

Nazwa projektu Uchwała Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029	Data sporządzenia 08.07.2025
Ministerstwo wiodące i ministerstwa współpracujące Ministerstwo Cyfryzacji	Źródło: Upoważnienie ustawowe: art. 68 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222)
Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu Paweł Olszewski, Sekretarz Stanu w Ministerstwie Cyfryzacji	Nr w Wykazie prac legislacyjnych i programowych Rady Ministrów: ID131
Kontakt do opiekuna merytorycznego projektu Łukasz Wojewoda, Dyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji, tel. (22) 245 59 22, e-mail: sekretariat.dc@cyfra.gov.pl Michał Strzelczyk, Departament Cyberbezpieczeństwa w Ministerstwie Cyfryzacji, tel. 734 117 947, e-mail: michal.strzelczyk@cyfra.gov.pl	

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Opracowanie i przyjęcie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, zwanej dalej „Strategią”, jest wymogiem realizacji przepisu art. 68 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Wraz z końcem 2024 r. upłynął 5-letni okres na jaki ustanowiona została Strategia na lata 2019–2024, przyjęta uchwałą nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (M.P. poz. 1037).

Strategia określa cele strategiczne oraz odpowiednie środki polityczne, które mają na celu podnoszenie i utrzymywanie poziomu cyberbezpieczeństwa Rzeczypospolitej Polskiej. Stale zmieniające się uwarunkowania związane z bezpieczeństwem w cyberprzestrzeni wymagają szybkiej i zdecydowanej reakcji organów państwa. Poziom zagrożeń w cyberprzestrzeni wzrasta w wymiarze globalnym i krajowym, gdyż pojawiają się nowe rodzaje zagrożeń oraz wzrasta aktywność grup prowadzących nielegalne działania w świecie cyfrowym, począwszy od hakywistów, przez grupy cyberprzestępcze o charakterze zarobkowym, po grupy powiązane z innymi państwami. Zagrożenia te mają wpływ na codzienne funkcjonowanie, bezpieczeństwo i prywatność obywateli (również dzieci, młodzieży oraz seniorów), przedsiębiorstw i instytucji publicznych. Ważne przy tym jest zapewnienie jak najszerzej współpracy przy wdrażaniu i rozwijaniu Krajowego Systemu Cyberbezpieczeństwa, zwanego dalej „KSC”, ze strony ministerstw i innych organów władzy państwowej.

Przyjęcie nowej Strategii pozwoli należycie zaplanować strategiczne kierunki działań państwa, które podniosą poziom cyberbezpieczeństwa w skali całego kraju, zarówno w odniesieniu do instytucji publicznych, podmiotów gospodarczych oraz obywateli. Pozwoli to w sposób skoordynowany i kompleksowy odpowiadać administracji publicznej na rosnący poziom zagrożeń w cyberprzestrzeni. Dzięki realizacji zadań przewidzianych w Strategii ograniczone zostaną ryzyka związane z tymi zagrożeniami, co umożliwi zapewnienie pomyślnego rozwoju gospodarczego przy zachowaniu możliwie wysokiego poziomu bezpieczeństwa w sferze cyfrowej. Przyjęcie a następnie wdrożenie Strategii stanowić będzie istotny wkład w wzmacnianie bezpieczeństwa narodowego, tak w sferze cywilnej, jak i wojskowej, zarówno w wymiarze wewnętrznym i międzynarodowym. Dzięki temu wzmocnieniami uleganie też pozycja Rzeczypospolitej Polskiej w ramach Organizacji Traktatu Północnoatlantyckiego, Unii Europejskiej oraz w relacjach dwu- i wielostronnych.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Projektowana uchwała ma na celu ustanowienie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029. Dokument ma charakter polityczno-strategiczny, natomiast na poziomie operacyjnym realizację jego zapisów zapewnia szczegółowy plan działań, stanowiący załącznik do Strategii. Plan działań opisuje podmioty zaangażowane w realizację Strategii oraz środki pozwalające na jej wdrożenie. Przy opracowywaniu Strategii korzystano z dotychczasowych doświadczeń funkcjonowania KSC. Nowa Strategia uwzględnia także zmiany w środowisku bezpieczeństwa międzynarodowego oraz kwestie związane postępem technologicznym i powszechną cyfryzacją wszystkich dziedzin życia.

