UZASADNIENIE

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 (Dz. U. z 2024 r. poz. 1077 i 1222). 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 i regulacyjne, 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 haktywistów, przez grupy cyberprzestępcze o charakterze zarobkowym, po grupy powiązane z innymi państwami. Zagrożenia te mają wpływ na codzienne funkcjonowanie, bezpieczeństwo i prywatność obywateli, przedsiębiorstw i instytucji publicznych. Ważne przy tym jest zapewnienie jak najszerszej współpracy przy wdrażaniu i rozwijaniu Krajowego Systemu Cyberbezpieczeństwa ze strony ministerstw i innych organów władzy państwowej.

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. Nowością jest dołączony w postaci załącznika „Plan działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej", który zawiera nowe szczegółowo określone zadania służące realizacji Strategii.

W zakresie realizacji celu szczegółowego „Rozwój krajowego systemu cyberbezpieczeństwa" przewidziano następujące kierunki interwencji:

1) doskonalenie krajowego systemu cyberbezpieczeństwa;

2) podniesienie efektywności krajowego systemu cyberbezpieczeństwa;

3) rozwój zintegrowanego systemu wymiany informacji na potrzeby zapewnienia ciągłości funkcjonowania administracji państwowej, bezpieczeństwa narodowego i ochrony ludności;

4) zwiększanie cyberbezpieczeństwa podmiotów nadzorowanych przez organy właściwe do spraw cyberbezpieczeństwa;

5) wypracowanie i wdrożenie metodyki szacowania ryzyka na poziomie krajowym.

W zakresie realizacji celu szczegółowego „Przeciwdziałanie i zwalczanie cyberprzestępczości oraz uzyskanie zdolności do prowadzenia pełnego spektrum działań w cyberprzestrzeni" przewidziano następujące kierunki interwencji:

1) wprowadzenie regulacji skuteczniej pozwalających zwalczać cyberprzestępczość;
2) wzmocnienie wyspecjalizowanych struktur zwalczania cyberprzestępczości;
3) podnoszenie zdolności analitycznych organów ścigania, służb specjalnych i wymiaru sprawiedliwości przy wykorzystaniu nowych technologii.

W zakresie realizacji celu szczegółowego „Podniesienie poziomu odporności systemów informacyjnych w sferze publicznej (w tym militarnej) oraz prywatnej" przewidziano następujące kierunki interwencji:

1) podniesienie poziomu odporności systemów informacyjnych;
2) rozwój krajowej kryptologii, w tym migracja do kryptografii postkwantowej oraz rozwój technologii kwantowych;
3) rozwiązania chmurowe dla wzmocnienia odporności systemów informacyjnych.

W zakresie realizacji celu szczegółowego „Zwiększanie potencjału krajowej bazy technologiczno-przemysłowej oraz wzmocnienie suwerenności technologicznej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa" przewidziano następujące kierunki interwencji:

1) wzmocnienie bezpieczeństwa łańcucha dostaw na poziomie krajowym i międzynarodowym;
2) stymulowanie badań, rozwoju i innowacji w obszarze cyberbezpieczeństwa.

W zakresie realizacji celu szczegółowego „Budowanie świadomości, wiedzy i kompetencji kadr podmiotów krajowego systemu cyberbezpieczeństwa oraz obywateli i przedsiębiorców" przewidziano następujące kierunki interwencji:

1) zwiększenie świadomości i wiedzy oraz wzmocnienie kompetencji kadr podmiotów krajowego systemu cyberbezpieczeństwa;
2) rozwój świadomości i wiedzy obywateli i przedsiębiorców z zakresu cyberbezpieczeństwa.

W zakresie realizacji celu szczegółowego „Wzmocnienie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa" przewidziano następujące kierunki interwencji:

1) aktywna współpraca międzynarodowa na poziomie strategiczno-politycznym i prawnym;

2) aktywna współpraca międzynarodowa na poziomie operacyjnym i technicznym;

3) koordynacja działań na arenie międzynarodowej w zakresie współpracy cywilno-wojskowej w obszarze cyberbezpieczeństwa.

Projektowana uchwała wejdzie w życie z dniem następującym po dniu ogłoszenia. Przyjęty termin wejścia w życie wynika z potrzeby niezwłocznego wprowadzenia do systemu prawnego nowej Strategii, w związku z upływem okresu obowiązywania Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024.

Projekt nie jest sprzeczny z prawem Unii Europejskiej.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2025 r. poz. 468).

Projekt nie wymaga przedłożenia instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projekt uchwały nie będzie miał wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców.

Projekt zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji.