toolbox.

Rozwiązania ujęte w projekcie nowelizacji KSC rozszerzają znacznie zakres regulacji w porównaniu z dyrektywą NIS2 oraz z **wytocznymi 5G Toolbox²**, co stanowi tzw. nadregulację. Rozwiązania wynikające z 5G Toolbox zostały rozszerzone na 18 sektorów gospodarki, zamiast poprzestać na elementach krytycznych w sieciach telekomunikacyjnych 5G.

Tak rozszerzone 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:

SEKTORY KLUCZOWE	
sektor	podsektor
energia	wydobywanie kopalin
	energia elektryczna
	ciepło
	gaz
	energetyka jądrowa
	wodór
transport	transport lotniczy
	transport kolejowy
	transport wodny
	transport drogowy
ochrona zdrowia	Udzielanie świadczeń zdrowotnych i zdrowie publiczne
	Produkcja i dystrybucja substancji czynnych, produktów leczniczych i wyrobów medycznych
Bankowość i infrastruktura rynków finansowych	
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 publiczne³	

2. Prof. dr hab. Artur Nowak-Far (SGH), PORÓWNANIE MODELI WYKONANIA DYREKTYWY NIS 2 W WYBRANYCH PAŃSTWACH CZŁONKOWSKICH UNII EUROPEJSKIEJ: W AUSTRII, CZECHACH, FINLANDII, IRLANDII, NIEMCZACH, SŁOWACJI, SŁOWENII, NA WĘGRZACH I WE WŁOSZACH. Ekspertyza przygotowana dla Polskiego Towarzystwa Gospodarczego, Stan prawny: 15 sierpnia 2025 r. https://iptg.pl/wp-content/uploads/2026/01/Opinia-o-wykonaniu-NIS2_2-FINAL_ANE.pdf

3. Przede wszystkim w zakresie organów władzy publicznej oraz urzędów je obsługujących, sądów i trybunałów, jednostek budżetowych, szeregu instytucji o zasięgu ogólnopolskim, wiele jednostek budżetowych i zakładów budżetowych na poziomie wojewódzkim, starostwa powiatowe, niektóre urzędy gminy.

SEKTORY WAŻNE	
sektor	podsektor
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
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
Inwestycje energetyki jądrowej	
Produkcja, wytwarzanie i dystrybucja chemikaliów	
Produkcja, przetwarzanie i dystrybucja żywności	
Usługi pocztowe	
Dostawcy usług cyfrowych	
Badania naukowe	
<i>Podmioty publiczne⁴</i>	

Należy także wskazać, że podmiotami kluczowymi, co do zasady, będą firmy działające w sektorze kluczowym, większe niż średnie. Z kolei podmiotami ważnymi będą przedsiębiorstwa średnie, działające w sektorze kluczowym, lub co najmniej średnie, działające w sektorze ważnym. Projekt przewiduje jednak wiele wyjątków, m.in. dla podsektora komunikacji elektronicznej. Przedsiębiorca komunikacji elektronicznej, w tym przedsiębiorca telekomunikacyjny, będzie podmiotem kluczowym już po osiągnięciu progu przedsiębiorcy średniego. Wszyscy pozostali przedsiębiorcy z tego podsektora będą podmiotami ważnymi. Istnieje również szereg innych kategorii przedsiębiorców mikro i małych, które zostaną objęte nowelizacją. Liczba podmiotów, która zostanie obciążona obowiązkami regulacyjnymi, jak wynika z Oceny Skutków Regulacji (OSR), wynosi ok. 42 000.

Na szczególną uwagę zasługuje kwestia tzw. dostawcy wysokiego ryzyka (DWR). Projekt ustawy określa go jako dostawcę sprzętu lub oprogramowania, które są wykorzystywane przez, co do zasady, podmioty kluczowe i ważne, jeżeli dostawca ten stanowi zagrożenie dla podstawowego interesu bezpieczeństwa państwa. Decyzja DWR zawiera wskazanie typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania uwzględnionych w postępowaniu w sprawie uznania za DWR.

4. Jedynie w zakresie samorządowych jednostek budżetowych, zakładów budżetowych i instytucji kultury oraz spółek wykonujące zadania o charakterze użyteczności publicznej.

Zaliczenie dostawcy do tej kategorii, w ramach procedury określonej w nowelizacji, opiera się m.in. na opinii sporządzanej przez Kolegium do Spraw Cyberbezpieczeństwa.

Opinia powinna obejmować aspekty techniczne (m.in. historia wykrytych incydentów bezpieczeństwa czy 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 (operatorzy telekomunikacyjnych sieci ruchomych, w zakresie sprzętu i oprogramowania pełniących wskazane w nowelizacji funkcje) lub 7 lat (**pozostałe podmioty**⁵).

To z kolei będzie prowadzić do poniesienia przez te podmioty znacznych nakładów finansowych na zakup nowych produktów i usług oraz ich wdrożenie w swojej organizacji.

Jednocześnie warto podkreślić, że rzeczywiste oddziaływanie decyzji DWR może wykraczać poza jej ramy. Nawet podmioty, które nie będą formalnie zobowiązane prawnie do usuwania sprzętu i oprogramowania DWR, mogą zostać do tego zmuszone pośrednio, ponieważ rynek telekomunikacyjny jest zespołem naczyń połączonych i nie działa w próżni.

Odnosząc się do podsektora komunikacja elektroniczna, który został zaliczony do sektorów kluczowych, opracowana przez Ministerstwo Cyfryzacji OSR wskazuje, że nowelizacja ustawy będzie miała wpływ na co najmniej **3332**⁶ podmiotów. OSR odwołuje się w tym zakresie do rejestru przedsiębiorców telekomunikacyjnych..

OSR – w kontekście skutków finansowych – prezentuje jedynie wpływ na sektor finansów publicznych. W sekcji pt. „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 (dotyczących nowych obowiązków w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz zgłaszania incydentów do właściwych CSIRT sektorowych, a także obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka), 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.

5. Podmioty kluczowe i ważne (przy czym w przypadku przedsiębiorców komunikacji elektronicznych, wyłącznie przedsiębiorcy, których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej są wyższe od kwoty 10 milionów złotych) oraz podmioty finansowe, z wyłączeniem podmiotów określonych w art. 16 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011.