Strategia uwzględnia następujące kwestie:

- 1) cele i priorytety w zakresie cyberbezpieczeństwa;
- 2) podmioty zaangażowane we wdrażanie i realizację Strategii;
- 3) środki służące realizacji celów Strategii;
- 4) określenie środków w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym zasady współpracy między sektorem publicznym i prywatnym;
- 5) podejście do oceny ryzyka;

- 6) działania odnoszące się do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa;
- 7) działania odnoszące się do planów badawczo-rozwojowych w zakresie cyberbezpieczeństwa.

Strategia uwzględnia również materię przeciwdziałania i zwalczania cyberprzestępczości oraz uzyskania zdolności do prowadzenia pełnego spektrum działań w cyberprzestrzeni. Ponadto Strategia uwzględnia międzynarodową współpracę w zakresie cyberbezpieczeństwa.

Strategia wyznacza najważniejsze kierunki działań państwa w obszarze cyberbezpieczeństwa. W dokumencie sformułowany jest cel główny związany z podniesieniem poziomu odporności krajowych podmiotów funkcjonujących w cyberprzestrzeni, jak również sześć celów szczegółowych odnoszących się do:

- 1) doskonalenia krajowego systemu cyberbezpieczeństwa;
- 2) przeciwdziałania i zwalczania cyberprzestępczości oraz uzyskania zdolności do prowadzenia pełnego spektrum działań w cyberprzestrzeni;
- 3) podniesienia poziomu odporności systemów informacyjnych w sferze publicznej oraz prywatnej;
- 4) zwiększanie potencjału krajowej bazy technologiczno-przemysłowej oraz wzmocnienie suwerenności technologicznej w obszarze cyberbezpieczeństwa;
- 5) budowania świadomości, wiedzy i kompetencji kadr podmiotów krajowego systemu cyberbezpieczeństwa oraz obywateli;
- 6) wzmocnienia pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa.

Dokument określa szereg przedsięwzięć, które pozwolą osiągnąć zakładane cele, w tym zmiany regulacyjne, instytucjonalne, działania operacyjne i techniczne oraz inwestycyjne. Przewidziane kierunki interwencji państwa wynikają z wniosków oraz doświadczeń funkcjonowania Krajowego Systemu Cyberbezpieczeństwa, zmian technologicznych oraz zmian w środowisku bezpieczeństwa międzynarodowego, jak również ewoluującego i rozszerzającego się prawodawstwa dotyczącego cyberbezpieczeństwa, w tym na poziomie Unii Europejskiej.

Zakres Strategii jest znacząco odmienny od dokumentu obowiązującego w latach 2019–2024. Nowa Strategia obejmuje wiele nowych elementów, co wynika z ewolucji Krajowego Systemu Cyberbezpieczeństwa oraz zmiany postrzegania samego cyberbezpieczeństwa. Nowym elementem jest dołączony w postaci załącznika „Plan działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej”, który zawiera nowe szczegółowo określone zadania służące realizacji Strategii.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Posiadanie krajowej strategii odnoszącej się do bezpieczeństwa sieci i systemów informatycznych było wymagane przepisem art. 7 dyrektywy Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (NIS) (Dz. Urz. UE L 194 z 19.07.2016, str. 1). Państwa członkowskie Unii Europejskiej przyjmowały dotychczas swoje krajowe strategie cyberbezpieczeństwa na podstawie tej dyrektywy. Wyżej wskazana dyrektywa została zastąpiona przez 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 (NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80.). Nowa regulacja także nakłada na państwa członkowskie obowiązek przyjęcia krajowych strategii cyberbezpieczeństwa (art. 7).

Państwa członkowskie Unii Europejskiej przyjmowały swoje krajowe strategie cyberbezpieczeństwa w następujących latach:

- 2016: Bułgaria, Litwa, Malta, Niemcy, Słowenia, Wielka Brytania.
- 2017: Grecja, Polska, Szwecja, Włochy.
- 2018: Dania, Holandia, Luksemburg, Węgry.
- 2019: Estonia, Hiszpania, Irlandia, Łotwa, Polska, Portugalia.
- 2020: Cypr, Grecja.
- 2021: Austria, Belgia, Czechy, Luksemburg, Niemcy, Słowacja.
- 2022: Dania, Rumunia, Włochy.
- 2023: Łotwa.

