**Zestawienie uwag zgłoszonych w trakcie opiniowania**

**Opinię wyraziły:** Komisja Nadzoru Finansowego (KNF), Rada ds. Cyfryzacji, Narodowe Centrum Badań i Rozwoju (NCBiR), Rzecznik Finansowy, Straż Graniczna, Najwyższa Izba Kontroli (NIK), Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK-PIB), Polskie Centrum Akredytacji (PCA)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nazwa projektu dokumentu: **projektu uchwały Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024** | | | | | | |
| **L.p.** | **Podmiot wnoszący uwagi** | **Jednostka redakcyjna, do której wnoszone są uwagi** | **Fragment tekstu opiniowanego** | **Treść uwagi wraz z propozycją zmian zapisu** | **Stanowisko MC** | **Stanowisko podmiotu wnoszącego uwagę - po konferencji uzgodnieniowej** |
|  | NCBiR | Uwaga o cel szczegółowy 1.5 (p 5.5) |  | NCBR: proponujemy dookreślić, że metodyka i narzędzia umożliwiające statyczne i dynamiczne szacowanie ryzyka dla systemów teleinformatycznych są opracowywane w ramach projektu badawczego pn. „Narodowej Platformy Cyberbezpieczeństwa”, realizowanego przez Naukową i Akademicką Sieć Komputerową i finansowanego przez Narodowe Centrum Badań i Rozwoju w ramach Programu CyberSecIdent – Cyberbezpieczeństwo i e-Tożsamość. | **Uwaga uwzględniona**  Dodany zostanie przypis. | **Przyjęto wyjaśnienie.** |
|  | NCBiR | Uwaga o cel szczegółowy 3.3 (p 7.3) | „[…] wspólnie z Narodowym Centrum Badań i Rozwoju kontynuowane będą programy badawcze, mające na celu przygotowanie i wdrożenie nowych metod ochrony przed cyberzagrożeniami” | NCBR: proponujemy by odnieść się bezpośrednio do obecnie prowadzonej współpracy NCBR i Ministerstwa Cyfryzacji tj. Programu CyberSecIdent. Cele Programu a także okres ich osiągnięcia są zbieżne z tymi, które wskazano w proponowanej Strategii. Na etapie opracowywania Planu Działań w ramach Strategii proponujemy przeprowadzenie konsultacji z Komitetem Sterującym Programu CyberSecIdent. | **Uwaga uwzględniona** |  |
|  | NCBiR | Uwaga o Finansowanie | Źródłami finansowania realizacji działań opisanych w dokumencie będą plany finansowe poszczególnych jednostek zaangażowanych we wdrażanie Strategii Cyberbezpieczeństwa, a także środki pochodzące z Narodowego Centrum Badań i Rozwoju oraz środki Unii Europejskiej, w miarę zaistnienia takich możliwości. | NCBR: należy doprecyzować, że źródłami finansowania opisanych działań będą także środki pochodzące z Narodowego Centrum Badań i Rozwoju przeznaczane na finansowanie projektów badawczo – rozwojowych obejmujących badania przemysłowe, prace rozwojowe lub zadania o charakterze przygotowawczym do wdrożenia. Brak dookreślenia w projekcie Strategii typu finansowanych przez NCBR projektów, może być w przyszłości mylnie interpretowane jako źródło finansowania wszelkich zadań wpisujących się w tworzone przez Ministerstwo Cyfryzacji plany działań. | **Uwaga nieuwzględniona**  Wynika to z definicji programów badawczo – rozwojowych. Strategia nie wchodzi w kompetencje NCBiR. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga do finansowania |  | Rada: Ani projekt Strategii, ani uzasadnienie do tego projektu nie wskazują poziomu nakładów finansowych niezbędnych dla osiągnięcia tego celu, ani konkretnych źródeł finansowania. | **Uwaga częściowo uwzględniona**  Konkretne działania wraz z harmonogramem ich realizacji będą ustalone w Planie działań.  Natomiast kwestie finansowania będą przedmiotem dyskusji w trakcie prac nad zmianami ustawy o ksc. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga do finansowania | Przyjęte rozwiązania nie spowodują dodatkowych skutków finansowych dla sektora finansów publicznych, w tym budżetu państwa i budżetów jednostek samorządu terytorialnego. | Rada: Teza ta nie znajduje odzwierciedlenia w rzeczywistości. Przeciwnie - skala problemu i wyzwań wymaga alokowania i przeznaczenia znacznych środków budżetowych na budowanie odporności cybernetycznej, a także zabezpieczenia ich w ramach negocjowania funduszy unijnych. Ta potrzeba powinna bardzo wyraźnie wybrzmieć w Strategii. | **Uwaga częściowo uwzględniona**  Uchwała Rady Ministrów nie może nakładać zobowiązań finansowych, gdyż może to nastąpić jedynie w drodze ustawy. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga ogólna |  | Rada: Strategia nie zawiera żadnych miar pozwalających ocenić stopień jej realizacji, przez co w niewielkim stopniu staje się dokumentem praktycznie wyznaczającym cele dla podmiotów wszystkich sektorów. Dopiero Plan działań na rzecz wdrożenia Strategii będzie wskazywał m.in. na oczekiwane efekty wynikające z realizacji poszczególnych zadań w ramach realizacji celów szczegółowych. Uważamy to za mankament dokumentu klasy „strategii”, który takie miary winien proponować. | **Uwaga nieuwzględniona**  Strategia jako dokument ramowy wskazuje kierunki działań rządu RP.  Szczegółowe działania wraz z harmonogramem ich realizacji, źródłami finansowania oraz miernikami realizacji, będą wskazane w Planie działań. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o dodanie celu szczegółowego |  | Rada: dokument w niewystarczającym stopniu odnosi się do stwierdzonego w niezależnych badaniach niskiego poziomu cyberbezpieczeństwa urzędów administracji samorządowej i samorządowych jednostek organizacyjnych. Wobec skali i zagrożeń, jakie wiążą się z nieprzygotowaniem jednostek samorządu terytorialnego do sprostania wyzwaniom cyberzagrożeń, jego zapewnienie – w naszym przekonaniu – stanowić winno odrębny cel szczegółowy Strategii. | **Uwaga nieuwzględniona.**  Strategia, wskazuje (za wynikami kontroli NIK z lat 2018-2019) na potrzebę szczególnego zwrócenia uwagi na kwestie cyberbezpieczeństwa w JST (cel szczegółowy 5.2). Konkretne działania wskazane zostaną w Planie działań. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga ogólna |  | Rada: Strategia w dużym stopniu pomija kwestie infrastrukturalne, w tym związane ze strukturą i charakterem podmiotów kluczowych z punktu widzenia realizacji Strategii i zapewnienia właściwego poziomu cyberbezpieczeństwa RP. | **Uwaga nieuwzględniona**  Poza zakresem Strategii. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o rozszerzenie celu głównego | Podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji. | Rada: postulujemy rozszerzenie definicji celu głównego o m. in. działania prewencyjne, działania zapewniające zdolność do reakcji na zmaterializowane zagrożenia, a także o ochronę infrastruktury cyfrowej i procesów cyfrowych, a nie tylko informacji. | **Uwaga nieuwzględniona**  Proponowane elementy mieszczą się w obecnej treści celu głównego. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga ogólna | Podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji. | Rada: Cel główny w zakresie zapewnienia cyberbezpieczeństwa obywateli ograniczony wyłącznie do lepszej ochrony ich informacji pomija istotny element niezakłóconego dostępu obywateli do informacji za pośrednictwem systemów teleinformatycznych. W efekcie, w celach szczegółowych potraktowano marginalnie działania związane ze zwiększeniem odporności na ataki mające na celu wpływanie na obywateli za pomocą nieprawdziwych informacji lub innych narzędzi wojny psychologicznej stanowiących element wojny hybrydowej toczonej w cyberprzestrzeni. Niewystarczająco opisano także ewentualne działania mające na celu zapobieganie pozbawiania obywateli dostępu do informacji prawdziwych, a usuwanych z przyczyn politycznych z cyberprzestrzeni przez podmioty prywatne z powołaniem się na ich wewnętrzne zasady i regulaminy pod pretekstem walki z nienawiścią lub podobnymi pretekstami. | **Uwaga nieuwzględniona**  W celu szczegółowym 8.3 są opisane kierunki działań rządu RP odnośnie działań o charakterze manipulacyjnym w cyberprzestrzeni. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga ogólna |  | Rada: Cele szczegółowe projektu Strategii nie odnoszą się do niektórych sektorów gospodarki narodowej, które powinny być przedmiotem szczególnej troski z punktu widzenia zapewnienia cyberbezpieczeństwa i odporności na ataki cybernetyczne, takich jak szeroko rozumiany sektor energii, i inne sektory krytyczne w tym dostarczające obywatelom podstawowe media, telekomunikacyjny, finansowy. W Strategii nie zapisano żadnych konkretnych działań, które odnoszą się do tych sektorów. Ich pominięcie uniemożliwia realizację celu głównego w zakresie zwiększenia poziomu  ochrony informacji m.in. w sektorze prywatnym. | **Wyjaśnienie**  Wymienione sektory – kluczowe dla państwa – są podmiotem uregulowań w ustawie o krajowym systemie cyberbezpieczeństwa lub w Prawie telekomunikacyjnym.  Przepisy prawa jasno określają obowiązki podmiotów np. w sektorze energii oraz zadania odpowiednich organów władzy państwowej. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o cel szczegółowy 1.1 (p 5.1) | Propozycje kierunków zmian i planów na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa będą opiniowane przez Kolegium, działające przy Radzie Ministrów, jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa. | Rada: W ramach realizacji postulatu o współpracy publiczno-prywatnej należy w tym miejscu dopuścić także konsultacje z podmiotami zewnętrznymi, w tym z sektorem prywatnym i organizacjami pozarządowymi. | **Uwaga nieuwzględniona**  Udział czynnika społecznego będzie realizowany w innych obszarach. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o cel szczegółowy 1.1 (p 5.1) | rząd w ramach współpracy administracji rządowej z administracją samorządową będzie rekomendował i działał na rzecz jednostek samorządu terytorialnego w zakresie podnoszenia kompetencji w doborze, wdrażaniu i utrzymaniu środków technicznych zwiększających cyberbezpieczeństwo, w tym korzystania z nowoczesnych i bezpiecznych modeli przetwarzania w chmurach obliczeniowych, tworzenia bezpiecznych aplikacji oraz korzystania z bezpiecznych systemów mobilnych | Rada: Naszym zdaniem dokument powinien bardziej precyzyjnie określić i opisać docelowy model współpracy centrum i jednostek samorządu terytorialnego w zakresie budowania odporności i zdolności, a także zapobiegania incydentom. | **Uwaga nieuwzględniona.**  Zakres współpracy z JST jest już ujęty w projekcie. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o cel szczegółowy 1.4 (p 5.4) | Wyrazem tego są przygotowywane już analizy dotyczące doprecyzowania wymagań bezpie-czeństwa niezbędnych do spełnienia przez operatorów telekomunikacyjnych, szczególnie przy budowie sieci 5G, która w przyszłości będzie podstawą funkcjonowania państwa. | Rada: Z uwagi na czasowy zakres dokumentu rekomendowane jest natomiast wzięcie pod 4 uwagę także technologii 6G, dlatego postuluje się rozważenie zapisu "5G i sieci komórkowych kolejnych generacji" | **Uwaga częściowo uwzględniona** | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o cel szczegółowy 3 (p 7) | Zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa | Rada: nie wskazano wprost na włączenie w te działania polskiego przemysłu obronnego, co wydaje się, że jest pewnym brakiem ze względu na specyfikę przedsiębiorców przemysłu obronnego w odróżnieniu od przedsiębiorców prowadzących działalność na rynku cywilnym. | **Wyjaśnienie**  Polski potencjał w obszarze cyberbezpieczeństwa obejmuje zarówno sektory: publiczny, prywatny, jak i militarny. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o cel szczegółowy 3.1 (p 7.1) | Rząd Polski stawia sobie za cel inwestowanie w rozbudowę zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa poprzez stwarzanie warunków dla rozwoju przedsiębiorstw, ośrodków naukowo-badawczych, jak i start-upów, których przedmiotem działalności jest tworzenie nowych rozwiązań w obszarze cyberbezpieczeństwa. Jednym z priorytetów jest wzrost zdolności w obszarze projektowania i wytwarzania oprogramowania, urządzeń i usług wykorzystywanych we wszystkich gałęziach polskiego przemysłu, zwiększających jego konkurencyjność. | Rada: Rząd Polski stawia sobie za cel inwestowanie w rozbudowę zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa poprzez stwarzanie warunków dla rozwoju przedsiębiorstw, ośrodków naukowobadawczych, jak i start-upów, których przedmiotem działalności jest tworzenie nowych rozwiązań w obszarze cyberbezpieczeństwa. Jednym z priorytetów jest wzrost zdolności w obszarze projektowania i wytwarzania urządzeń oraz oprogramowania systemowego i użytkowego, a także realizacji usług wykorzystywanych we wszystkich gałęziach polskiego przemysłu, zwiększających jego cyberbezpieczeństwo, co bezpośrednio przełoży się na realizację celów związanych z transformacją cyfrową gospodarki i na zwiększenie jej konkurencyjności. Sektor cyberbezpieczeństwa, w ramach sektora teleinformatycznego, może także stać się siłą napędową wzrostu gospodarczego. | **Uwaga nieuwzględniona**  Propozycja niezgodna z założeniami. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o cel szczegółowy 3.1 (p 7.1) | Stymulowane będzie podnoszenie kompetencji ośrodków naukowych oraz wyższych uczelni w obszarze cyberbezpieczeństwa **w zakresie rozwoju zasobów technologicznych.** | Rada proponuje dodanie zwrotu: **w zakresie rozwoju zasobów technologicznych.** | **Uwaga nieuwzględniona**  Niepotrzebne ograniczenie. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o cel szczegółowy 3.1 (p 7.1) | Poprzez instrumenty prawne rząd będzie stymulował na wyższych uczelniach nauczanie służące **pozyskiwaniu specjalistów z zakresu cyberbezpieczeństwa**, w ramach studiów pierwszego i drugiego stopnia oraz studiów doktoranckich i podyplomowych. | Rada proponuje zamienić zwrot na: „**rozwojowi zasobów ludzkich z zakresu cyberbezpieczeństwa**” | **Uwaga nieuwzględniona**  Ta uwaga zawęża te kwestię. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o cel szczegółowy 3.3 (p 7.3) | jak również chmury obliczeniowych, sieci mobilnej łączności szerokopasmowej (5G i kolejnych generacji), czy megadanych (Big Data) zachodzi konieczność intensyfikacji działań badawczych | Rada proponuje zamienić zwrot na: „**czy technologii komputerów kwantowych oraz sztucznej inteligencji, a tym samym zwiększenia ilości przetwarzanych danych**” | **Uwaga nieuwzględniona**  To jest katalog otwarty. Nie wskażemy wszystkiego. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o cel szczegółowy 3.3 (p 7.3) | zapewnienia bezpieczeństwa produktu, usługi lub procesu już na etapie projektowania (Security by Design), a także ochronę danych i prywatności (Privacy by Design). | Rada proponuje dodać zwrot: „**a także ochronę danych i prywatności (Privacy by Design).**” | **Uwaga uwzględniona**  Plus dodanie przypisu z wyjaśnieniem pojęcia „Privacy by design”. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o cel szczegółowy 3.3 (p 7.3) | Rząd RP będzie promował i wspierał podejście uwzględniające bezpieczeństwo i ochronę danych i prywatności już od etapu projektowania. | Rada proponuje dodać zwrot: „**i ochronę danych i prywatności**” | **Uwaga nieuwzględniona**  Uwaga 20 – zostało to zaadresowane. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o cel szczegółowy 4.1 (p 8.1) | W celu utrzymania w administracji publicznej pracowników o wysokich kompetencjach, równolegle z wykorzystaniem innych instrumentów wspierających ich aktywność, podjęte będą działania w celu zbliżenia zarobków tych pracowników do poziomu, jaki mogliby uzyskać zatrudniając się w sektorze prywatnym. | Rada: Nie wskazano, jak zapobiegać utracie wykształconych w Polsce specjalistów w wyniku emigracji do innych krajów, ani mechanizmów powrotu do Polski specjalistów, którzy uprzednio wyemigrowali z Polski i uzyskali kwalifikację za granicą. | **Uwaga nieuwzględniona**  Delegacja ustawowa ( ustawa o ksc) nie przewiduje tego u i nie wychodzimy poza nią. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o cel szczegółowy 5 (p 9) | Istotna jest również współpraca z krajami regionu, w tym wzmocnienie współpracy w ramach Grupy Wyszehradzkiej, jak i z państwami tzw. Trójmorza. | Rada: należy konsekwentnie wspomnieć o potrzebie wypracowania wspólnych procedur działania także w ramach współpracy krajów Trójmorza. | **Uwaga nieuwzględniona**  Nie jest to niezbędne w kontekście Strategii. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga ogólna |  | Rada: Projekt Strategii nie zawiera bezpośrednich odniesień do realizowanego obecnie procesu zapewnienia obywatelom dowodów osobistych z warstwą elektroniczną i związanych z tym potencjalnych możliwości zwiększenia bezpieczeństwa obrotu z wykorzystaniem elektronicznych nośników tożsamości. | **Uwaga nieuwzględniona**  Poza zakresem Strategii. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o treść Wstępu | Rozwój społeczny i gospodarczy, a także bezpieczeństwo (militarne) w coraz większym stopniu | Rada proponuje dodanie zwrotu: „**a także bezpieczeństwo (militarne)**” | **Uwaga nieuwzględniona**  Proponowana zmiana drastycznie zmienia znaczenie zdania. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o treść Wstępu | Dynamiczny rozwój systemów informacyjnych, a także zwiększanie wydajności centrów przetwarzania danych, służą rozwojowi gospodarki, w szczególności w obszarze komunikacji, handlu, transportu czy też usług finansowych, a także warunkują zdolności obronne państw | Rada proponuje dodanie zwrotu: „**a także warunkują zdolności obronne państw.**” | **Uwaga nieuwzględniona**  Niezgodne z koncepcją Strategii. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o treść Wstępu | Z wykorzystaniem technologii cyfrowych **tworzących** cyberprzestrzeń tworzone są i kształtowane | Rada proponuje zamienić na zwrot: „**budujących**” | **Uwaga nieuwzględniona**  Niepotrzebna zmiana. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o treść Wstępu | a także oddziaływania w sferze politycznej **i geopolitycznej.** | Rada proponuje dodanie zwrotu: „**i geopolitycznej**” | **Uwaga nieuwzględniona**  Poza zakresem Strategii. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o treść Wizji | oraz codzienne funkcjonowanie indywidualnego członka społeczeństwa, **jak i bezpieczeństwo Państwa** | Rada proponuje dodać zwrot: „**jak i bezpieczeństwo Państwa**” | **Uwaga nieuwzględniona**  Poza zakresem Strategii. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o treść Wizji | są związane ze sprawnym i **bezpiecznym** działaniem systemów teleinformatycznych | Rada proponuje zamienić zwrot na: „**niezakłóconym**” | **Uwaga nieuwzględniona**  W bezpieczeństwie zawiera się pojęcie „niezakłócone” | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o cel szczegółowy 5.1 (p 9.1) | w tym szczególnie pomiędzy ministrem właściwym ds. informatyzacji oraz z ministrem spraw zagranicznych odpowiadającym za całokształt polskiej polityki zagranicznej i Ministrem Obrony Narodowej. | Rada proponuje dodać: Ministra Obrony Narodowej | **Uwaga nieuwzględniona**  Do decyzji MON. | **Przyjęto wyjaśnienie.** |
|  | Rada ds. Cyfryzacji | Uwaga o uzasadnienie | Projekt uchwały nie będzie miał wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców. | Rada: Powyższe stwierdzenie pozostaje w sprzeczności z częścią zapisów projektu Strategii (w celu głównym jest m.in. mowa o sektorze prywatnym bez ograniczenia go wyłącznie do dużych przedsiębiorców, w celu szczegółowym 3. jest mowa m.in. o stwarzaniu warunków dla rozwoju przedsiębiorstw jak i start-upów). | **Uwaga nieuwzględniona**  Ten zapis jest zgodny z zasadami sporządzania OSR. Dopiero konkretne działania na poziomie Planu działań będą miały wpływ na gospodarkę. Na obecnym etapie nie jest możliwe oszacowanie wpływu. | **Przyjęto wyjaśnienie.** |
|  | Rzecznik Finansowy | Uwaga o cel szczegółowy 4.3 (p 8.3) | wolności w środowisku cyfrowym **oraz uprawnień osób, które padły ofiarą cyberataku i poniosły szkodę w wyniku naruszeń bezpieczeństwa w sieci.** | Pani Aleksandra Wiktorow proponuje dodać zwrot „**oraz uprawnień osób, które padły ofiarą cyberataku i poniosły szkodę w wyniku naruszeń bezpieczeństwa w sieci.**” | **Uwaga nieuwzględniona**  Ochrona ofiar zawiera się w tym zapisie. | **Uwaga została uwzględniona. Dokonano zmiany zapisu.** |
|  | KNF | Uwaga o p 4.3 | **Cel szczegółowy 2.** Stymulowanie podniesienia poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty **oraz** **działania po ich wystąpieniu** | KNF proponuje dodać zwrot: Stymulowanie podniesienia poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty **oraz** **działania po ich wystąpieniu** | **Uwaga nieuwzględniona**  Reagowanie jest pojęciem szerszym i dotyczy także działań po jego wystąpieniu. | **Przyjęto wyjaśnienie.** |
|  | KNF | Uwaga o cel szczegółowy 1.1 (p 5.1) | odpowiadają ministrowie według właściwości wynikającej z ustawy o działach administracji rządowej **oraz organy właściwe wynikające z ustawy o Krajowym Systemie Cyberbezpieczeństwa.** | KNF proponuje dodanie zwrotu: **oraz organy właściwe wynikające z ustawy o Krajowym Systemie Cyberbezpieczeństwa.** | **Uwaga uwzględniona** |  |
|  | KNF | Uwaga o cel szczegółowy 1.1 (p 5.1) | W ramach prac legislacyjnych minister właściwy do spraw informatyzacji, we współpracy z innymi resortami **i organami właściwymi, odpowiedzialnymi za sprawowanie nadzoru w zakresie systemów teleinformatycznych w sektorach** | KNF proponuje dodać: „**i organami właściwymi, odpowiedzialnymi za sprawowanie nadzoru w zakresie systemów teleinformatycznych w sektorach**” | **Uwaga uwzględniona** |  |
|  | KNF | Uwaga o cel szczegółowy 1.1 (p 5.1) | zachodzących w obszarze cyberbezpieczeństwa niezbędne będzie **okresowe** monitorowanie zjawisk tam zachodzących | KNF proponuje zamienić zwrot na: „**ciągłe**” | **Uwaga uwzględniona** |  |
|  | KNF | Uwaga o cel szczegółowy 1.1 (p 5.1) | będą opiniowane przez Kolegium **ds. cyberbezpieczeństwa**, działające przy Radzie Ministrów | KNF proponuje dodać zwrot: „**ds. cyberbezpieczeństwa**” | **Uwaga uwzględniona** |  |
|  | KNF | Uwaga o cel szczegółowy 1.1 (p 5.1) | oraz działalności **w tym zakresie** CSIRT MON, CSIRT NASK, CSIRT GOV | KNF proponuje usunąć zwrot: „**w tym zakresie**” | **Wyjaśnienie**  Zapis został zmieniony. |  |
|  | KNF | Uwaga o cel szczegółowy 1.2 (p 5.2) | współpracujących z nimi **sektorowych zespołów reagowania na incydenty**, regionalnych i lokalnych zespołów cyberbezpieczeństwa | KNF: W KSC brak jest informacji o „sektorowych zespołach reagowania na incydenty”. Czy chodzi o „sektorowe zespoły cyberbezpieczeństwa”? | **Uwaga uwzględniona** |  |
|  | KNF | Uwaga o cel szczegółowy 1.2 (p 5.2) | współpracujących z nimi **sektorowych zespołów reagowania na incydenty, regionalnych i lokalnych zespołów cyberbezpieczeństwa** a także centrów analizy i wymiany informacji. | KNF proponuje ujednolicić nazewnictwo wg KSC na samo: „**sektorowych zespołów cyberbezpieczeństwa**”. | **Uwaga uwzględniona** |  |
|  | KNF | Uwaga o cel szczegółowy 1.2 (p 5.2) | wymianę informacji pomiędzy interesariuszami i dzielenie się wiedzą, co do **podatności,** zagrożeń i incydentów. | KNF proponuje dodać zwrot: „**podatności**” | **Uwaga uwzględniona** |  |
|  | KNF | Uwaga o cel szczegółowy 1.2 (p 5.2) | jednostek samorządu terytorialnego w zakresie podnoszenia kompetencji w **doborze, wdrażaniu i utrzymaniu środków technicznych zwiększających cyberbezpieczeństwo,** w tym korzystania z nowoczesnych | KNF proponuje zamienić zwrot na: jednostek samorządu terytorialnego w zakresie podnoszenia kompetencji w **projektowaniu procesów zwiększających cyberbezpieczeństwo, w szczególności: doborze, wdrażaniu i utrzymaniu środków technicznych,** w tym korzystania z nowoczesnych | **Wyjaśnienie**  Zmiana w zapisie. |  |
|  | KNF | Uwaga o cel szczegółowy 1.3 (p 5.3) | dla potrzeb administracji publicznej **oraz podmiotów wchodzących w skład KSC** wykorzystującego najnowocześniejsze | KNF proponuje dodanie zwrotu: dla potrzeb administracji publicznej **oraz podmiotów wchodzących w skład KSC** wykorzystującego najnowocześniejsze | **Uwaga nieuwzględniona**  W tym punkcie mowa jest o SKBN, który nie będzie otwarty dla podmiotów wchodzących w skład KSC. | **Przyjęto wyjaśnienie.** |
|  | KNF | Uwaga o cel szczegółowy 1.4 (p 5.4) | reagowaniu na incydenty **krytyczne i** poważne, | KNF proponuje dodać zwrot: „**krytyczne i**” | **Uwaga uwzględniona** |  |
|  | KNF | Uwaga o cel szczegółowy 1.4 (p 5.4) | a także w ramach współpracy transatlantyckiej z brytyjskimi i amerykańskimi instytucjami stymulującymi podnoszenie standardów cyberbezpieczeństwa przez **dostawców usług cyfrowych.** | KNF: Proponujemy uwzględnić w nowych regulacjach ryzyko koncentracji i włączenie dostawców (firm trzecich), którzy świadczą w ramach outsourcingu kluczowe usługi IT dla podmiotów sektora finansowego, do krajowego systemu cyberbezpieczeństwa (np. IBM, Asseco w sektorze Bankowości Spółdzielczej) | **Uwaga nieuwzględnienia**  Kwestia do dyskusji przy nowelizacji ustawy o ksc | **Przyjęto wyjaśnienie.** |
|  | KNF | Uwaga o cel szczegółowy 2 | Podniesienie poziomu odporności sieci i systemów teleinformatycznych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zwalczania skutków incydentów | KNF proponuje zmienić na: Podniesienie poziomu odporności **systemów informacyjnych** administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego **zapobiegania i reagowania na incydenty** | **Wyjaśnienie**  Zmiana zapisu. |  |
|  | KNF | Uwaga o cel szczegółowy 2.1 (p 6.1) | W celu zwiększenia odporności **sieci i systemów teleinformatycznych** administracji publicznej **i** **podmiotów** **KSC** na cyberzagrożenia | KNF proponuje zmienić i dodać zwroty: W celu zwiększenia odporności **systemów informacyjnych** administracji publicznej **i** **podmiotów** **KSC** na cyberzagrożenia | **Wyjaśnienie**  Narodowe Standardy Cyberbezpieczeństwa będą obowiązkowe dla administracji publicznej | **Przyjęto wyjaśnienie.** |
|  | KNF | Uwaga o cel szczegółowy 2.1 (p 6.1) | zbioru wymagań organizacyjnych i technicznych dotyczących w szczególności **bezpieczeństwa**: | KNF proponuje zamienić na zwrot: „**cyberbezpieczeństwa**” | **Uwaga nieuwzględniona**  Niepotrzebne zawężenie. | **Przyjęto wyjaśnienie.** |
|  | KNF | Uwaga o cel szczegółowy 2.1 (p 6.1) | w szczególności bezpieczeństwa:   1. aplikacji, 2. urządzeń mobilnych, 3. stacji roboczych **i urządzeń peryferyjnych**, | KNF proponuje dodać do pkt 3 zwrot:  „**i urządzeń peryferyjnych**” | **Uwaga nieuwzględniona**  Nie jest to zamknięty wykaz. | **Przyjęto wyjaśnienie.** |
|  | KNF | Uwaga o cel szczegółowy 2.1 (p 6.1) | w szczególności bezpieczeństwa:   1. aplikacji, 2. urządzeń mobilnych, 3. stacji roboczych 4. serwerów, **urządzeń sieciowych** i sieci, | KNF proponuje dodać do pkt 4 zwrot:  „**urządzeń sieciowych**” | **Uwaga nieuwzględniona**  Nie jest to zamknięty katalog. | **Przyjęto wyjaśnienie.** |
|  | KNF | Uwaga o cel szczegółowy 2.1 (p 6.1) | w szczególności bezpieczeństwa:   1. aplikacji, 2. urządzeń mobilnych, 3. stacji roboczych, 4. serwerów i sieci, 5. **modeli chmur obliczeniowych**. | KNF proponuje zamienić w pkt 5 zwrot na:  „**usług chmur obliczeniowych**” | **Uwaga nieuwzględniona**  Nie jest to zamknięty katalog. | **Przyjęto wyjaśnienie.** |
|  | KNF | Uwaga o cel szczegółowy 2.1 (p 6.1) | W celu zapewnienia bezpiecznej i optymalnej kosztowo infrastruktury przetwarzania systemów IT administracji publicznej **i podmiotów KSC** | KNF proponuje dodać zwrot: „**i podmiotów KSC**” | **Uwaga nieuwzględniona**  Nie będą obowiązkowe dla wszystkich podmiotów ksc. | **Przyjęto wyjaśnienie.** |
|  | KNF | Uwaga o cel szczegółowy 2.1 (p 6.1) |  | KNF proponuje dodać zdanie na końcu celu: **W celu zapewnienia sprawnego zarządzania incydentami wprowadzone zostaną procedury oparte na dobrych praktykach i międzynarodowych standardach.** | **Uwaga nieuwzględniona**  Wynika to już z obowiązującej ustawy o KSC. | **Przyjęto wyjaśnienie.** |
|  | KNF | Uwaga o cel szczegółowy 2.2 (p 6.2) | Działania te składają się na tak zwany bezpieczny łańcuch dostaw **budowy**, który | KNF proponuje usunąć zwrot: „**budowy**” | **Uwaga uwzględniona** |  |
|  | KNF | Uwaga o cel szczegółowy 2.2 (p 6.2) | Działania na poziomie krajowym będą obejmowały, w szczególności, wyznaczenie krajowego **orangu** ds. certyfikacji cyberbezpieczeństwa | KNF proponuje zamienić zwrot na: „**organu**” | **Uwaga uwzględniona** |  |
|  | KNF | Uwaga o cel szczegółowy 2.3 (p 6.3) | Kolejnym środkiem oceny bezpieczeństwa są okresowe testy (w tym testy penetracyjne), które pozwalają na rzeczywistą ocenę odporności systemu na zagrożenia. | KNF: Zgodnie z aktualnym kierunkiem prac grup roboczych EBA należy wypracować jednolity europejski framework dot. przeprowadzania testów penetracyjnych przez podmioty nadzorowane obejmujacy opracowanie wspólnej metodyki przeprowadzania testów oraz certyfikację podmiotów mogących przeprowadzać testy | **Wyjaśnienie**  O ile pożądane są działania w tym zakresie, to wypracowanie tego typu frameworka wykracza zakres Strategii. | **Zgodnie z ustaleniami w trakcie konferencji KNF zobowiązał się przekazać stanowisko w tej kwestii. KNF w informacji przesłanej 11.09 wycofał się z tej uwagi.** |
|  | KNF | Uwaga o cel szczegółowy 2.3 (p 6.3) | Kolejnym środkiem oceny bezpieczeństwa są okresowe testy (w tym testy penetracyjne), które pozwalają na rzeczywistą ocenę odporności systemu na zagrożenia. **W tym celu należy aktywnie wspierać działania zmierzające do opracowania wspólnego europejskiego standardu dot. przeprowadzania testów penetracyjnych obejmującego opracowanie wspólnej metodyki przeprowadzania testów oraz certyfikację podmiotów mogących przeprowadzać testy.** Ich wyniki stanowią podstawę weryfikacji przyjętych założeń w zakresie ustanowionych zabezpieczeń. | KNF proponuje dodać zdanie: **W tym celu należy aktywnie wspierać działania zmierzające do opracowania wspólnego europejskiego standardu dot. przeprowadzania testów penetracyjnych obejmującego opracowanie wspólnej metodyki przeprowadzania testów oraz certyfikację podmiotów mogących przeprowadzać testy.** | **Uwaga nieuwzględniona**  Poza zakresem Strategii. | **Zgodnie z ustaleniami w trakcie konferencji KNF zobowiązał się przekazać stanowisko w tej kwestii. KNF w informacji przesłanej 11.09 wycofał się z tej uwagi.** |
|  | KNF | Uwaga o cel szczegółowy 3.1 (p 7.1) | Poprzez instrumenty prawne **i finansowe** rząd będzie stymulował na wyższych uczelniach nauczanie | KNF proponuje dodać zwrot: „**i finansowe**” | **Uwaga nieuwzględniona**  Sposób finansowania będzie określony w Planie działań. | **Przyjęto wyjaśnienie.** |
|  | KNF | Uwaga o cel szczegółowy 3.3 (p 7.3) | Ponadto we współpracy ze środowiskiem naukowo-akademickim zostaną opracowane programy badawcze mające na celu **w szczególności**: | KNF: „**w szczególności**” | **Uwaga uwzględniona** |  |
|  | KNF | Uwaga o cel szczegółowy 4.1 (p 8.1) | podjęte będą działania w celu **zbliżenia** zarobków tych pracowników do poziomu | KNF proponuje zamienić zwrot na: „**dostosowania**” | **Uwaga nieuwzględniona**  Użyty termin jest właściwszy. | **Przyjęto wyjaśnienie.** |
|  | KNF | Uwaga o cel szczegółowy 4.3 (p 8.3) | grup docelowych (między innymi dzieci, rodziców, seniorów). **Identyfikując problem wykluczenia cyfrowego, w szczególności seniorów, należy rozwijać programy edukacyjne mające na celu budowanie ich kompetencji w cyberprzestrzeni oraz świadomości występujących zagrożeń w celu aktywnego uczestnictwa w społeczeństwie informacyjnym.** | KNF proponuje dodać zdanie: **Identyfikując problem wykluczenia cyfrowego, w szczególności seniorów, należy rozwijać programy edukacyjne mające na celu budowanie ich kompetencji w cyberprzestrzeni oraz świadomości występujących zagrożeń w celu aktywnego uczestnictwa w społeczeństwie informacyjnym.** | **Wyjaśnienie**  Kwestia aktywizacji zawodowej grup docelowych może być elementem Planu działań. | **Zgodnie z ustaleniami w trakcie konferencji KNF zobowiązał się przekazać stanowisko w tej kwestii. KNF w informacji przesłanej 11.09 wycofał się z tej uwagi.** |
|  | KNF | Uwaga do Uzasadnienia (Pkt 4. Podmioty na które oddziałuje projekt) |  | KNF: „Komisja Nadzoru Finansowego jest szczególnym organem administracji publicznej – państwowej, ale usytuowanym poza strukturą administracji rządowej” WYROK Trybunału Konstytucyjnego z dnia 15 czerwca 2011 r. Sygn. akt K 2/09 (Pkt. 5.11, 5.12, 6) | **Uwaga uwzględniona** |  |
|  | Straż Graniczna | Uwaga do Oceny skutków regulacji (p 6 Wpływ na sektor finansów publicznych) |  | Straż Graniczna proponuje uzupełnić pkt 6 Oceny Skutków Regulacji o następującą informację:  „**W związku z realizacją przez Straż Graniczną przedmiotowej Strategii powstaną dodatkowe skutki finansowe w kwocie ok. 33 mln zł z przeznaczeniem na rozbudowę i utrzymanie systemów bezpieczeństwa, co wiąże się z koniecznością dodatkowego zabezpieczenia wskazanej kwoty w budżecie Straży Granicznej.**” | **Uwaga nieuwzględniona**  Poza zakresem Strategii. | **Przyjęto wyjaśnienie.** |
|  | NIK | Uwaga ogólna |  | Nie określa się wartości mierników pozwalających określić stopień realizacji celu głównego oraz osiągnięcia celów szczegółowych. Brak jednoznacznych mierników i wskaźników realizacji celów nie będzie pozwalał na skuteczne monitorowanie ich realizacji, a Strategia będzie pełnić rolę spisu poszczególnych luźno powiązanych ze sobą zadań państwa, które jednak nie łączyć się będą w logiczną jedną całość pozwalającą ocenić stan bezpieczeństwa Państwa. | **Uwaga nieuwzględniona**  Mierniki będą określone w poszczególnych zadaniach i działaniach, a nie na poziomie Strategii. | **Przyjęto wyjaśnienie.** |
|  | NIK | Uwagi do p. 10 (Zarządzanie Strategią) |  | Umożliwia się opracowanie odrębnego Planu działań oraz odrębnego sprawozdania z jego wykonania przez Ministra Obrony Narodowej, który zdaniem NIK może utrudnić współpracę, monitorowanie oraz koordynację? Strategii, ze względu na fakt, iż zagrożenia cyberprzestrzeni w dzisiejszych czasach nie są jednoznacznie powiązane jedynie z domeną cywilną czy militarną. Ponadto należy zauważyć, iż to Minister właściwy do spraw informatyzacji jako jedyny jest odpowiedzialny za monitorowanie wdrażania całej Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej oraz realizację planów działań na rzecz jej wdrożenia (art. 45 ust. 1 pkt 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa). | **Uwaga nieuwzględniona**  Plan MON nadal jest przekazywany koordynatorowi Strategii. Nie ma ryzyka utrudnienia współpracy w tym zakresie. | **W trakcie konferencji NIK zobowiązał się do przekazania stanowiska w tej kwestii. Ostatecznie stanowisko NIK nie zostało przekazane MC.** |
|  | NIK | Uwago do p. 11 (Finansowanie) |  | Nie podejmuje się próby stworzenia całościowego systemu finansowania zadań zapewniających bezpieczeństwo w cyberprzestrzeni RP poprzestając jedynie na doraźnych rozwiązaniach np. środki z Narodowego Centrum Badań i Rozwoju lub środki Unii Europejskiej. | **Wyjaśnienie**  Do dyskusji przy nowelizacji ustawy | **Przyjęto wyjaśnienie.** |
|  | NASK | Uwagi do p. 10 (Zarządzanie Strategią) |  | NASK: W punkcie „Zarządzanie strategią”, w procesie opracowywania *Panu działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa*, wskazane byłoby uwzględnienie CSIRT poziomu krajowego. | **Wyjaśnienie**  Plan działań będzie konsultowany także z zespołami CSIRT |  |
|  | NASK | Uwago do p. 11 (Finansowanie) |  | NASK: Wdrażanie bardzo ambitnych celów postawionych w Strategii może być utrudnione poprzez brak jasnych źródeł finasowania. Wskazane byłoby utworzenie budżetu na rzecz wdrażania *Strategii*, którego zarządzaniem zajmowałby się Pełnomocnik. | **Uwaga częściowo uwzględniona**  Kwestie finansowania będą przedmiotem prac nad Planem działań oraz w ramach przeglądu ustawy o ksc. |  |
|  | NASK | Uwaga ogólna |  | NASK: Ponieważ od 27 czerwca obowiązuje *Cybersecurity Act* wskazane byłoby odniesienie się do tej regulacji i zaadresowanie wyzwań stojących przed RP w tym zakresie, a więc m.in. powołanie Krajowego organu ds. certyfikacji cyberbezpieczeństwa (KOCC), Krajowej jednostki akredytującej, Jednostek oceniających zgodność | **Uwaga uwzględniona, zmiana w zapisie** |  |
|  | PCA | Uwaga o cel szczegółowy 2.2 (6.2) | Ważnym elementem zapewnienia jakości w łańcuchu dostaw jest ocena i certyfikacja produktów (w szczególności oprogramowania, urządzeń i usług). Priorytetowe w tym zakresie będzie utworzenie, a następnie utrzymanie i rozwój krajowego systemu oceny i certyfikacji cyberbezpieczeństwa **bazującego na działalności akredytowanych jednostek oceniających zgodność**, co umożliwi Polsce uzyskanie pełnego i rozpoznawanego na arenie europejskiej i międzynarodowej statusu państwa producenta w dziedzinie rozwiązań cyberbezpieczeństwa. | PCA proponuje dopisanie: „**bazującego na działalności akredytowanych jednostek oceniających zgodność**” | **Uwaga uwzględniona** |  |
|  | PCA | Uwaga o cel szczegółowy 2.2 (6.2) | Działania na poziomie krajowym będą obejmowały, w szczególności, wyznaczenie krajowego organu ds. certyfikacji cyberbezpieczeństwa, który będzie wydawał europejskie certyfikaty cyberbezpieczeństwa oraz nadzorował krajowe jednostki oceniające zgodność produktów, usług i procesów z wymaganiami określonymi w europejskich programach certyfikacji cyberbezpieczeństwa **oraz wspierał krajową jednostkę akredytującą – Polskie Centrum Akredytacji, w monitorowaniu i nadzorowaniu działalności akredytowanych jednostek oceniających zgodność w odniesieniu do wymagań rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881**. | PCA proponuje dopisanie: „**oraz wspierał krajową jednostkę akredytującą – Polskie Centrum Akredytacji, w monitorowaniu i nadzorowaniu działalności akredytowanych jednostek oceniających zgodność w odniesieniu do wymagań rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881**” | **Uwaga uwzględniona** | **W propozycji zmieniono wyraz „wspierał” na „współpracował z” i dostosowano resztę zdania żeby uzyskać logiczne brzmienie.**  **Przyjęta wersja:**  **„oraz współpracował z krajową jednostką akredytującą – Polskim Centrum Akredytacji, w celu monitorowania i nadzorowania działalności akredytowanych jednostek oceniających zgodność w odniesieniu do wymagań rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881”** |