Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej

Spis treści

Wykaz stosowanych skrótów

1) ABW – Agencja Bezpieczeństwa Wewnętrznego;
2) akt o cyberbezpieczeństwie – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013;
3) akt o cyberodporności – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828;
4) AW – Agencja Wywiadu;
5) B+R – badania i rozwój;
6) B+R+I – badania, rozwój i innowacje;
7) CBZC – Centralne Biuro Zwalczania Cyberprzestępczości;
8) CPPC – Centrum Projektów Polska Cyfrowa;
9) CSAM – treści przedstawiające wykorzystywanie seksualne dzieci;
10) CSIRT – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego;
11) CTI – rozpoznawanie zagrożeń w cyberprzestrzeni;
12) DEP – Program Cyfrowa Europa;
13) DKWOC – Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni;
14) DLT – technologia rozproszonego rejestru;
15) DUC – dostawca usług cyfrowych;
16) dyrektywa 2022/2556 – dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2556 z dnia 14 grudnia 2022 r. w sprawie zmiany dyrektyw 2009/65/WE, 2009/138/WE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 oraz (UE) 2016/2341 w odniesieniu do operacyjnej odporności cyfrowej sektora finansowego;
17) dyrektywa CER – dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE;
18) dyrektywa NIS – dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii;
19) dyrektywa NIS 2 – dyrektywa 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, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148;
20) EBSI – Europejska Infrastruktura Usług Blockchain;
21) ECCC – Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa;
22) ECSC – Eksperckie Centrum Szkolenia Cyberbezpieczeństwa;
23) ENISA – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa;
24) EUCC – Europejski system certyfikacji cyberbezpieczeństwa oparty na wspólnych kryteriach;
25) ICS – przemysłowe systemy sterowania;
26) ICT – technologie informacyjno-telekomunikacyjne;
27) IK – infrastruktura krytyczna;

28) IŁ – Instytut Łączności – Państwowy Instytut Badawczy;
29) Inicjatywa WIIP – Inicjatywa „Wspólna Infrastruktura Informatyczna Państwa”;
30) IoT – Internet Rzeczy;
31) ISAC – Centrum Wymiany i Analizy Informacji;
32) IT – technologie informacyjne;
33) JST – jednostki samorządu terytorialnego;
34) Kodeks Sieci – rozporządzenie delegowane Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej;
35) KNF – Komisja Nadzoru Finansowego;
36) KG PSP – Komenda Główna Państwowej Straży Pożarnej;
37) KG SG – Komenda Główna Straży Granicznej;
38) Kodeks karny – ustawa z dnia 6 czerwca 1997 r. – Kodeks karny;
39) KSC – krajowy system cyberbezpieczeństwa;
40) MAP – Ministerstwo Aktywów Państwowych, urząd obsługujący ministra właściwego do spraw aktywów państwowych;
41) MC – Ministerstwo Cyfryzacji, urząd obsługujący ministra właściwego do spraw informatyzacji;
42) MEN – Ministerstwo Edukacji Narodowej, urząd obsługujący ministra właściwego do spraw oświaty i wychowania;
43) MF – Ministerstwo Finansów, urząd obsługujący ministra właściwego do spraw budżetu, ministra właściwego do spraw finansów publicznych i ministra właściwego do spraw instytucji finansowych;
44) MI – Ministerstwo Infrastruktury, urząd obsługujący ministra właściwego do spraw transportu, ministra właściwego do spraw gospodarki morskiej, ministra właściwego do spraw żeglugi śródlądowej i ministra właściwego do spraw gospodarki wodnej;
45) ME – Ministerstwo Energii, urząd obsługujący ministra właściwy do spraw energii i ministra właściwego do spraw gospodarki surowcami energetycznymi;
46) MKSS – Minister Koordynator Służb Specjalnych;
47) MNiSW – Ministerstwo Nauki i Szkolnictwa Wyższego, urząd obsługujący ministra właściwego do spraw szkolnictwa wyższego i nauki;
48) MON – Ministerstwo Obrony Narodowej;
49) MRiT – Ministerstwo Rozwoju i Technologii, urząd obsługujący ministra właściwego do spraw gospodarki oraz ministra właściwego do spraw budownictwa, planowania i zagospodarowania przestrzennego oraz mieszkalnictwa;
50) MS – Ministerstwo Sprawiedliwości;
51) MSWiA – Ministerstwo Spraw Wewnętrznych i Administracji, urząd obsługujący ministra właściwego do spraw wewnętrznych, ministra właściwego do spraw administracji publicznej i ministra właściwego do spraw wyznań religijnych oraz mniejszości narodowych i etnicznych;
52) MSZ – Ministerstwo Spraw Zagranicznych, urząd obsługujący ministra właściwego do spraw zagranicznych i ministra właściwego do spraw członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej;
53) MZ – Ministerstwo Zdrowia, urząd obsługujący ministra właściwego do spraw zdrowia;
54) NASK – Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy;
55) NATO – Organizacja Traktatu Północnoatlantyckiego;
56) NCBR – Narodowe Centrum Badań i Rozwoju;
57) NCC-PL – Krajowe Centrum Kompetencji Cyberbezpieczeństwa;

58) NCH – Krajowy Cyber Hub;
59) OChK – Operator Chmury Krajowej;
60) ONZ – Organizacja Narodów Zjednoczonych;
61) OUK – operator usługi kluczowej;
62) organ właściwy – organ właściwy do spraw cyberbezpieczeństwa, o którym mowa w art. 41 ustawy o KSC;
63) OT – technologie operacyjne;
64) QKD – kwantowa dystrybucja klucza;
65) PCOC – Połączone Centrum Operacyjne Cyberbezpieczeństwa;
66) Pełnomocnik – Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa;
67) Plan działań – Plan działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej;
68) PK – Prokuratura Krajowa;
69) PWCyber – Program Współpracy w Cyberbezpieczeństwie;
70) PZP – ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych;
71) RM – Rada Ministrów;
72) RCB – Rządowe Centrum Bezpieczeństwa;
73) RP – Rzeczpospolita Polska;
74) RON – resort obrony narodowej;
75) rozporządzenie 2022/2554 – rozporządzenie 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;
76) SBŁP – System Bezpiecznej Łączności Państwowej;
77) SKW – Służba Kontrwywiadu Wojskowego;
78) Strategia – Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej;
79) SWW – Służba Wywiadu Wojskowego;
80) SZ RP – Siły Zbrojne Rzeczypospolitej Polskiej;
81) UE – Unia Europejska;
82) UKE – Urząd Komunikacji Elektronicznej;
83) ustawa o KSC – ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
84) ustawa o KSCC – ustawa z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa;
85) WIŁ – Wojskowy Instytut Łączności – Państwowy Instytut Badawczy.

1. Wstęp – przesłanki do działań zwiększających cyberbezpieczeństwo

Od czasu przyjęcia uchwałą nr 125 Rady Ministrów z dnia 22 października 2019 r.[1)] Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej (Strategia) na lata 2019–2024, rozwój społeczny i gospodarczy niezmiennie pozostaje zależny od szybkiego i nieskrępowanego dostępu do informacji oraz jej wykorzystania w zarządzaniu, produkcji, sektorze usług oraz sektorze publicznym. Działania podjęte na podstawie Strategii na lata 2019–2024 pozwoliły, aby wszystkie sektory polskiej gospodarki rozwijały się w wymiarze cyfrowym, a społeczeństwo i państwo funkcjonowały w sposób zapewniający możliwy do osiągnięcia poziom cyberbezpieczeństwa.

Poziom zagrożeń w cyberprzestrzeni nadal jednak 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 lub wręcz bezpośrednio działające w ramach instytucji nieprzyjaznych państw. Zagrożenia te mają wpływ na codzienne funkcjonowanie, bezpieczeństwo i prywatność obywateli (w szczególności dzieci, młodzieży oraz seniorów), przedsiębiorstw i instytucji publicznych.

Diametralne zmiany w środowisku bezpieczeństwa skutkują m.in. trwającymi nieustannie wrogimi i szkodliwymi działaniami w cyberprzestrzeni. Rosyjska pełnoskalowa agresja na Ukrainę wiązała się także z wysokim natężeniem cyberataków na jej systemy informacyjne i infrastrukturę informatyczną. Obiektem coraz liczniejszych cyberataków stała się również polska cyberprzestrzeń, których część jest elementem niespotykanych dotychczas na taką skalę działań hybrydowych podejmowanych wobec Rzeczypospolitej Polskiej (RP) oraz innych krajów Unii Europejskiej (UE) i Organizacji Traktatu Północnoatlantyckiego (NATO). Tocząca się walka o dominację gospodarczą, obejmująca m.in. produkty i surowce niezbędne dla rozwoju technologii (w tym tzw. wojna o chipy), digitalizacja i rozwój usług cyfrowych dodatkowo przyspieszone przez pandemię COVID-19, rozwój nowych i przełomowych technologii (takich jak sztuczna inteligencja czy technologie kwantowe), mających wpływ na wszystkie obszary funkcjonowania społeczeństw, gospodarek i systemów bezpieczeństwa narodowego, to najważniejsze czynniki przyczyniające się do diametralnego przeobrażania się świata. Mają one również wpływ na bezpieczeństwo cyberprzestrzeni.

Poważne kryzysy, takie jak pandemia COVID-19 oraz wojna Federacji Rosyjskiej z Ukrainą, pokazały, jak ważne jest zapewnienie bezpieczeństwa łańcucha dostaw i jak jego zakłócenia mogą mieć negatywne wielosektorowe i transgraniczne skutki gospodarcze i społeczne. Wobec powyższego zapewnienie cyberbezpieczeństwa łańcucha dostaw na potrzeby utrzymania krytycznej działalności społecznej i gospodarczej, ciągłości działania administracji publicznej i Sił Zbrojnych Rzeczypospolitej Polskiej (SZ RP) oraz usług realizowanych na ich rzecz staje się kluczowym wyzwaniem, przed jakim stoi RP.

W obliczu nowych zagrożeń i rosnącej ich skali, biorąc pod uwagę ich transgraniczny charakter, szczególne znaczenie ma współpraca na arenie międzynarodowej w ramach organizacji międzynarodowych, takich jak UE, NATO czy Organizacja Narodów Zjednoczonych (ONZ), oraz w formacie dwustronnym i wielostronnym, w szczególności z najbliższymi sojusznikami i partnerami.

Rolą państwa jest podjęcie działań, które pozwolą systemowo zwiększać poziom cyberbezpieczeństwa krajowego i ograniczać ryzyka związane z cyberprzestrzenią, a w szczególności zapewnić odporność na zagrożenia kluczowych zasobów i usług z punktu widzenia działalności społecznej, gospodarczej, administracji publicznej oraz bezpieczeństwa i obronności państwa. Przyjęcie nowej Strategii wynika z 5-letnich ram czasowych określonych w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[2)] (ustawa o KSC) oraz jest podyktowane zmianami, jakie zachodzą na świecie. Przyjęcie nowej Strategii musi być także spójne z innymi dokumentami strategicznymi oraz polityką państwa wewnętrzną i zagraniczną we wszystkich obszarach funkcjonowania.

[1)] M.P. poz. 1037.
[2)] Dz. U. z 2026 r. poz. 20 i 252.

2. Kontekst strategiczny cyberbezpieczeństwa w Rzeczypospolitej Polskiej

Niniejsza Strategia jest kontynuacją i rozszerzeniem działań, podejmowanych przez administrację rządową, mających na celu podniesienie poziomu cyberbezpieczeństwa w RP.

W zakresie aktów legislacyjnych poprzednie działania obejmowały wejście w życie ustawy o KSC wraz z jej nowelizacjami. Ustawa ta wdrożyła do polskiego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa NIS)[3)].

Zakończyły się prace legislacyjne nad nowelizacją ustawy o KSC, która ma na celu wdrożenie dyrektywy 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, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)[4)]. W rezultacie znacząco zostanie zmodyfikowany krajowy system cyberbezpieczeństwa (KSC), w szczególności przez rozszerzenie katalogu podmiotów objętych tymi regulacjami.

Ponadto ustawa z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa[5)] (ustawa o KSCC) dostosowywała polski porządek prawny do obowiązków wynikających z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)[6)]. Regulacje te stanowią ważne uzupełnienie KSC w zakresie certyfikacji.

W zakresie dokumentów strategicznych poprzednie działania obejmowały przyjęcie przez rząd:

1) w 2013 r. Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, przyjętej uchwałą nr 111/2013 Rady Ministrów z dnia 25 czerwca 2013 r. w sprawie Polityki Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej[7)];
2) w 2017 r. Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, przyjętych uchwałą nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022[8)];
3) w 2019 r. Strategii na lata 2019–2024, przyjętej uchwałą nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024[9)].

Kwestia cyberbezpieczeństwa ujęta jest także w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej zatwierdzonej w 2020 r. przez Prezydenta Rzeczypospolitej Polskiej, jak również będzie uwzględniona w przygotowywanej nowej Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, w związku z czym zostanie zachowana spójność strategiczna między niniejszą Strategią a Strategią Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Przy opracowywaniu Strategii wzięto także pod uwagę trwające prace nad Strategią Rozwoju Polski do 2035 r. – nową średniookresową strategią rozwoju kraju.

---

3) Dz. Urz. UE L 194 z 19.07.2016, str. 1.
4) Dz. Urz. UE L 333 z 27.12.2022, str. 80 oraz Dz. Urz. UE L 2025/90884 z 06.11.2025.
5) Dz. U. poz. 1017.
6) Dz. Urz. UE L 151 z 07.06.2019, str. 15 oraz Dz. Urz. UE L 2025/37 z 15.01.2025.
7) Uchwała niepublikowana w M.P.
8) Uchwała niepublikowana w M.P.
9) M.P. poz. 1037.

Strategia jest spójna z głównymi celami i działaniami określonymi w Strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę[10]. Jej realizacja, przez wzmocnienie krajowego systemu cyberbezpieczeństwa, przełoży się również na podniesienie poziomu cyberodporności UE.

Niniejsza Strategia zastąpi Strategię na lata 2019–2024, obejmując działania od 2025 r., na okres kolejnych 5 lat, to jest do 2029 r.

Zamierzeniem niniejszego dokumentu jest określenie celów strategicznych oraz odpowiednich środków politycznych i regulacyjnych, mających na celu podniesienie poziomu odporności w wymiarze cyberbezpieczeństwa, zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich własnych danych i informacji. Realizacja celów strategicznych ma również wpływać na podniesienie poziomu bezpieczeństwa narodowego, zdolności do rozpoznawania cyberzagrożeń i osiągnięcie zdolności do prowadzenia działań w cyberprzestrzeni defensywnych i ofensywnych, neutralizacji zagrożeń ze strony grup hakerskich powiązanych z obcymi państwami, zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu cyberprzestępstw oraz działań o charakterze hybrydowym (w tym działań o charakterze terrorystycznym) i szpiegowskim w cyberprzestrzeni. Ważnym uzupełnieniem, istotnym dla całego bezpieczeństwa narodowego, są zdolności przewidywania i prognozowania rozwoju sytuacji (foresight) oraz wnioskowania na podstawie danych (data science).

Strategia jest spójna z prowadzonymi działaniami dotyczącymi bezpieczeństwa systemów teleinformatycznych operatorów infrastruktury krytycznej (IK) oraz zmianami systemowymi wynikającymi z przygotowywanego wdrożenia do polskiego porządku prawnego dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylającej dyrektywę Rady 2008/114/WE (dyrektywa CER)[11]. Uwzględnia również potrzeby zapewnienia SZ RP zdolności do prowadzenia działań militarnych w układzie krajowym, sojuszniczym i koalicyjnym w przypadku zagrożenia cyberbezpieczeństwa powodującego konieczność działań obronnych.

Podejmując działania mające na celu wdrożenie Strategii, rząd będzie w pełni gwarantował prawo do prywatności oraz stał na stanowisku, że wolny i otwarty internet jest istotnym elementem funkcjonowania współczesnego społeczeństwa. Jednocześnie istotne jest, aby prawo do prywatności nie utrudniało identyfikacji cyberprzestępców oraz ich ścigania i nie zapewniało im bezkarności.

[10] Wspólny komunikat do Parlamentu Europejskiego i Rady „Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę", Bruksela, 16.12.2020 r., JOIN (2020) 18 final.
[11] Dz. Urz. UE L 333 z 27.12.2022, str. 164.

3. Zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej

Strategia obejmuje w szczególności[12)]:

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, przyjęta w drodze uchwały Rady Ministrów (RM), oddziałuje w sposób bezpośredni na podmioty administracji rządowej, a w sposób pośredni, po przyjęciu z inicjatywy RM przepisów prawa powszechnie obowiązującego, na pozostałe podmioty, w tym m.in. na przedsiębiorców i obywateli.

Cyberbezpieczeństwo jest pośrednio związane z zagadnieniami takimi jak bezpieczeństwo przestrzeni informacyjnej, wojna kognitywna i dezinformacja. Uwzględniając zakres Strategii określony w ustawie o KSC, ustawową definicję cyberbezpieczeństwa oraz całość ustawy o KSC, które nie obejmują bezpośrednio tych zagadnień, Strategia uwzględnia je wyłącznie w odniesieniu do działań dotyczących wzmacniania odporności na zagrożenia hybrydowe, które łączą kampanie dezinformacyjne z cyberatakami, oraz w odniesieniu do budowania świadomości obywateli w zakresie cyberbezpieczeństwa i odporności społecznej na wrogie działania w cyberprzestrzeni.

[12)] Art. 69 ust. 1 i 2 ustawy o KSC.

4. Wizja, cel główny, cele szczegółowe

4.1. Wizja

Zapewnienie bezpieczeństwa oraz pomyślny rozwój RP, wzrost jej zasobności, efektywności gospodarki, sprawności działania instytucji, podmiotów, w tym aktywność społeczna oraz codzienne funkcjonowanie każdego członka społeczeństwa, są związane ze sprawnym i bezpiecznym działaniem systemów informacyjnych i środków komunikacji elektronicznej. Dlatego w ramach działań zaplanowanych w Strategii rząd będzie systematycznie wzmacniał i rozwijał KSC. Działania uwzględniają systemowe rozwiązania organizacyjne, finansowe, operacyjne, technologiczne, prawne, kreowanie postaw społecznych oraz prowadzenie badań naukowych i prac rozwojowych, jak również rozwój polskiej branży cyberbezpieczeństwa, w sposób zapewniający spełnienie wysokich standardów cyberbezpieczeństwa w obszarze oprogramowania, urządzeń i usług cyfrowych. Działania rządu będą podejmowane z poszanowaniem praw i wolności obywateli oraz przez budowę zaufania między administracją rządową a poszczególnymi sektorami rynkowymi. W obszarze międzynarodowym działania rządu będą ukierunkowane na wzajemnie korzystną współpracę oraz promowanie i ochronę otwartej, wolnej, stabilnej i bezpiecznej cyberprzestrzeni opartej na prawach człowieka, podstawowych wolnościach, demokracji i praworządności.

4.2. Cel główny

Podniesienie poziomu odporności krajowych podmiotów przez zwiększenie poziomu ochrony informacji oraz zwiększenie zdolności do wykrywania i reagowania na zagrożenia, promowanie wiedzy i dobrych praktyk oraz podnoszenie kompetencji w zakresie cyberbezpieczeństwa w sektorze publicznym (w tym militarnym), prywatnym, a także wśród obywateli.

4.3. Cele szczegółowe

Cel szczegółowy 1. Rozwój krajowego systemu cyberbezpieczeństwa.

Cel szczegółowy 2. Przeciwdziałanie i zwalczanie cyberprzestępczości oraz uzyskanie zdolności do prowadzenia pełnego spektrum działań w cyberprzestrzeni.

Cel szczegółowy 3. Podniesienie poziomu odporności systemów informacyjnych w sferze publicznej (w tym militarnej) oraz prywatnej.

Cel szczegółowy 4. Zwiększanie potencjału krajowej bazy technologiczno-przemysłowej oraz wzmocnienie suwerenności technologicznej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa.

Cel szczegółowy 5. Budowanie świadomości, wiedzy i kompetencji kadr podmiotów krajowego systemu cyberbezpieczeństwa oraz obywateli i przedsiębiorców.

Cel szczegółowy 6. Wzmocnienie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa.

Tabela 1. Układ celów i kierunków interwencji

Cel główny	Podniesienie poziomu odporności krajowych podmiotów przez zwiększenie poziomu ochrony informacji oraz zwiększenie zdolności do wykrywania i reagowania na zagrożenia, promowanie wiedzy i dobrych praktyk oraz podnoszenie kompetencji w zakresie cyberbezpieczeństwa w sektorze publicznym (w tym militarnym), prywatnym, a także wśród obywateli					
Cele szczegółowe	1. Rozwój krajowego systemu cyberbezpieczeństwa	2. Przeciwdziałanie i zwalczanie cyberprzestępczości oraz uzyskanie zdolności do prowadzenia pełnego spektrum działań w cyberprzestrzeni	3. Podniesienie poziomu odporności systemów informacyjnych w sferze publicznej (w tym militarnej) oraz prywatnej	4. Zwiększanie potencjału krajowej bazy technologiczno-przemysłowej oraz wzmocnienie suwerenności technologicznej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa	5. Budowanie świadomości, wiedzy i kompetencji kadr podmiotów krajowego systemu cyberbezpieczeństwa oraz obywateli i przedsiębiorców	6. Wzmocnienie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa
Kierunki interwencji	1.1 Doskonalenie krajowego systemu cyberbezpieczeństwa	2.1 Wprowadzenie regulacji skuteczniej pozwalających zwalczać cyberprzestępczość	3.1 Podniesienie poziomu odporności systemów informacyjnych	4.1 Wzmocnienie bezpieczeństwa łańcucha dostaw na poziomie krajowym i międzynarodowym	5.1 Zwiększenie świadomości i wiedzy oraz wzmocnienie kompetencji kadr podmiotów krajowego systemu cyberbezpieczeństwa	6.1 Aktywna współpraca międzynarodowa na poziomie strategiczno-politycznym i prawnym
	1.2 Podniesienie efektywności krajowego systemu cyberbezpieczeństwa	2.2 Wzmocnienie wyspecjalizowanych struktur zwalczania cyberprzestępczości	3.2 Rozwój krajowej kryptologii, w tym migracja do kryptografii postkwantowej oraz rozwój technologii kwantowych	4.2 Stymulowanie badań, rozwoju i innowacji w obszarze cyberbezpieczeństwa	5.2 Rozwój świadomości i wiedzy obywateli i przedsiębiorców z zakresu cyberbezpieczeństwa	6.2 Aktywna współpraca międzynarodowa na poziomie operacyjnym i technicznym
	1.3 Rozwój zintegrowanego systemu wymiany informacji na potrzeby zapewnienia ciągłości funkcjonowania administracji państwowej, bezpieczeństwa narodowego i ochrony ludności	2.3 Podnoszenie zdolności analitycznych organów ścigania, służb specjalnych i wymiaru sprawiedliwości przy wykorzystaniu nowych technologii	3.3 Rozwiązania chmurowe dla wzmocnienia odporności systemów informacyjnych			6.3 Koordynacja działań na arenie międzynarodowej w zakresie współpracy cywilno-wojskowej w obszarze cyberbezpieczeństwa
	1.4 Zwiększanie cyberbezpieczeństwa podmiotów nadzorowanych przez organy właściwe do spraw cyberbezpieczeństwa	2.4 Podniesienie skuteczności organów ścigania przez wymianę wiedzy i doświadczeń z zakresu cyberbezpieczeństwa oraz metod wykorzystywanych przez sprawców cyberprzestępstw	3.4 Rozwój zdolności do skutecznego zapobiegania i reagowania na incydenty cyberbezpieczeństwa			
	1.5 Wypracowanie i wdrożenie metodyki szacowania ryzyka na poziomie krajowym	2.5 Zwalczanie cyberterroryzmu i cyberszpiegostwa	3.5 Rozwój standaryzacji w cyberbezpieczeństwie			
		2.6 Uzyskanie zdolności do prowadzenia pełnego spektrum działań w cyberprzestrzeni	3.6 Współpraca publiczno-prywatna w obszarze cyberbezpieczeństwa			

5. Cel szczegółowy 1. Rozwój krajowego systemu cyberbezpieczeństwa

5.1. Doskonalenie krajowego systemu cyberbezpieczeństwa

KSC formalnie został ustanowiony w 2018 r. przez uchwalenie ustawy o KSC. Jednak system ten w praktyce istniał od lat i wciąż ewoluuje. Istotne zmiany w funkcjonowaniu KSC nastąpią wraz z nowelizacją ustawy o KSC, która zaimplementuje do polskiego porządku prawnego dyrektywę NIS 2, przyjętą w 2022 r. Jednak przygotowywane zmiany ustawowe nie dotyczą tylko implementacji prawa UE, ale są też odpowiedzią na zidentyfikowane potrzeby zmian, jak również wynikają z postępu technologicznego, nowych zagrożeń i ewolucji środowiska bezpieczeństwa.

Najważniejsze zmiany wynikające z implementacji dyrektywy NIS 2 są związane z zastąpieniem przez ten akt prawny dotychczasowego podziału na operatorów usług kluczowych (OUK) i dostawców usług cyfrowych (DUC), na podmioty kluczowe i podmioty ważne. Ponadto rozszerzeniu ulegnie katalog sektorów objętych dyrektywą NIS 2. Dyrektywa ta określa również szereg obowiązków podmiotów kluczowych i podmiotów ważnych. Jako podstawowy obowiązek należy wskazać stosowanie odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu. Przez nowelizację ustawy o KSC zostaną wdrożone także postanowienia unijnego zestawu środków dla cyberbezpieczeństwa sieci 5G (Toolbox 5G).

Ponadto uchwalona w dniu 23 stycznia 2026 r. nowelizacja ustawy o KSC dotyczy w szczególności:

1) rozszerzenia katalogu podmiotów KSC o nowe sektory gospodarki;
2) nałożenia obowiązków z zakresu środków zarządzania ryzykiem na podmioty kluczowe i podmioty ważne w cyberbezpieczeństwie, zgodne z dyrektywą NIS 2;
3) wprowadzenia obowiązku zgłaszania incydentów przez podmioty kluczowe i podmioty ważne, za pomocą systemu teleinformatycznego ministra właściwego do spraw informatyzacji, do właściwych zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) sektorowych i CSIRT poziomu krajowego;
4) utworzenia CSIRT sektorowych, które będą wspierać podmioty kluczowe i podmioty ważne w obsłudze incydentów cyberbezpieczeństwa;
5) wzmocnienia kompetencji nadzorczych organów właściwych do spraw cyberbezpieczeństwa (organów właściwych);
6) wprowadzenia nowych administracyjnych kar pieniężnych za niewykonanie obowiązków ustawowych przez podmioty kluczowe i podmioty ważne;
7) wprowadzenia Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę;
8) rozszerzenia kompetencji ministra właściwego do spraw informatyzacji (organ ten będzie mógł dokonać, w drodze decyzji, prawnej identyfikacji dostawcy wysokiego ryzyka, będzie mógł też wydać polecenie zabezpieczające ze wskazaniem zachowania, które ograniczy skutki trwającego incydentu krytycznego);
9) rozszerzenia kompetencji ministra właściwego do spraw informatyzacji i Ministra Obrony Narodowej o zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę;
10) rozszerzenia zakresu zadań CSIRT-ów poziomu krajowego (CSIRT MON, CSIRT NASK i CSIRT GOV), które będą mogły m.in. przeprowadzić ocenę bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty KSC i prowadzić działania w zakresie identyfikowania podatności systemów dostępnych w otwartych sieciach teleinformatycznych;

11) wprowadzenia odpowiedzialności kierownika podmiotu kluczowego lub podmiotu ważnego za realizację zadań z zakresu cyberbezpieczeństwa.

Ocena KSC wskazuje na potrzebę lepszej koordynacji i zinstytucjonalizowanego zarządzania cyberbezpieczeństwem na poziomie krajowym. W związku z tym w nowelizacji ustawy o KSC zostanie wzmocniona rola Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa (Pełnomocnik), który otrzyma więcej uprawnień, aby lepiej zarządzać i koordynować KSC. Funkcja Pełnomocnika zostanie na stałe związana z urzędem obsługującym ministra właściwego do spraw informatyzacji. Pełnomocnik zostanie także przewodniczącym Zespołu do spraw Incydentów Krytycznych, a do urzędu go obsługującego zostanie przeniesiona obsługa tego Zespołu. Rola Pełnomocnika będzie dalej wzmacniana. Będzie on koordynował w porozumieniu z Ministrem Obrony Narodowej działania w zakresie współpracy cywilno-wojskowej w obszarze cyberbezpieczeństwa w czasie pokoju. Pozwoli to zwiększyć efektywność działań i należycie zsynchronizować aktywności w obszarze cyberbezpieczeństwa podejmowane zarówno w sferze wojskowej, jak i cywilnej, a przez to skuteczniej realizować cele strategiczne.

W uchwalonej zmianie ustawy o KSC sformalizowane zostanie funkcjonowanie Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC), które działa od 2022 r. Formuła spotkań koordynacyjnych w formacie PCOC, w których biorą udział przedstawiciele kluczowych dla cyberbezpieczeństwa kraju instytucji, dzięki szybkiej wymianie informacji i sprawnemu reagowaniu na pojawiające się incydenty cyberbezpieczeństwa, stanowi istotną wartość dodaną dla KSC.

W kolejnym kroku nastąpi rozszerzenie charakteru PCOC przez utworzenie pod tą nazwą komórki organizacyjnej w urzędzie obsługującym ministra właściwego do spraw informatyzacji, która będzie organizacyjnie i merytorycznie obsługiwać Pełnomocnika i spotkania PCOC, koordynować z ramienia Pełnomocnika działania instytucji zapewniających cyberbezpieczeństwo na poziomie krajowym oraz realizować część zadań ministra właściwego do spraw informatyzacji przewidzianych w ustawie o KSC.

Docelowo PCOC zostanie przekształcone w centralną instytucję zapewniającą cyberbezpieczeństwo na poziomie krajowym, dysponującą odpowiednią pozycją ustrojową, kompetencjami, zasobami osobowymi, budżetem i infrastrukturą. Nowa instytucja będzie pełnić funkcję koordynującą w KSC, a także będzie stanowić „jedno okienko" dla podmiotów KSC i obywateli w zakresie zgłaszania incydentów, jak również będzie odpowiadać za wsparcie działań Pełnomocnika. Pozwoli to jeszcze bardziej zwiększyć efektywność systemu i zapewni sprawniejsze reagowanie na zagrożenia w cyberprzestrzeni. Wnioski krajowe oraz z innych państw pokazują, że potrzebne jest powołanie do życia nowej instytucji centralnej, odpowiedzialnej za cyberbezpieczeństwo w skali całego państwa, pozwalającej w sposób centralny zarządzać cyberbezpieczeństwem w RP. W związku z rozbudowywaniem i komplikacją przepisów dotyczących cyberbezpieczeństwa na poziomie UE, PCOC będzie wspierać działania mające na celu upraszczanie i harmonizację wdrażania przepisów dotyczących cyberbezpieczeństwa, w tym identyfikowanie obszarów przenikania się regulacji, synchronizację działań i uproszczenie procedur dla podmiotów zobowiązanych do stosowania regulacji związanych z cyberbezpieczeństwem.

Jednocześnie ważnym uzupełnieniem KSC jest ustawa o KSCC, która wprowadziła system certyfikacji cyberbezpieczeństwa w RP oraz procedury niezbędne do zapewnienia prawidłowości procesów certyfikacyjnych.

W obliczu rosnącej liczby aktów prawa UE i prawa krajowego dotyczących cyberbezpieczeństwa będą prowadzone działania, które pozwolą zadbać o ich należytą harmonizację i skoordynowane wdrażanie. Do porządku krajowego zaimplementowane zostaną lub zostanie zapewnione stosowanie także sektorowych regulacji UE, w tym rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającego rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (rozporządzenie 2022/2554)[13)] oraz dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2556 z dnia 14 grudnia 2022 r. w sprawie zmiany dyrektyw

[13)] Dz. Urz. UE L 333 z 27.12.2022, str. 1 oraz Dz. Urz. UE L 2024/90177 z 12.03.2024.

2009/65/WE, 2009/138/WE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 oraz (UE) 2016/2341 w odniesieniu do operacyjnej odporności cyfrowej sektora finansowego[14)].

5.2. Podniesienie efektywności krajowego systemu cyberbezpieczeństwa

Wzrastająca skala zagrożeń oraz związane z tym zwiększanie zakresu działań w ramach KSC stwarzają konieczność ciągłego monitorowania i poprawiania efektywności całego systemu, aby należycie zapewniać bezpieczeństwo polskiej cyberprzestrzeni i koordynować służące temu działania.

Podnoszenie efektywności funkcjonowania KSC jest realizowane m.in. przez uruchomiony z dniem 1 stycznia 2021 r. przez ministra właściwego do spraw informatyzacji system S46 wspierający:

1) współpracę podmiotów wchodzących w skład KSC;
2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;
3) zgłaszanie i obsługę incydentów cyberbezpieczeństwa;
4) szacowanie ryzyka na poziomie krajowym;
5) ostrzeganie o cyberzagrożeniach;
6) czynności nadzorcze organów właściwych;
7) dokonywanie zgłoszenia naruszenia ochrony danych osobowych.

System S46 będzie rozwijany, w tym przez zwiększenie jego efektywności oraz wprowadzenie nowych funkcjonalności, takich jak gromadzenie informacji o podmiotach kluczowych i podmiotach ważnych (po wejściu w życie projektowanej nowelizacji ustawy o KSC), istotne z punktu widzenia zarządzania KSC. Ponadto do systemu S46 będą przyłączone kolejne podmioty KSC, w tym wszystkie podmioty kluczowe i podmioty ważne. System S46 będzie podstawą wymiany informacji między podmiotami kluczowymi, podmiotami ważnymi oraz instytucjami państwowymi. Informacje z tego systemu będą również przekazywane do organów odpowiedzialnych za zarządzanie kryzysowe. Zmodernizowany system S46 będzie też wykorzystywany przez PCOC dla zautomatyzowania wymiany informacji w ramach KSC.

Uruchomiony został także portal cyber.gov.pl – nowoczesna, rządowa platforma stworzona z myślą o bezpieczeństwie cyfrowym obywateli, firm i instytucji publicznych. W jednym miejscu znajdują się wszystkie kluczowe usługi i narzędzia – od zgłaszania incydentów, przez monitorowanie zagrożeń, po dostęp do rozwiązań takich jak system Artemis, S46 czy aplikacji moje.cert.pl. Platforma oferuje również dostęp do bazy wiedzy, szkoleń, ostrzeżeń i praktycznych informacji o obowiązkach wynikających z ustawy o KSC i dyrektywy NIS 2. Dzięki integracji m.in. z węzłem krajowym identyfikacji elektronicznej, o którym mowa w art. 21a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej[15)], logowanie i korzystanie z serwisu będzie łatwe i bezpieczne.