Dokument o charakterze strategicznym w obszarze cyberbezpieczeństwa posiadają również państwa europejskie spoza Unii Europejskiej, np. Islandia (2022 r.), Norwegia (2019 r.), Szwajcaria (2018 r.), oraz państwa pozaeuropejskie, np. USA - „National Cybersecurity Strategy” (2023 r.).

4. Podmioty, na które oddziałuje projekt			
Grupa	Wielkość	Źródło danych	Oddziaływanie
Centralna administracja rządowa – ministerstwa oraz jednostki im podległe i nadzorowane	20 urzędów obsługujących ministrów + ok. kilkaset jednostek podległych i nadzorowanych	Skład Rady Ministrów oraz urzędów obsługujących ministrów	Udział w realizacji Strategii oraz wpływ na działalność w zakresie cyberbezpieczeństwa.
Terenowa administracja rządowa – wojewodowie, ich jednostki podległe i nadzorowane oraz administracja zespólna i niezespólna w województwie	16 urzędów wojewódzkich + kilkaset jednostek podległych i nadzorowanych przez wojewodów oraz administracji zespólna i niezespólna w województwie	Podział administracyjny Rzeczypospolitej Polskiej	Udział w realizacji Strategii oraz wpływ na działalność w zakresie cyberbezpieczeństwa.
Komisja Nadzoru Finansowego	1	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa	Udział w realizacji Strategii oraz wpływ na działalność w zakresie cyberbezpieczeństwa.
CSIRT poziomu krajowego	3	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa	Udział w realizacji Strategii oraz wpływ na działalność w zakresie cyberbezpieczeństwa.
Operatorzy usług kluczowych	378	Wykaz operatorów usług kluczowych	Pośredni wpływ na działalność w zakresie cyberbezpieczeństwa.
Inne podmioty publiczne	>10 000	Wiedza ogólnodostępna	Pośredni wpływ na działalność w zakresie cyberbezpieczeństwa oraz możliwy udział w realizacji Strategii w przypadku podmiotów w ramach administracji rządowej.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Projekt uchwały został poddany uzgodnieniom i opiniowaniu, a także został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego ministra właściwego do spraw informatyzacji.

Z uwagi na to, iż projektowana uchwała Rady Ministrów ma charakter wewnętrzny nie przewiduje się przeprowadzania konsultacji publicznych w ramach rządowego procesu legislacyjnego. W ramach przeprowadzonych konsultacji społecznych projektu Strategii Cyfryzacji Państwa konsultowana była także jej część dotycząca cyberbezpieczeństwa. Przeprowadzone konsultacje zostały wykorzystane również na potrzeby prac nad Strategią. Ponadto projekt Strategii był prekonsultowany z Radą do Spraw Cyfryzacji, która jest organem opiniodawczo-doradczym reprezentującym różne środowiska społeczne i gospodarcze, jak również z ponad 30 instytucjami publicznymi oraz z podmiotami naukowymi. Ponadto za nie przeprowadzaniem ponownych konsultacji społecznych przemawia także potrzeba pilnego uchwalenia tej Strategii z uwagi na to, że upłynął okres na jaki została przyjęta poprzednia Strategia.

W ramach 14-dniowego opiniowania projekt uchwały został skierowany do następujących podmiotów:

- 1) Agencji Bezpieczeństwa Wewnętrznego;
- 2) Agencji Wywiadu;
- 3) Biura Bezpieczeństwa Narodowego;
- 4) Centralnego Biura Antykorupcyjnego;
- 5) Centralnego Ośrodka Informatyki;
- 6) Instytutu Łączności – Państwowego Instytutu Badawczego;
- 7) Komendy Głównej Policji;
- 8) Komisji Nadzoru Finansowego;