6. Na etapie rządowego procesu legislacyjnego liczba ta wynosiła 3784. Dodatkowo OSR nie zawiera danych w stosunku do podmiotów świadczących usługę komunikacji interpersonalnej niewykorzystującej numerów (OTT-1).

III. CELE ANALIZY

W związku z tym, że projektodawca nie przygotował na potrzeby OSR nawet szacunkowych danych dotyczących kosztów niezbędnych do poniesienia przez firmy z branży komunikacji elektronicznej 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 pozyskane przez Krajową Izbę Komunikacji Elektronicznej.

Dodatkowymi celami analizy są: określenie świadomości przedsiębiorców 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.

IV. MATERIAŁY ŹRÓDŁOWE

Do analizy wykorzystano informacje przekazane przez przedsiębiorców telekomunikacyjnych z segmentu mikro, małych i średnich przedsiębiorców (MŚP). Dane te zostały pozyskane z ankiety umieszczonej na dedykowanej podstronie Krajowej Izby Komunikacji Ethernetowej i udostępnionej przedsiębiorcom MŚP do wypełnienia. Okres ankietowania trwał od 16 listopada 2025 r. do 16 stycznia 2026 r. Dane do analizy zostały przekazane w postaci pliku .xls. Ankiety na potrzeby tej analizy zostały wypełnione przez 152 przedsiębiorców.

Dodatkowo do analizy wykorzystano projekt nowelizacji ustawy KSC w wersji po I czytaniu w Sejmie, które odbyło się 5 grudnia 2025 r., w szczególności informacje znajdujące się w OSR i uzasadnieniu, a także informacje ogólnodostępne w źródłach otwartych.

V. WYNIKI ANALIZY

W ramach ankiety sformułowano 13 następujących pytań:

1

Czy znane są Pani/Panu konsekwencje wejścia w życie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa przyjętej przez Radę Ministrów w październiku 2025?

2

Ile w zasobach firmy znajduje się sprzętu teleinformatycznego, w tym sieciowego, urządzeń elektronicznych (komputery, serwery, routery, switchy, DWDM, firewalles, anty-DDoS itp.) od producentów pochodzących spoza państw Unii Europejskiej i NATO?

3

Czy Pani/Pana zdaniem istnieje realna możliwość wymiany powyższego sprzętu teleinformatycznego i zastąpienie ich wyłącznie urządzeniami produkowanymi przez firmy z państw Unii Europejskiej i NATO?

4

Jeżeli TAK to: czy Pani/Pana zdaniem koszt netto wymiany powyższego sprzętu (koszt wymiany jest rozumiany jako zakup nowych urządzeń, utylizacja wymienianych oraz usługa demontażu i instalacji nowych urządzeń) będzie na poziomie?

5

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?

6

Czy Pani/Pana zdaniem istnieje realna możliwość wymiany powyższego oprogramowania i zastąpienie go wyłącznie oprogramowaniem od producentów pochodzących z państw Unii Europejskiej i NATO?

7

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) będzie na poziomie?

8

Jakie są roczne koszty serwisu i wsparcia technicznego posiadanego sprzętu od producentów pochodzących spoza państw Unii Europejskiej i NATO?

9

Jakie są roczne koszty serwisu i wsparcia technicznego dla posiadanego oprogramowania pochodzącego od producentów spoza państw Unii Europejskiej i NATO?

10

Czy Pani/Pana zdaniem wymiana posiadanego sprzętu i urządzeń na sprzęt pochodzący wyłącznie z państw Unii Europejskiej i NATO będzie wiązała się z większymi kosztami serwisu i wsparcia technicznego?

11

Jeżeli TAK to: będzie to kwota netto na poziomie?

12

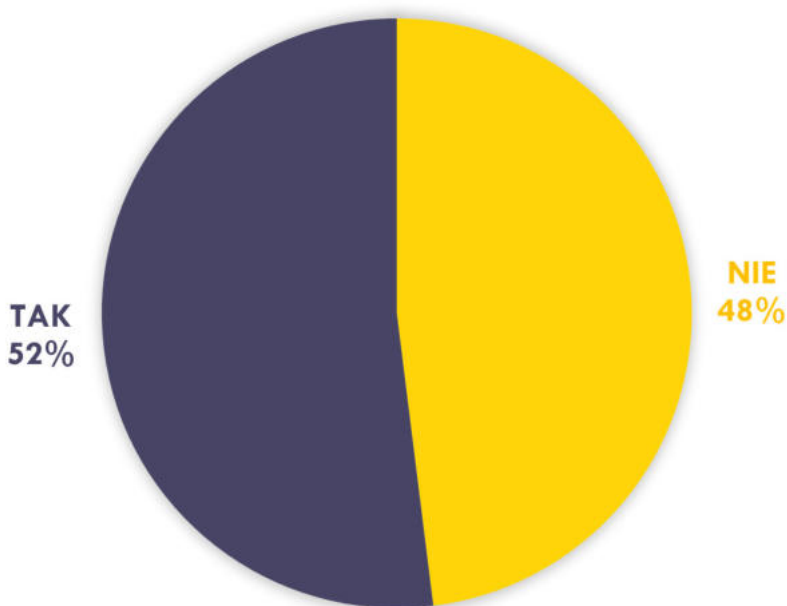
Czy Pani/Pana zdaniem wymiana posiadanego oprogramowania na oprogramowanie pochodzące wyłącznie z państw Unii Europejskiej i NATO będzie wiązała się z większymi kosztami serwisu i wsparcia technicznego?

13

Jeżeli TAK to: będzie to kwota netto na poziomie?

Pierwszym celem analizy było określenie poziomu świadomości przedsiębiorców z branży komunikacji elektronicznej, jaki wpływ na ten podsektor będą mieć przepisy nowelizacji ustawy KSC. Zagadnienie zostało zaadresowane pytaniem nr 1. Spośród 152 odpowiedzi, w 73 przypadkach ankietowani wskazali odpowiedź „NIE”.

Stanowi to 48%, czyli blisko połowę ankietowanych. Prowadzi to do wniosku, że przedsiębiorcy nadal nie posiadli wystarczającego poziomu wiedzy na temat konsekwencji wejścia przepisów w życie na prowadzenie działalności gospodarczej – zarówno w wymiarze organizacyjnym jak i finansowym, co może w przyszłości generować dla nich dodatkowe ryzyka.

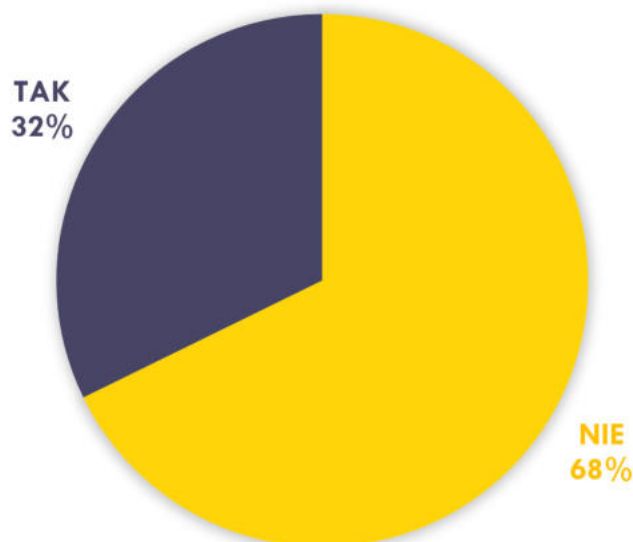


Wykres nr 1 – Odpowiedzi udzielone na pytanie: Czy znane są Pani/Panu konsekwencje wejścia w życie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa przyjętej przez Radę Ministrów w październiku 2025?

Kolejnym celem była próba ustalenia, czy dla sprzętu i oprogramowania podmiotów uznanych za dostawców wysokiego ryzyka istnieje realna alternatywa w postaci produktów i usług ICT dostarczanych przez firmy z UE lub NATO. Ten aspekt jest niezwykle istotny dla bezpieczeństwa państwa.

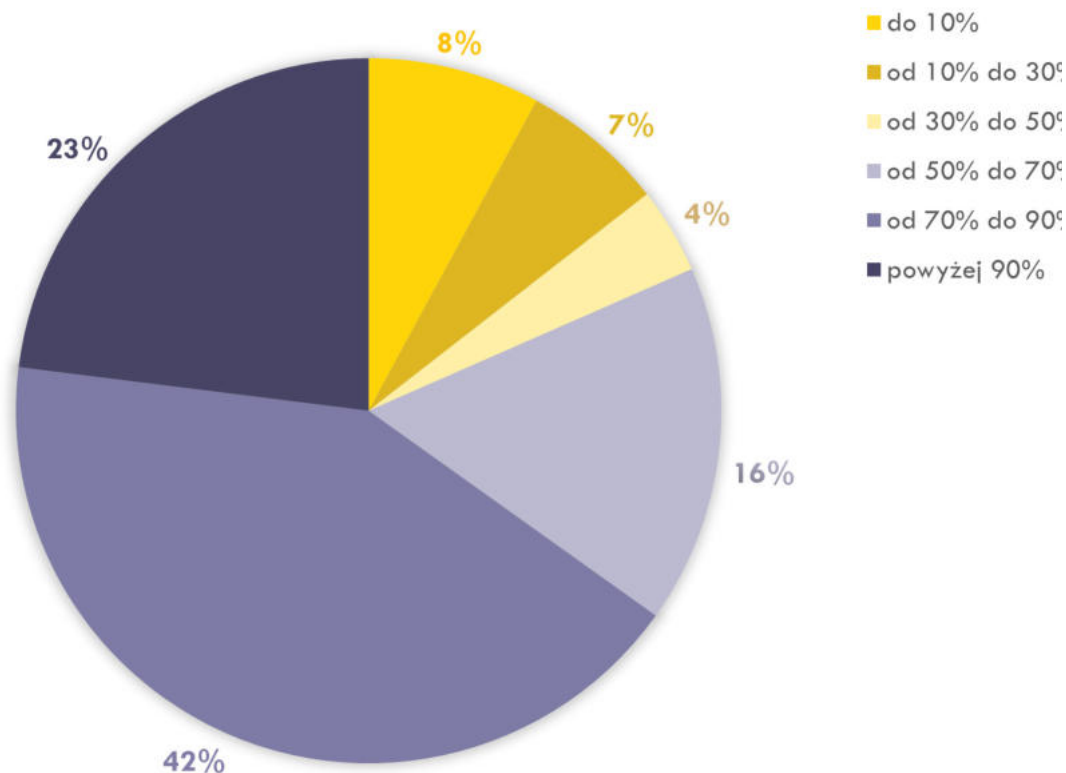
Jeżeli podmioty ważne i kluczowe zostaną zobowiązane do wycofania z użytkowania określonego sprzętu i oprogramowania, a nie będzie dla nich zamienników w wymiarze funkcjonalnym (aspekt kosztowy zostanie omówiony w dalszej części raportu), może to doprowadzić do zatrzymania lub znaczącego spowolnienia procesów w tych organizacjach, które działają w sektorach uznanych przez projektodawcę za fundamentalne dla bezpieczeństwa wewnętrznego i stabilności państwa.

W przypadku możliwości wymiany sprzętu 103 z 152 ankietowanych stwierdziło, że taka możliwość nie istnieje. Stanowi to 68% wszystkich odpowiedzi.



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

W celu oceny, na ile ewentualna konieczność wymiany sprzętu i oprogramowania dostawców spoza UE i NATO może być problematyczna oraz, czy w praktyce doprowadzić do zatrzymania lub utrudnienia prowadzenia działalności gospodarczej, należy także ocenić jaki udział sprzętu takich dostawców znajduje się obecnie w zasobach ankietowanych przedsiębiorców. Taki właśnie cel miało pytanie nr 2 ankiety. Poniżej zostały przedstawione dane w ujęciu procentowym, prezentujące ten podział.

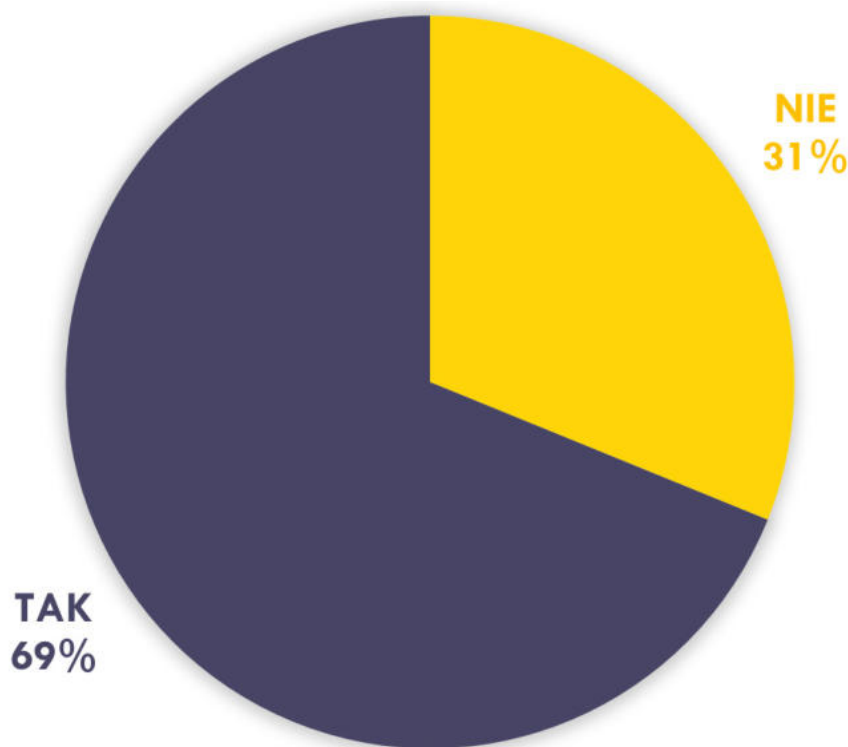


Wykres nr 3 – Odpowiedzi udzielone na pytanie: Ile w zasobach Pani/Pana firmy znajduje się sprzętu teleinformatycznego, w tym sieciowego, urządzeń elektronicznych (komputery, serwery, routery, switchy, DWDM, firewalle, anty-DDoS itp.) od producentów pochodzących spoza państw Unii Europejskiej i NATO?

Z przedstawionych danych wynika, że w praktyce aż 81% firm może doświadczyć ryzyka zatrzymania świadczonych usług i procesów biznesowych. Jest to grupa oznaczona kolorami: szarym, fioletowym i granatowym, w której ponad połowa sprzętu pochodzi spoza UE i NATO. Z kolei dodatkowe 4% podmiotów może mieć problem z utrzymaniem niezakłóconej ciągłości prowadzenia działalności, gdyż w tej grupie sprzęt spoza UE i NATO stanowi między 30% a 50% zasobów.

Podsumowując, można założyć, że w przypadku konieczności wycofania z użytkowania sprzętu dostawców spoza UE i NATO, 85% przedsiębiorców może borykać się z różnej skali problemami utrzymania efektywności, jakości i liczby świadczonych usług na poziomie sprzed pojawienia się takiej konieczności.

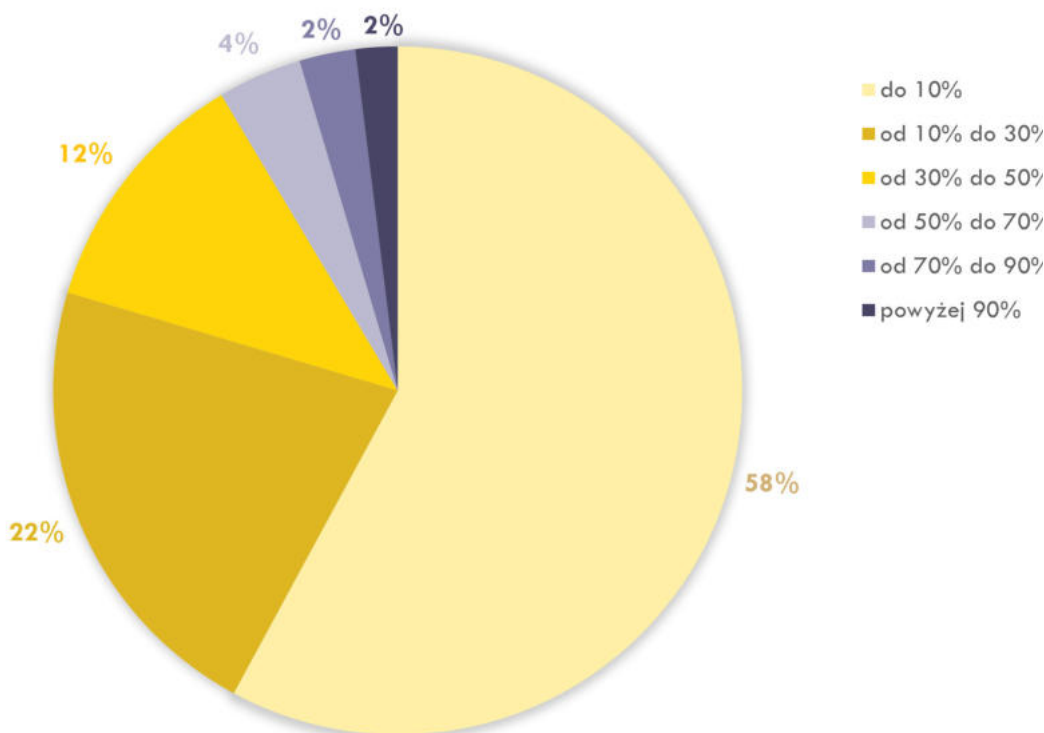
Odmienne wygląda natomiast sytuacja w przypadku oprogramowania dostarczanego przez podmioty spoza UE i NATO. Z przeprowadzonej ankiety wynika, że 69% przedsiębiorców widzi możliwość wymiany i zastąpienia go wyłącznie oprogramowaniem firm z państw UE i NATO.



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 70% należy uznać za obiektywnie wysoki, tym samym konieczność wymiany oprogramowania najprawdopodobniej nie wywoła znaczącego wpływu organizacyjnego na firmy, tym bardziej, że 80% ankietowanych wskazało, że w swoich zasobach informatycznych posiada mniej niż 30% **oprogramowania**⁷ dostawców spoza UE i NATO, a tylko 8% stwierdziło, że takie oprogramowanie stanowi więcej niż 50% całości takich zasobów. Szczegółowe dane z podziałem procentowym zostały zaprezentowane na poniższym wykresie.

7. 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 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?

Z powyższych danych wynika, że konieczność wymiany oprogramowania dostawców pochodzących spoza UE i NATO nie powinna negatywnie wpłynąć na realizowane procesy i świadczenie usług przez przedsiębiorców z branży komunikacji elektronicznej.

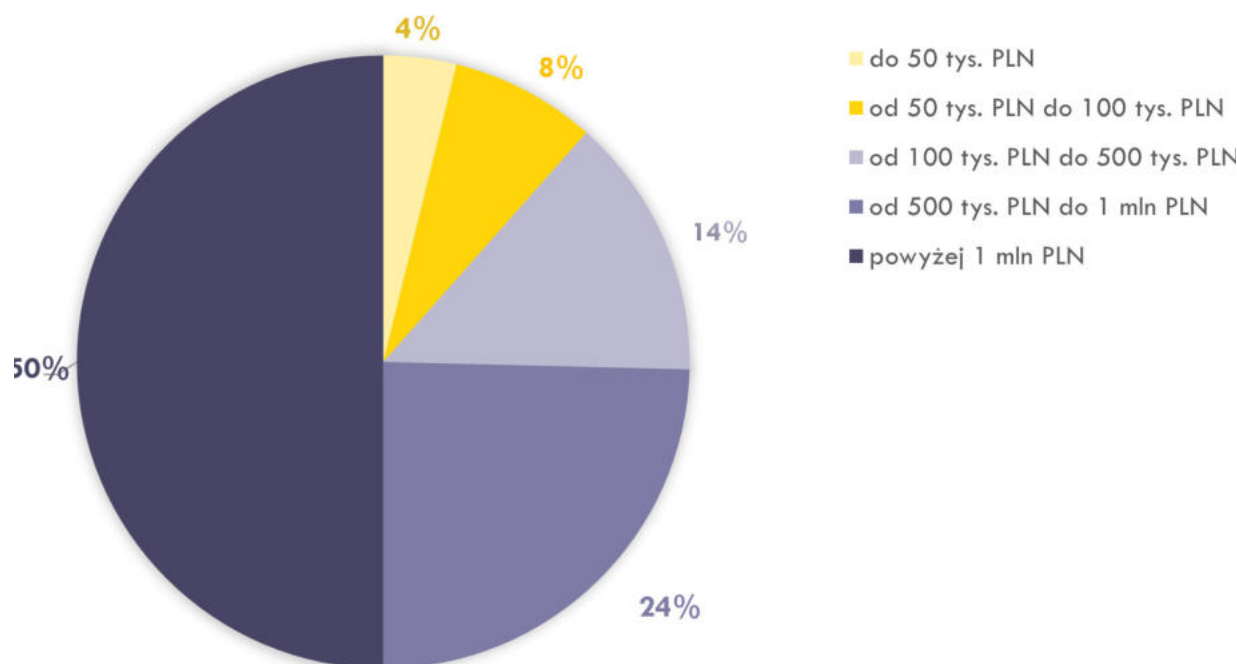
Podstawowym celem analizy była próba udzielenia odpowiedzi na pytanie, w jaki sposób wejście w życie nowelizacji ustawy KSC wpłynie na aspekt finansowy prowadzonej przez firmy działalności gospodarczej, precyzując – czy nastąpi wzrost kosztów, a jeżeli tak, to szacunkowo o jaką kwotę. Ze względu na to, że dane podlegające analizie opierają się na pytaniach ankietowych, poza procesem szacowania kosztów pozostają inne czynniki kosztotwórcze zawarte w projekcie nowelizacji, m.in. wprowadzenie odpowiednich i proporcjonalnych środków technicznych, operacyjnych i **organizacyjnych**⁸.

Badanie skupia się wyłącznie na oszacowaniu kosztów, które mogliby ponieść przedsiębiorcy w związku z ewentualnymi decyzjami ministra właściwego ds. informatyzacji w przedmiocie uznania dostawców sprzętu i oprogramowania spoza UE i NATO za dostawców wysokiego ryzyka, co w konsekwencji mogłoby doprowadzić do konieczności zastąpienia sprzętu i oprogramowania 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.

8. Obejmują one m.in.: politykę analizy ryzyka i bezpieczeństwa systemów informatycznych, zarządzanie incydentami, opracowanie planu ciągłości działania oraz zarządzania kryzysowego, bezpieczeństwo łańcucha dostaw, politykę i procedury oceny skuteczności środków zarządzania ryzykiem, szkolenia z cyberbezpieczeństwa czy zarządzanie dostępami i aktywami.

Z udzielonych przez ankietowane firmy odpowiedzi wynika, że 50% z nich uważa, iż koszt wymiany sprzętu przekroczyłby 1 mln PLN netto, 24% twierdzi, że byłaby to kwota w przedziale od 500 tys. PLN do 1 mln PLN. Pełne dane prezentuje poniższy wykres.



Wykres nr 6 – Odpowiedzi udzielone na pytanie: Czy Pani/Pana zdaniem koszt netto wymiany sprzętu (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 1 – Wyniki średniej arytmetycznej dla przedziałów kwotowych z pytania nr 4

przedział kwotowy z pytania nr 4	średnia arytmetyczna
do 50 tys. PLN	25 000 PLN
od 50 tys. PLN do 100 tys. PLN	75 000 PLN
od 100 tys. PLN do 500 tys. PLN	300 000 PLN
od 500 tys. PLN do 1 mln PLN	750 000 PLN
powyżej 1 mln PLN	1 100 000 PLN⁹

Uwaga: Metodę obliczania średniej arytmetycznej zastosowaną w Tabeli nr 1 przyjęto jako ujednoliconą metodę dla wszystkich pozostałych obliczeń w raportowanym badaniu.

9. 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.

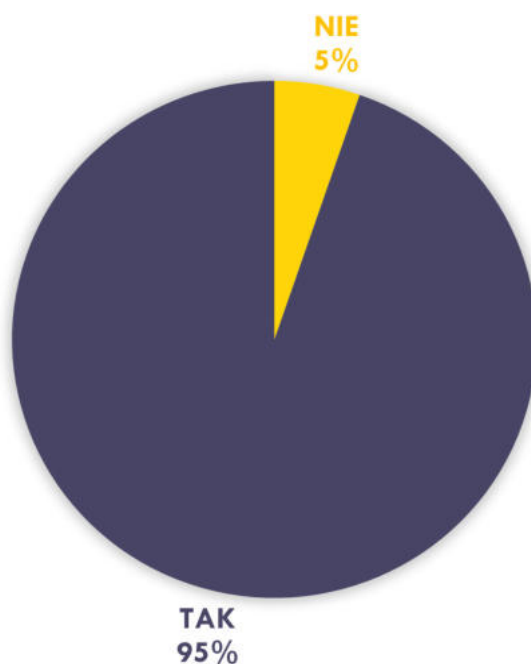
Następnie podanym w tabeli uśrednionym kwotom przypisano wagę odpowiadającą wartościom procentowym dla odpowiedniego przedziału kwotowego z wykresu nr 6.

W ostatnim etapie tak przygotowane dane, ułożone w tabeli, przeliczono z wykorzystaniem formuły w programie **MS Excel¹⁰**. 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 2 – Wyniki średniej ważonej dla kosztów wymiany sprzętu

przedział kwotowy z pytania nr 4	Waga - procent udzielonych odpowiedzi	średnia kwota w PLN
do 50 tys. PLN	4%	25 000
od 50 tys. PLN do 100 tys. PLN	8%	75 000
od 100 tys. PLN do 500 tys. PLN	14%	300 000
od 500 tys. PLN do 1 mln PLN	24%	750 000
powyżej 1 mln PLN	50%	1 100 000
średnia arytmetyczna		450 000
średnia ważona		779 000

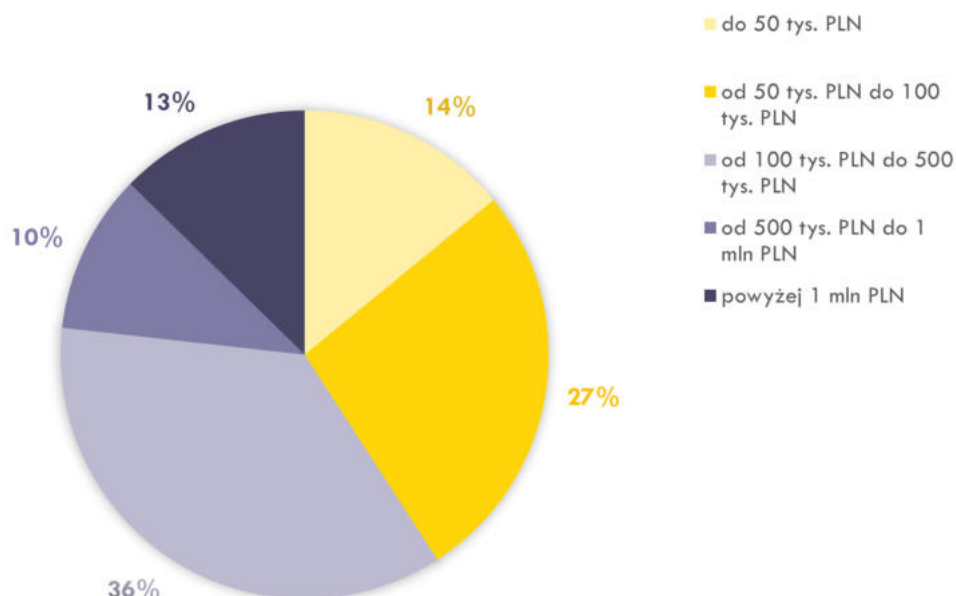
W celu oszacowania całościowych kosztów związanych z wymianą sprzętu, należało także przeanalizować koszty serwisu i wsparcia technicznego dla tych urządzeń. W tym przypadku aż 95% ankietowanych wskazało, że wymiana sprzętu wiązałaby się ze wzrostem kosztów. Wyniki zapytania zostały zaprezentowane na poniższym wykresie.



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

10. Formuła dla tej tabeli to =SUMA.ILOCZYNÓW(C2:C6;B2:B6)/SUMA(B2:B6)

Z udzielonych przez ankietowane firmy odpowiedzi wynika, że 36% z nich uważa, iż koszt serwisu i wsparcia technicznego wyniosłby w przedziale od 100 tys. PLN do 500 tys. PLN, a 27% podmiotów twierdzi, że wzrost wyniosłby 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 3 – Wyniki średniej ważonej dla kosztów serwisu i wsparcia technicznego sprzętu

przedział kwotowy z pytania nr 11	Waga - procent udzielonych odpowiedzi	średnia kwota w PLN
do 50 tys. PLN	14%	25 000
od 50 tys. PLN do 100 tys. PLN	27%	75 000
od 100 tys. PLN do 500 tys. PLN	36%	300 000
od 500 tys. PLN do 1 mln PLN	10%	750 000
powyżej 1 mln PLN	13%	1 100 000
średnia arytmetyczna		450 000
średnia ważona¹¹		349 750

Podsumowując, całościowe koszty związane z koniecznością wymiany sprzętu dostawców spoza UE i NATO u jednego przedsiębiorcy można oszacować na poziomie **1 128 750 PLN netto¹²** w pierwszym roku, natomiast w przeciągu **5 lat¹³** kwota ta może wynosić **2 527 750 PLN netto¹⁴**

11. Formuła dla tej tabeli to =SUMA.ILOCZYNÓW(C2:C6;B2:B6)/SUMA(B2:B6)

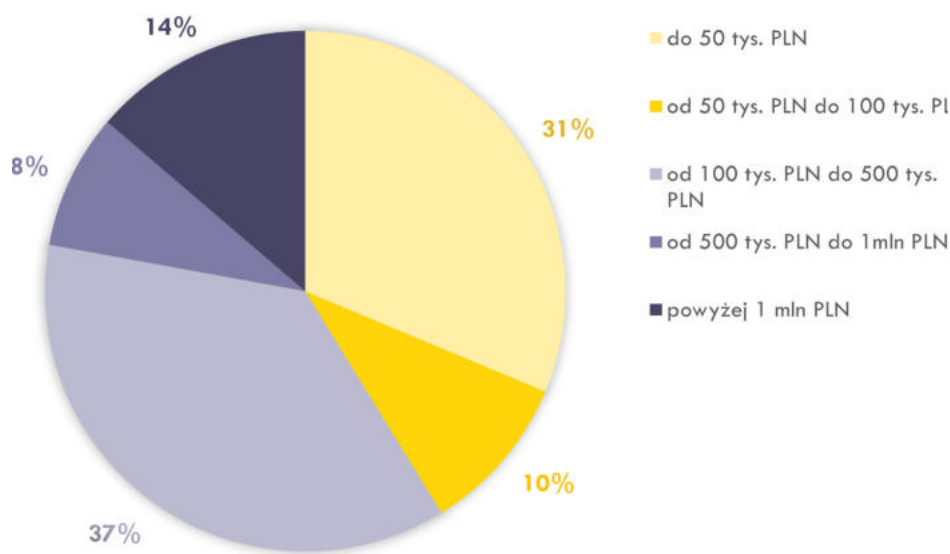
12. Suma średniego kosztu wymiany sprzętu z tabeli nr 2 i średniego rocznego kosztu serwisu z tabeli nr 3.

13. 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.

14. Suma średniego kosztu wymiany sprzętu z tabeli nr 2 i pięciokrotności średniego rocznego kosztu serwisu z tabeli nr 3.

Drugim elementem badania wpływu nowelizacji ustawy KSC na aspekt finansowy prowadzonej przez przedsiębiorców telekomunikacyjnych działalności gospodarczej jest analiza kosztów związanych z wymianą oprogramowania oraz usług jego serwisu i wsparcia technicznego. Z udzielonych przez ankietowane podmioty odpowiedzi wynika, że 37% z nich uważa, iż koszt wymiany oprogramowania mieściłby się w przedziale od 100 tys. PLN do 500 tys. PLN, a 31% twierdzi, że byłaby to kwota w przedziale do 50 tys. PLN.

Pełne dane prezentuje poniższy wykres.



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) będzie na poziomie?

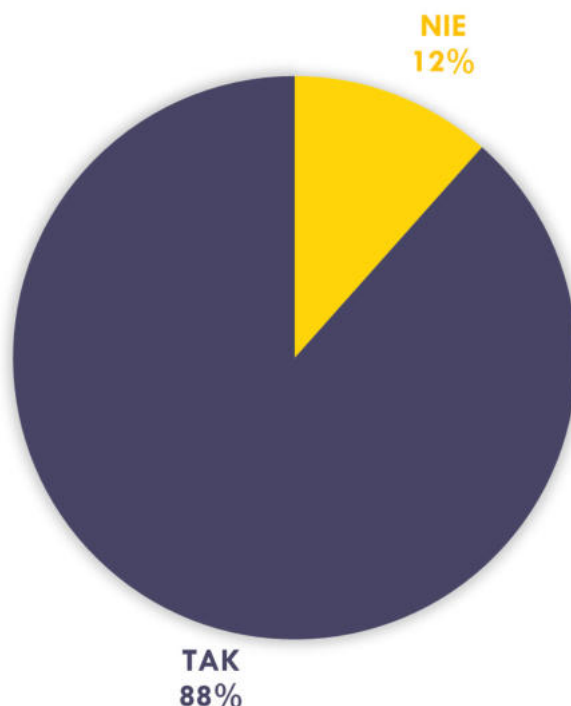
Dla oszacowania kosztów wymiany oprogramowania ponownie posłużono się metodą wyliczania średniej ważonej, analogicznie jak w przypadku obliczenia kosztów wymiany sprzętu. Poniższa tabela zawiera wyniki tego przeliczenia.

Tabela nr 4 – Wyniki średniej ważonej dla kosztów wymiany oprogramowania

przedział kwotowy z pytania nr 7	Waga - procent udzielonych odpowiedzi	średnia kwota w PLN
do 50 tys. PLN	31%	25 000
od 50 tys. PLN do 100 tys. PLN	10%	75 000
od 100 tys. PLN do 500 tys. PLN	37%	300 000
od 500 tys. PLN do 1 mln PLN	8%	750 000
powyżej 1 mln PLN	14%	1 100 000
średnia arytmetyczna		450 000
średnia ważona¹⁵		340 250

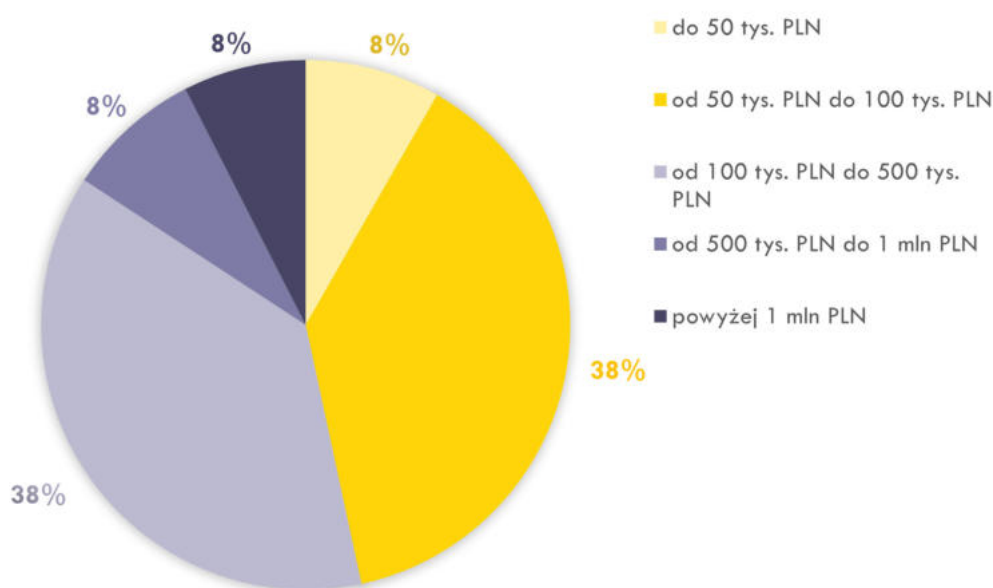
15. Formuła dla tej tabeli to =SUMA.ILOCZYNÓW(C2:C6;B2:B6)/SUMA(B2:B6)

Następnie powtórzono proces analityczny dla oszacowania wzrostu kosztów związanych z usługą serwisu i wsparcia technicznego oprogramowania. W tym przypadku 88% 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 firmy odpowiedzi wynika, że 38% z nich uważa, iż koszt serwisu i wsparcia technicznego oprogramowania wzrósłby w przedziale od 50 tys. PLN do 100 tys. PLN. Tyle samo podmiotów uważa, że byłby to wzrost w przedziale od 100 tys. PLN do 500 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 5 – Wyniki średniej ważonej dla kosztów serwisu i wsparcia technicznego oprogramowania

przedział kwotowy z pytania nr 13	Waga - procent udzielonych odpowiedzi	średnia kwota w PLN
do 50 tys. PLN	8%	25 000
od 50 tys. PLN do 100 tys. PLN	38%	75 000
od 100 tys. PLN do 500 tys. PLN	38%	300 000
od 500 tys. PLN do 1 mln PLN	8%	750 000
powyżej 1 mln PLN	8%	1 100 000
średnia arytmetyczna		450 000
średnia ważona¹⁶		292 500

Podsumowując, całkowite koszty związane z koniecznością wymiany oprogramowania producenta uznanego za dostawcę wysokiego ryzyka u jednego przedsiębiorcy można oszacować na poziomie **632 750 PLN netto¹⁷** w pierwszym roku, natomiast w przeciągu 5 lat kwota ta może wynosić **1 802 750 PLN netto¹⁸**.

Z przeprowadzonej analizy szacowania kosztów związanych z koniecznością wymiany sprzętu i oprogramowania dostawców spoza UE i NATO, której skutkiem byłaby faktyczna konieczność usunięcia całego sprzętu i oprogramowania takich dostawców wynika, że łączna kwota dla jednego przedsiębiorcy w pięcioletnim okresie może wynieść **4 330 500 PLN netto.**

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

17. Suma średniego kosztu wymiany oprogramowania z tabeli nr 4 i średniego rocznego kosztu serwisu z tabeli nr 5.

18. Suma średniego kosztu wymiany oprogramowania z tabeli nr 4 i pięciokrotności średniego rocznego kosztu serwisu z tabeli nr 5.

VI. SZCZEGÓŁOWE WNIOSKI I PODSUMOWANIE KOŃCOWE

1. Koszty przestrzegania obowiązków wynikających dla przedsiębiorców z przepisów nowelizacji ustawy KSC nie zostały zwymiarowane przez projektodawcę w aspekcie finansowym. W Ocenie Skutków Regulacji można jedynie odnaleźć potwierdzenie, że projektodawca ma świadomość zwiększenia nakładów finansowych, które będą musieli ponosić przedsiębiorcy z branży komunikacji elektronicznej, jednak nie podjął trudu ich pełnego oszacowania.
2. Blisko połowa firm, na które bezpośrednio będą oddziaływać przepisy nowelizacji KSC nie posiada świadomości konsekwencji nowych regulacji. Potwierdza to także wynik przeprowadzonej ankiety, w której 48% podmiotów wskazało, że nie są mu znane konsekwencje związane z wejściem w życie tej nowelizacji.
3. Na podstawie wyników ankiety można przyjąć założenie, że ewentualna konieczność wymiany oprogramowania dostawców spoza UE i NATO nie powinna spowodować w skali ogólnopolskiej znaczących problemów z zachowaniem ciągłości działania świadczenia usług z obszaru komunikacji elektronicznej. Blisko 70% ankietowanych stwierdziło, że istnieje możliwość wymiany tego oprogramowania na pochodzące wyłącznie z państw UE i NATO. Tym bardziej, że 80% ankietowanych wskazało, iż w swoich zasobach posiada mniej niż 30% oprogramowania dostawców spoza UE i NATO.
4. Istnieje realne ryzyko, że w przypadku konieczności wymiany sprzętu dostawców z państw spoza UE i NATO, 85% przedsiębiorców borykałoby się z dużymi problemami utrzymania efektywności, jakości i liczby świadczonych usług na poziomie sprzed pojawienia się takiej konieczności, ponieważ obecnie ponad 80% firm posiada w swoich zasobach ponad 50% sprzętu pochodzącego spoza 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 i usług ICT pochodzących od firm z UE i NATO można przyjąć, że szacunkowa kwota dla jednego przedsiębiorcy telekomunikacyjnego mogłaby wynieść 4,3 mln PLN netto w pięcioletniej perspektywie. W tej kwocie zawarty jest szacunkowy koszt zakupu nowych produktów, koszt deinstalacji starych i instalacji nowych urządzeń, koszt utylizacji zdemontowanego sprzętu oraz koszty pięcioletniej usługi serwisu i wsparcia technicznego.
6. W oparciu o wyliczoną szacunkową kwotę kosztów jakie może ponieść pojedynczy przedsiębiorca, można także oszacować przybliżony skutek finansowy dla wszystkich przedsiębiorców telekomunikacyjnych z podsektora komunikacja elektroniczna. Według danych zawartych w Ocenie Skutków Regulacji, nowelizacja będzie miała wpływ na 3332 podmioty z branży, co po przemnożeniu przez wartość finansową skutku dla jednej firmy daje kwotę około 14,4 mld PLN netto w pięcioletniej perspektywie.
7. Należy pamiętać, że przedmiotem analizy było oszacowanie kosztów, które mogliby ponieść przedsiębiorcy telekomunikacyjni, gdyby praktycznym skutkiem decyzji DWR było usunięcie całego sprzętu i oprogramowania dostawców z państw spoza UE i NATO. Tym samym poza badaniem pozostały inne obciążenia i obowiązki wynikające z projektowanej nowelizacji KSC, takie jak obowiązek wprowadzenia systemu zarządzania bezpieczeństwem informacji, obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych, czy wykonywanie okresowych audytów. To będzie mieć również bezpośredni wpływ na organizację pracy i koszty funkcjonowania tych przedsiębiorców.