- 9) Krajowej Rady Radiofonii i Telewizji;
- 10) Najwyższej Izby Kontroli;
- 11) Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego;
- 12) Polskiego Komitetu Normalizacyjnego;
- 13) Prezesa Głównego Urzędu Statystycznego;
- 14) Prezesa Urzędu Komunikacji Elektronicznej;
- 15) Prezesa Urzędu Ochrony Danych Osobowych;
- 16) Prezesa Urzędu Ochrony Konkurencji i Konsumentów;
- 17) Prezesa Urzędu Zamówień Publicznych;
- 18) Prokuraturii Generalnej Rzeczypospolitej Polskiej;
- 19) Prokuratury Krajowej;
- 20) Rządowego Centrum Bezpieczeństwa;
- 21) Rzecznika Małych i Średnich Przedsiębiorców;
- 22) Rzecznika Praw Obywatelskich;
- 23) Służby Kontrwywiadu Wojskowego;
- 24) Służby Ochrony Państwa;
- 25) Służby Wywiadu Wojskowego.

Ponadto projekt uchwały został przekazany do zaopiniowania Radzie do Spraw Cyfryzacji stosownie do z art. 17 ust. 2 pkt 3 i ust. 4 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557 i 1717).

Projekt uchwały został przekazany również do zaopiniowania Komisji Wspólnej Rządu i Samorządu Terytorialnego.

Dodatkowo zgodnie z art. 21f ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju (Dz. U. z 2025 r. poz. 198) projekt uchwały został przedstawiony do zaopiniowania ministrowi właściwemu do spraw rozwoju regionalnego w celu oceny zgodności ze średniookresową strategią rozwoju kraju oraz z wymogami określonymi w art. 21e tej ustawy.

Projekt uchwały nie mieści się w zakresie działalności Rady Działalności Pożytku Publicznego oraz Rady Dialogu Społecznego – wobec tego nie został przekazany do zaopiniowania do tych podmiotów.

Wyniki z przeprowadzonego opiniowania zostaną przedstawione w raporcie.

6. Wpływ na sektor finansów publicznych

(ceny stałe z r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0-10)
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Przyjęte rozwiązania nie spowodują dodatkowych skutków finansowych dla sektora finansów publicznych, w tym budżetu państwa i budżetów jednostek samorządu terytorialnego.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Nie dotyczy.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

Skutki

Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	Łącznie (0-10)
W ujęciu pieniężnym (w mln zł, ceny stałe z r.)	duże przedsiębiorstwa	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
W ujęciu niepieniężnym	duże przedsiębiorstwa	Brak wpływu.						
	sektor mikro-, małych i średnich przedsiębiorstw	Brak wpływu.						
	rodzina, obywatele oraz gospodarstwa domowe	Brak wpływu.						
Niemierzalne	(dodaj/usuń)							
	(dodaj/usuń)							
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń		Projekt uchwały nie ma wpływu na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na sytuację ekonomiczną i społeczną rodziny, osób niepełnosprawnych oraz osób starszych, a także na obywateli i gospodarstwa domowe.						
8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu								
☒ nie dotyczy								
Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).				☐ tak ☐ nie ☒ nie dotyczy				
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne: ...				☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne: ...				
Wprowadzane obciążenia są przystosowane do ich elektronizacji.				☐ tak ☐ nie ☐ nie dotyczy				
Komentarz:								
9. Wpływ na rynek pracy								
Brak wpływu projektowanej regulacji na rynek pracy.								
10. Wpływ na pozostałe obszary								
☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne: ...			☐ demografia ☐ mienie państwowe			☒ informatyzacja ☐ zdrowie		
Omówienie wpływu		Realizacja przedsięwzięć z Planu działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029 przyczyni się do zwiększenia bezpieczeństwa usług cyfrowych.						
11. Planowane wykonanie przepisów aktu prawnego								
Uchwała wejdzie w życie z dniem następującym po dniu ogłoszenia.								
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?								
Minister właściwy do spraw informatyzacji we współpracy z Pełnomocnikiem Rządu do Spraw Cyberbezpieczeństwa, innymi ministrami i właściwymi kierownikami urzędów centralnych, dokonuje przeglądu Strategii co 2 lata.								
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)								
Brak załączników.								