Działaniem zmierzającym do budowania krajowego i europejskiego cyberbezpieczeństwa będzie wytworzenie w oparciu o system S46 oraz usługę wymiany informacji na temat incydentów bezpieczeństwa sieci n6 krajowej platformy wspomagającej wykrywanie i budowanie świadomości sytuacyjnej zagrożeń i incydentów cyberbezpieczeństwa dla sektora publicznego i prywatnego, stanowiącej Krajowy Cyber Hub (National Cyber Hub – NCH). Docelowo platforma ta stanie się elementem europejskiej sieci komunikacji o zagrożeniach cyberbezpieczeństwa (European Cybersecurity Alert System).

Wzmacniana będzie rola organów właściwych przez zwiększenie ich uprawnień związanych z nadzorem danego sektora, ponadto organ właściwy będzie ustanawiać CSIRT sektorowy. Oprócz możliwości przeprowadzania kontroli organy właściwe zyskają m.in. możliwość zobowiązania

[14)] Dz. Urz. UE L 333 z 27.12.2022, str. 153.
[15)] Dz. U. z 2024 r. poz. 1725 oraz z 2026 r. poz. 252.

podmiotu w drodze decyzji do przeprowadzenia audytu bezpieczeństwa czy uprawnienie do nakazania podmiotom podjęcia określonych czynności dotyczących obsługi incydentu. W określonych ustawowo sytuacjach organ właściwy będzie mógł z urzędu wpisać dany podmiot do wykazu podmiotów kluczowych i podmiotów ważnych. Organy właściwe będą ponadto odgrywać istotną rolę w zakresie oceny bezpieczeństwa łańcucha dostaw. Organy właściwe będą także zacieśniać współpracę między sobą, aby należycie synchronizować działania podejmowane w poszczególnych sektorach, zapewniać sobie wzajemną pomoc oraz w stosownych przypadkach prowadzić wspólne działania nadzorcze.

Wzmacniana będzie efektywność zespołów cyberbezpieczeństwa podmiotów KSC, w szczególności tych, których systemy teleinformatyczne lub sieci teleinformatyczne są objęte jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład IK. Specjalistyczne ćwiczenia i warsztaty cyberbezpieczeństwa, w tym w formacie międzynarodowym, z wykorzystaniem nowoczesnych platform typu CyberRange i zaawansowanych scenariuszy adresujących współczesne wyzwania i zagrożenia w domenie cyberbezpieczeństwa, dadzą możliwość zgrywania zespołów cyberbezpieczeństwa oraz weryfikacji ich umiejętności w bezpośrednich działaniach.

W ramach struktur Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK), w ramach którego funkcjonuje jeden z CSIRT-ów poziomu krajowego (CSIRT NASK) – zostanie utworzone Centrum Cyberbezpieczeństwa NASK (CCN), na które złożą się jakościowo nowe tematyczne specjalistyczne centra, ośrodki i laboratoria kluczowe dla wzmocnienia KSC. Realizacja tego działania pozwoli na podniesienie poziomu bezpieczeństwa informacji, przez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych państwa oraz podmiotów mających kluczowe znaczenie dla gospodarki.

Niezbędne zmiany zostaną również wprowadzone w strukturze Agencji Bezpieczeństwa Wewnętrznego (ABW), polegające na powołaniu nowej jednostki organizacyjnej posiadającej kompetencje w zakresie rozpoznawania, przeciwdziałania i zwalczania cyberterroryzmu i cyberszpiegostwa.

Newralgicznym elementem KSC są jednostki samorządu terytorialnego (JST). Stworzone zostaną wojewódzkie zespoły specjalistów cyberbezpieczeństwa działających lokalnie i wspierających podmioty publiczne w obsłudze incydentów i odzyskiwaniu danych oraz prowadzeniu działań podnoszących świadomość o cyberbezpieczeństwie. Kontynuowany będzie program Cyberbezpieczny Samorząd obejmujący szkolenia i zakupy niezbędnego sprzętu i oprogramowania. Rząd będzie wspierać JST w budowie i rozbudowie samorządowych struktur odpowiedzialnych za cyberbezpieczeństwo tych jednostek, co jest szczególnie istotne, biorąc pod uwagę ograniczone zasoby poszczególnych JST. W celu ograniczenia deficytu specjalistów z obszaru cyberbezpieczeństwa w jednostkach samorządu terytorialnego zostanie uruchomione przedsięwzięcie budowy Lokalnych Centrów Cyberbezpieczeństwa, działających jako Centra Usług Wspólnych w obszarze IT, które zapewnią wysoki poziom cyberbezpieczeństwa dla wielu instytucji działających na szczeblu lokalnym i regionalnym. Prowadzone będą również działania zorientowane na wsparcie samorządów na poziomie wojewódzkim w zakresie realizacji przedsięwzięć w obszarze cyberbezpieczeństwa w ramach programów regionalnych.

W kontekście podnoszenia poziomu cyberbezpieczeństwa kluczowe znaczenie ma zapewnienie dostępu do wiedzy eksperckiej dotyczącej cyberzagrożeń. Jednym ze sposobów na zapewnienie takiego dostępu jest tworzenie Centrów Wymiany i Analizy Informacji (ISAC) oraz ośrodków kompetencji. ISAC gromadzi informacje o podatnościach i cyberzagrożeniach, a następnie przekazuje te informacje oraz zestawy dobrych praktyk do podmiotów, które uczestniczą w systemie wymiany takich informacji. Funkcjonowanie ISAC w sektorach objętych zakresem ustawy o KSC, a także jej nowelizacji, które mają kluczowe znaczenie dla polskiej gospodarki, przyczyni się do wzmocnienia współpracy i zaufania między podmiotami z tego samego sektora. Tworzenie ISAC w dalszym ciągu będzie wspierane na zasadach ogólnych – na przykład w formie stowarzyszeń, fundacji, partnerstw publiczno-prywatnych lub innych jednostek organizacyjnych, bez regulowania tej materii w ustawie KSC.

Kontynuowane będą działania dotyczące cyberbezpieczeństwa w ramach systemu zarządzania kryzysowego oraz zarządzania kryzysowego w cyberbezpieczeństwie w ramach KSC. Nowym elementem będzie przygotowanie Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę oraz monitorowanie jego wykonania. Pozwoli to zbliżyć

regulacje KSC oraz zarządzania kryzysowego, zapewniając przepływ niezbędnych informacji i synergię działań. Działania te obejmować będą także zwiększenie cyberbezpieczeństwa IK. Zgodnie z rozporządzeniem delegowanym Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniającym rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej[16)] (Kodeks Sieci) w ramach Krajowego planu zostaną również uwzględnione kwestie zarządzania kryzysami i reagowania na nie w odniesieniu do transgranicznych przepływów energii elektrycznej (art. 41 ust. 2 i 3 Kodeksu Sieci).

Rozwijane będą zdolności analityczne w oparciu o dane na potrzeby określania dalszego kierunku rozwoju KSC oraz przewidywania i prognozowania rozwoju sytuacji w środowisku cyberbezpieczeństwa (cyber-foresight). Rozwiązania z zakresu technologii informacyjno-telekomunikacyjnych (ICT) wspierające działalność analityczną będą współdzielone przez podmioty KSC, jak również wzajemnie udostępniane będą uzyskane z użyciem tych rozwiązań produkty analityczne.

5.3. Rozwój zintegrowanego systemu wymiany informacji na potrzeby zapewnienia ciągłości funkcjonowania administracji państwowej, bezpieczeństwa narodowego i ochrony ludności

Systemy bezpiecznej wymiany informacji na potrzeby kierowania bezpieczeństwem narodowym są konieczne nie tylko dla zapewnienia cyberbezpieczeństwa w kraju, ale także dla kompleksowego systemu bezpieczeństwa narodowego.

Utworzony zostanie System Bezpiecznej Łączności Państwowej (SBŁP) zapewniający wymianę informacji między organami odpowiedzialnymi za realizację zadań z zakresu zarządzania kryzysowego, bezpieczeństwa państwa, ochrony porządku publicznego, ratownictwa, ochrony ludności i obrony cywilnej. Podsystemy tworzące SBŁP obejmą swoim zakresem jawną i niejawną łączność stacjonarną, infrastrukturę wideokonferencyjną, bezpieczną łączność mobilną, w tym niejawną łączność komórkową, łączność trankingową, łączność radiową oraz bezpieczną łączność satelitarną. Nastąpi wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach przepływu informacji. Zapewnione zostaną wydajne, bezpieczne i dostępne usługi systemów telekomunikacyjnych, pozwalające na dostarczanie usług łączności także w przypadkach relokowania stanowisk kierowania i dowodzenia w kontekście ochrony ludności, zwiększenia bezpieczeństwa obywateli i skuteczności reagowania na sytuacje kryzysowe. Rozwijane będą rozwiązania kryptograficzne, w tym mechanizmy szyfrowania i bezpiecznej transmisji danych. Powstanie hybrydowa infrastruktura umożliwiająca przełączanie między sieciami naziemnymi a systemami satelitarnymi w przypadku zakłóceń. Zostanie opracowana możliwość komunikacji między systemem a rozwiązaniami wojskowymi w czasie pokoju, kryzysu i konfliktu.

Bezpośrednimi użytkownikami systemu będą organy administracji publicznej, urzędy obsługujące te organy oraz jednostki organizacyjne podległe tym organom lub przez nie nadzorowane wykonujące zadania z zakresu bezpieczeństwa państwa, ochrony porządku publicznego, ratownictwa, ochrony ludności i obrony cywilnej oraz zarządzania kryzysowego, powiadamiania, ostrzegania i alarmowania ludności.

Kontynuowane będą zbudowane i wdrożone już rozwiązania bezpiecznej łączności mobilnej: system łączności mobilnej umożliwiający przetwarzanie informacji niejawnych do klauzuli „zastrzeżone” w oparciu o system CATEL (SKR-Z), bazujący na wytycznych dotyczących budowy i zasad funkcjonowania systemu CATEL, jak również „Komunikator” mający na celu zapewnienie bezpiecznej (jawnej) komunikacji rządowej i KSC na urządzeniach służbowych. Nacisk będzie położony na utrzymanie tych systemów na wysokim poziomie dostępności, z zapewnieniem ich dostępności cyfrowej oraz sukcesywne zwiększanie liczby użytkowników oraz wzbogacanie funkcjonalności

[16)] Dz. Urz. UE L 2024/1366 z 24.05.2024, Dz. Urz. UE L 2024/90558 z 16.09.2024 oraz Dz. Urz. UE L 2025/1759 z 25.08.2025.

systemu. Rozwijana będzie też platforma elektronicznego zarządzania dokumentami niejawnymi zabezpieczona krajowymi rozwiązaniami kryptograficznymi oraz dokonane zostaną niezbędne zmiany w przepisach prawa umożliwiające funkcjonowanie platformy zgodnie z wymogami dotyczącymi ochrony informacji niejawnych. Zostanie również stworzony komunikator narodowy na potrzeby administracji publicznej. Podejmowane będą działania, aby wykorzystywane, komercyjne rozwiązania komunikacyjne były zastępowane rozwiązaniami udostępnianymi przez instytucje państwowe.

5.4. Zwiększanie cyberbezpieczeństwa podmiotów nadzorowanych przez organy właściwe do spraw cyberbezpieczeństwa

Uchwalona zmiana ustawy o KSC związana z wdrożeniem dyrektywy NIS 2 doprowadzi do zastąpienia OUK i DUC przez podmioty kluczowe i podmioty ważne. Dotychczasowy podział na OUK oraz DUC okazał się nieaktualny, ponieważ nie odzwierciedlał znaczenia danych sektorów oraz usług dla działalności społecznej i gospodarczej państw członkowskich UE. Dlatego zakresem obowiązywania dyrektywy NIS 2, a tym samym projektowanej ustawy implementującej tę dyrektywę, objęto nowe sektory gospodarki mające kluczowe znaczenie dla działalności społecznej i gospodarczej państwa.

Oprócz rozszerzenia zakresu podmiotowego dyrektywa NIS 2 wprowadziła również m.in. znacznie rozbudowany katalog obowiązków, którym podlegają podmioty kluczowe i podmioty ważne. Zobowiązanie podmiotów kluczowych i podmiotów ważnych do wdrożenia środków zarządzania ryzykiem w cyberbezpieczeństwie przyczyni się w znacznym stopniu do zwiększenia poziomu cyberbezpieczeństwa tych podmiotów, a tym samym bezpieczeństwa na poziomie krajowym, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia usług oraz zapewnienie obsługi incydentów.

Wzrost liczby cyberataków wymaga podjęcia konkretnych działań strategicznych wpływających na zwiększenie poziomu cyberbezpieczeństwa podmiotów kluczowych oraz podmiotów ważnych. CSIRT będą zapewniać właściwe wsparcie (w tym prowadzenie działań proaktywnych) w zakresie cyberbezpieczeństwa i bezpieczeństwa podmiotów kluczowych i podmiotów ważnych. Szczególna uwaga będzie zwrócona na podmioty powiązane funkcjonalnie/technologicznie z IK, administracją publiczną oraz instytucjami bezpieczeństwa i obronności państwa, jako potencjalne cele ataku. Szkolenia dla podmiotów KSC obejmą także kwestie zabezpieczenia interesów podmiotów od strony prawnej w sytuacji wystąpienia incydentu poważnego.

Cyberbezpieczeństwo podmiotów kluczowych i podmiotów ważnych zostanie zwiększone również przez zapewnienie skutecznego nadzoru nad tymi podmiotami, który będzie sprawowany przez organy właściwe do spraw cyberbezpieczeństwa prewencyjnie lub następczo – w zależności od rodzaju podmiotu. Wyposażenie organów właściwych do spraw cyberbezpieczeństwa w szersze kompetencje nadzorcze pozwoli na zapewnienie odpowiednio wysokiego poziomu cyberbezpieczeństwa, w szczególności przez wydawanie poleceń co do obsługi incydentu, wdrożenia zaleceń z audytu czy nakazanie zapewnienia zgodności środków zarządzania ryzykiem w cyberbezpieczeństwie. Ważną rolę w zapewnianiu cyberbezpieczeństwa podmiotów kluczowych i podmiotów ważnych będzie pełnić nadzór o charakterze prewencyjnym, który ma na celu zapewnienie, że podmioty kluczowe będą zdolne do uniknięcia cyberzagrożeń i naruszeń przepisów ustawy o KSC, które mogą prowadzić do wystąpienia incydentów. Ponadto podmiotom tym zostanie udostępniony system S46, co umożliwi im m.in. bardziej efektywne zarządzanie cyberbezpieczeństwem oraz współpracę i wymianę informacji z innymi podmiotami KSC. Wdrożone zostaną postanowienia Kodeksu Sieci, których stosowanie umożliwią przepisy przygotowanej nowelizacji ustawy o KSC. Kodeks Sieci zapewnia dodatkowy katalog obowiązków w celu zwiększania cyberbezpieczeństwa dla podmiotów, które mają wpływ na transgraniczne przepływy energii elektrycznej, jak i katalog uprawnień nadzorczych i obowiązków w zakresie współpracy krajowej i międzynarodowej dla wyznaczonego w tym zakresie organu właściwego. Efektem tych działań będzie wzmocnienie współpracy między poszczególnymi podmiotami oraz właściwymi organami w dziedzinie energii elektrycznej i cyberbezpieczeństwa, a także ułatwienie zapobiegania kryzysom elektroenergetycznym, których podstawową przyczyną może być incydent cyberbezpieczeństwa.

W cyklicznie odbywających się ćwiczeniach cyberbezpieczeństwa na większą skalę będą uczestniczyć także podmioty kluczowe i podmioty ważne.

Udzielone zostanie również wsparcie dla 500 podmiotów KSC w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT, w tym wsparcie podmiotów wykorzystujących technologie informacyjne (IT) oraz technologie operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS).

5.5. Wypracowanie i wdrożenie metodyki szacowania ryzyka na poziomie krajowym

Na potrzeby zarządzania cyberbezpieczeństwem na poziomie krajowym została opracowana, a następnie zaimplementowana w systemie S46, metodyka statycznego i dynamicznego szacowania ryzyka dla systemów teleinformatycznych. Praktyka wykorzystania tej metodyki wykazała, że jest ona trudna do wdrożenia w podmiotach KSC i nie daje oczekiwanych rezultatów.

Zostanie opracowane i zaimplementowane w systemie S46 inne podejście dotyczące szacowania ryzyka, w powiązaniu z osiąganiem oczekiwanego poziomu cyberbezpieczeństwa, zarówno na poziomie podmiotów KSC, jak i ryzyka uogólnionego na poziomie krajowym. W tym celu wykorzystywane będą informacje przekazywane przez podmioty kluczowe i podmioty ważne oraz informacje o zagrożeniach, podatnościach i incydentach pozyskiwane z innych źródeł, w szczególności z CSIRT. Nowe rozwiązanie w zakresie szacowania ryzyka będzie mogło być efektywniej wykorzystane, jak również będzie łatwiejsze w implementacji w podmiotach o różnej wielkości.

6. Cel szczegółowy 2. Przeciwdziałanie i zwalczanie cyberprzestępczości oraz uzyskanie zdolności do prowadzenia pełnego spektrum działań w cyberprzestrzeni

6.1. Wprowadzenie regulacji skuteczniej pozwalających zwalczać cyberprzestępczość

Zapewniony zostanie kompleksowy ekosystem regulacji odnoszących się do zwalczania cyberprzestępczości, zabezpieczenia elektronicznego materiału dowodowego oraz przeciwdziałania kradzieży tożsamości. Rozwój nowoczesnych technologii informacyjno-komunikacyjnych, dostępność środków komunikowania się na odległość i związany z tym rozwój elektronicznych usług wpłynął na sposoby działania sprawców przestępstw skierowanych przeciwko różnym dobrom prawnie chronionym.

W celu szybszego wykrywania sprawców przestępstw w internecie zostaną przygotowane projekty zmian przepisów umożliwiających szybszy dostęp organom ścigania do informacji stanowiących tajemnicę bankową. Projektowane zmiany prawne będą dotyczyć też umożliwienia żądania danych objętych tajemnicą bankową jedynie na podstawie postanowienia prokuratora, bez udziału właściwego miejscowo sądu okręgowego. Taka zmiana w znaczący sposób wpłynie na skuteczność prowadzonych postępowań, koncentrację materiału dowodowego, w szczególności we wstępnej fazie prowadzonego śledztwa czy dochodzenia.

Zaproponowane zostaną zmiany przepisów dotyczące obowiązków banków i innych instytucji finansowych w zakresie retencjonowania oraz przekazywania informacji i danych dotyczących prowadzonych rachunków bankowych i innych usług oraz produktów za pośrednictwem internetu. Zaproponowane zostanie rozwiązanie nakładające obowiązek na instytucje finansowe (w tym banki) oraz podmioty świadczące usługi drogą elektroniczną[17)] gromadzenia również informacji o portach przypisanych do ustalonego adresu IP przez jednoznaczne wskazanie portów źródłowych jako danych identyfikujących zakończenie sieci telekomunikacyjnej, co znacząco wpłynie na możliwości wykrywania tożsamości sprawców w toku prowadzonych postępowań przygotowawczych. Podjęte zostaną prace legislacyjne mające na celu umożliwienie prokuratorom prowadzącym postępowania karne (w tym dotyczących oszustw na pozagiełdowym rynku forex) blokowania stron internetowych, za pośrednictwem których przestępcza działalność jest prowadzona.

Zaproponowane zostaną także rozwiązania prawne w zakresie retencjonowania danych oraz przekazywania informacji i danych przez podmioty świadczące usługi w zakresie kryptoaktywów. Docelowo, w dłuższym horyzoncie czasowym, zaproponowane zostaną mechanizmy prawne umożliwiające „zamrażanie" tych aktywów.

Jednocześnie uchwalenie przepisów zapewniających należyte stosowanie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych)[18)] wprowadzi rozwiązania odnoszące się do egzekwowania odpowiedzialności finansowej platform internetowych, za których pośrednictwem są rozpowszechniane naruszające prawo reklamy (w szczególności reklamy przygotowane przez oszustów, zachęcające do inwestowania w produkty, które nie istnieją), w tym możliwość nakładania adekwatnych kar finansowych na platformy, które wielokrotnie dopuściły się publikacji oszukańczych i dezinformujących treści.

Przygotowane zostaną także rozwiązania legislacyjne, organizacyjne i techniczne służące zwiększeniu ochrony użytkowników internetu przed szkodliwymi i niebezpiecznymi treściami, w tym w szczególności ochrona dzieci i młodzieży (zwalczanie treści przedstawiających wykorzystywanie seksualne dzieci (CSAM), patostreamów, grooming[19)] itp.). Uwzględniać to będzie utworzenie

[17)] Działające w oparciu o ustawę z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2024 r. poz. 1513), w szczególności w zakresie wskazanym w art. 18 ust. 5 pkt 2 tej ustawy.

[18)] Dz. Urz. UE L 277 z 27.10.2022, str. 1 oraz Dz. Urz. UE L 163 z 29.06.2023, str. 107.

[19)] Działania podejmowane w celu zaprzyjaźnienia się i nawiązania więzi emocjonalnej z dzieckiem, aby zmniejszyć opory dziecka i później wykorzystać je seksualnie.

i wdrożenie systemu wymiany informacji o wartościach hash (baza HASH) oraz krajowej bazy materiałów przedstawiających wykorzystywanie seksualne dzieci (repozytorium wizerunków CSAM), o których mowa w pkt 2.1.12 i 2.4.2 Krajowego Planu Przeciwdziałania Przestępstwom Przeciwko Wolności Seksualnej i Obyczajności na Szkodę Małoletnich na lata 2023–2026[20)].

Przepisy przeciwdziałające kradzieży tożsamości, w szczególności w zakresie weryfikowania tożsamości klienta bez jego fizycznej obecności przy zastosowaniu środków identyfikacji elektronicznej przy zawieraniu transakcji i korzystaniu z nowych produktów finansowych oraz rejestracji przedpłaconych kart SIM, będą dostosowywane do wyzwań związanych z postępem technologicznym. Zaproponowane zostaną rozwiązania prawne ograniczające masową aktywację kart SIM i wykorzystanie ich w celach niezgodnych z prawem, w tym do sztucznego zwiększania wiarygodności podmiotów czy wspierania działalności zorganizowanych struktur przestępczych i operacji o charakterze hybrydowym.

Dokonany zostanie przegląd przepisów dotyczących odpowiedzialności karnej za część cyberprzestępstw i zaproponowane zostanie ich urealnienie.

Rozwijane będą narzędzia wprowadzone w ustawie z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej[21)], służące przeciwdziałaniu oszustwom wykorzystującym podszywanie się (spoofing[22)]) czy fałszywym wiadomościom tekstowym. Tego rodzaju przestępczość jest szczególnie uciążliwa dla obywateli i prowadzi do obniżenia zaufania zarówno do instytucji publicznych, pod które często podszywają się przestępcy, jak również do legalnie działających przedsiębiorców. Minister właściwy do spraw informatyzacji jest odpowiedzialny za przegląd rozwiązań zawartych w ww. ustawie i w razie potrzeby będzie proponować do niej zmiany służące skutecznemu stosowaniu środków zwalczania nadużyć w komunikacji elektronicznej. W 2026 r. przeprowadzona zostanie ewaluacja wprowadzonych rozwiązań, a kolejne ewaluacje będą przeprowadzane co 2 lata. Pozwoli to na dynamiczne dostosowanie przepisów do zmian w tym obszarze, w szczególności na uwzględnienie nowych metod stosowanych przez cyberprzestępców.

Zaproponowane zostaną rozwiązania pozwalające na monitorowanie i ograniczanie wykorzystania sztucznej inteligencji do działań przestępczych w cyberprzestrzeni, to jest przestępstw terrorystycznych, automatyzacji ataków phishingowych, generowania fałszywych treści, unikania systemów wykrywania zagrożeń.

W zakresie zwalczania cyberprzestępczości zaproponowane zostaną zmiany w ustawach pragmatycznych poszczególnych służb specjalnych, jak również zmiany w ustawie z dnia 6 czerwca 1997 r. – Kodeks karny[23)] (Kodeks karny), które docelowo pozwolą na realizację pełnego spektrum działań, w tym w odniesieniu do zagrożeń cyberterroryzmu i cyberszpiegostwa.

Przygotowana zostanie nowelizacja przepisów ustawowych w kierunku wprowadzenia kontratypów działań operacyjnych i analitycznych podejmowanych w cyberprzestrzeni przez funkcjonariuszy służb specjalnych i służb o charakterze policyjnym w zakresie ustawowego wyłączenia bezprawności czynu, w sytuacjach gdy działanie funkcjonariusza odbywa się w ramach jego ustawowych zadań, służy ochronie interesu publicznego oraz podlega określonym warunkom legalności i nadzoru, jak również przy zastosowaniu zasady proporcjonalności oraz objęciu nadzorem przez sąd lub prokuratora. Umożliwi to skuteczne ściganie najpoważniejszych form cyberprzestępczości, zapewniając jednocześnie odpowiednią ochronę prawną osobom realizującym zadania służbowe z użyciem stosownych narzędzi i metod, jednocześnie chronić to będzie przed nadużyciami.

Policja i prokuratura oraz inne właściwe instytucje będą wykorzystywać scentralizowane narzędzia informatyczne zapewniające, że czynności przeciwko jednej grupie przestępców będą prowadzone

---

[20)] Wprowadzonego uchwałą nr 204 Rady Ministrów z dnia 17 października 2023 r. w sprawie przyjęcia Krajowego Planu Przeciwdziałania Przestępstwom Przeciwko Wolności Seksualnej i Obyczajności na Szkodę Małoletnich na lata 2023–2026 (M.P. poz. 1235).

[21)] Dz. U. z 2024 r. poz. 1803 oraz z 2026 r. poz. 252.

[22)] Cyberatak polegający na podszywaniu się pod zaufaną osobę, urządzenie lub instytucję w celu oszukania ofiary i uzyskania dostępu do poufnych danych lub pieniędzy.

[23)] Dz. U. z 2025 r. poz. 383, 1818 i 1872.

w jednym miejscu. Współpraca ta będzie realizowana z wykorzystaniem najnowszych narzędzi ICT. Proces zgłaszania cyberprzestępstw zostanie przeorganizowany w taki sposób, aby zapewnić, że więcej poszkodowanych będzie kontaktować się z organami ścigania.

6.2. Wzmocnienie wyspecjalizowanych struktur zwalczania cyberprzestępczości

Utworzenie Centralnego Biura Zwalczania Cyberprzestępczości (CBZC) w 2021 r. było ważnym krokiem w wyspecjalizowaniu struktur Policji do walki z cyberprzestępczością. CBZC integruje kompetencje techniczne, operacyjne i analityczne, jednak jego skuteczność zależy od współpracy z prokuraturami wyspecjalizowanymi w cyberprzestępczości oraz zrozumienia technologii przez sądy (np. przy orzekaniu w sprawach dotyczących danych cyfrowych, blockchain czy zabezpieczeń elektronicznych). Dlatego też, oprócz dalszego wzmacniania potencjału CBZC, będzie kontynuowane rozszerzanie wyspecjalizowanych jednostek w innych strukturach państwa, w tym w prokuraturze i sądach, aby zapewnić spójność i skuteczność całego systemu.

Tworzony i rozwijany będzie wyspecjalizowany zasób kadrowy, który będzie zajmować się zwalczaniem cyberprzestępczości, a piony zwalczania cyberprzestępczości będą wyposażane w niezbędne narzędzia służące do zbierania i analizowania dowodów, w tym dowodów elektronicznych, w toku prowadzonych postępowań karnych.

Prowadzone będą działania w zakresie integracji wiedzy technicznej i prawnej wśród kadr organów ścigania i wymiaru sprawiedliwości. Zwalczanie cyberprzestępczości łączy aspekty zarówno prawa karnego, informatyki śledczej, prawa dowodowego (np. dopuszczalność i integralność materiału cyfrowego) oraz międzynarodowej współpracy śledczej. Bez wyspecjalizowanych kadr – od policjanta, przez prokuratora, po sędziego – dochodzi do zbyt długich postępowań, nieefektywnego zabezpieczania dowodów, ryzyka uniewinnień z powodów proceduralnych.

Z uwagi na rozwój nowoczesnych technologii i związane z nim pojawianie się nowych podatności, wektorów ataków, usług elektronicznych wykorzystywanych w przestępczym procederze czy nowych sposobów działania sprawców, będzie prowadzone ustawiczne kształcenie zarówno kadr wymiaru sprawiedliwości, Policji i służb specjalnych, jak i tworzenie wyspecjalizowanych komórek organizacyjnych do spraw cyberprzestępczości w prokuraturze oraz Policji.

Prowadzony będzie dalszy rozwój specjalizacji w zakresie ścigania cyberprzestępczości, która na poziomie jednostek organizacyjnych prokuratury powinna przejawiać się przeszkoleniem wytypowanych prokuratorów w zwalczaniu tego rodzaju przestępczości na poziomie prokuratur rejonowych, utworzeniem działów lub wydziałów do spraw cyberprzestępczości w prokuraturach okręgowych oraz regionalnych, w których będą pracować prokuratorzy specjalizujący się w zwalczaniu tego rodzaju przestępczości.

6.3. Podnoszenie zdolności analitycznych organów ścigania, służb specjalnych i wymiaru sprawiedliwości przy wykorzystaniu nowych technologii

Podnoszenie zdolności analitycznych organów ścigania, służb specjalnych i wymiaru sprawiedliwości jest kluczowym elementem skutecznej strategii walki z cyberprzestępczością. Organy ścigania będą wyposażane w możliwości szybkiego i dokładnego analizowania dużych ilości danych z różnych źródeł, takich jak logi serwerów, zapisy ruchu sieciowego czy dane z urządzeń mobilnych. Zaawansowana analiza danych pozwoli na identyfikację wzorców działań przestępczych, co może prowadzić do wykrycia zarówno pojedynczych sprawców, jak i całych grup przestępczych, dodatkowo wykorzystanie analityki predykcyjnej umożliwi prognozowanie przyszłych ataków oraz wykrywanie potencjalnych luk w systemach bezpieczeństwa. Podnoszenie zdolności analitycznych będzie realizowane przez wdrożenie nowoczesnych systemów analizy danych (w tym opartych na sztucznej inteligencji, które mogą automatyzować procesy analizy i przetwarzania informacji). Wykorzystywane do tego będą

zaawansowane technologie, takie jak komputery kwantowe do dekodowania zaszyfrowanych danych, śledzenia transakcji w kryptowalutach oraz analizy Darknetu.

Organizowane będą regularne szkolenia dla funkcjonariuszy organów ścigania oraz przedstawicieli wymiaru sprawiedliwości w zakresie nowych technologii, cyberbezpieczeństwa i metod analizy danych, w tym z uwzględnieniem aspektów prawnych. Prowadzona będzie współpraca z uczelniami i firmami technologicznymi w celu podnoszenia kwalifikacji osób zaangażowanych w walkę z cyberprzestępczością.

Równolegle w strukturach organów ściągania wprowadzane będą zmiany organizacyjne, legislacyjne i proceduralne, pozwalające na maksymalne wykorzystanie potencjału nowych technologii.

6.4. Podniesienie skuteczności wymiaru sprawiedliwości i organów ścigania przez wymianę wiedzy i doświadczeń z zakresu cyberbezpieczeństwa oraz metod wykorzystywanych przez sprawców cyberprzestępstw

Podejmowane będą działania edukacyjne mające na celu przekazanie przedstawicielom wymiaru sprawiedliwości i organów ścigania szczegółowej wiedzy zarówno teoretycznej, jak i praktycznej, z zakresu zwalczania cyberprzestępczości. Nabyte umiejętności pozwolą na usprawnienie postępowań karnych, w tym przy wykorzystaniu nowych technologii, oraz wpłyną na poprawę jakości współpracy między wyspecjalizowanymi służbami.

Rozwijana będzie współpraca z Interpolem i Europolem w zakresie zwalczania cyberprzestępczości. W związku z postępującą globalizacją będzie prowadzona działalność szkoleniowa obejmująca współpracę z podmiotami zagranicznymi świadczącymi usługi w internecie, jak i stworzonymi w celu zwalczania cyberprzestępczości.

Rozbudowaniu ulegną również szkolenia dotyczące uzyskania danych od podmiotów zagranicznych, co niejednokrotnie stanowi główną przeszkodę w procesie dowodowym. Ofiarami cyberprzestępstw są podmioty gospodarcze, instytucje użytku publicznego oraz osoby indywidualne. Równolegle z prowadzoną działalnością edukacyjną obejmującą organy ścigania i wymiaru sprawiedliwości będą prowadzone kampanie edukacyjne wśród społeczeństwa informujące o metodach wykorzystywanych przez cyberprzestępców.

6.5. Zwalczanie cyberterroryzmu i cyberszpiegostwa

W celu uzyskania zdolności do zwalczania cyberterroryzmu i cyberszpiegostwa będą podejmowane działania – z wiodącą rolą ABW i Służby Kontrwywiadu Wojskowego (SKW) – polegające na wykrywaniu, analizie oraz przeciwdziałaniu zagrożeniom godzącym w cyberbezpieczeństwo RP oraz państw sojuszniczych. Służby specjalne będą stale wspierane w rozpoznawaniu zagrożeń w cyberprzestrzeni, przez CSIRT poziomu krajowego oraz inne właściwe instytucje państwowe.

Zaproponowane zostaną zmiany w przepisach ustaw regulujących funkcjonowanie służb specjalnych w sposób umożliwiający skuteczne prowadzenie działań operacyjnych w cyberprzestrzeni, przez nadanie stosownych i niebudzących wątpliwości uprawnień do prowadzenia przez służby specjalne działań w zakresie rozpoznawania, przeciwdziałania i zwalczania zagrożeń o charakterze terrorystycznym, jak i działalności obcych służb specjalnych w cyberprzestrzeni. W tym celu zostaną także odpowiednio zmienione przepisy Kodeksu karnego.

Rozbudowany zostanie potencjał służb specjalnych umożliwiający realizację zadań w zakresie cyberbezpieczeństwa, w tym zwalczania cyberterroryzmu i cyberszpiegostwa, przez rozbudowę struktur organizacyjnych, jak również zostanie przyznane niezbędne wsparcie finansowe na realizację nowych zadań.

Opracowany zostanie system umożliwiający skuteczne utrwalanie treści generowanych przez osoby zaangażowane w działalność terrorystyczną wykorzystujące komunikatory internetowe oraz inne środki komunikacji interpersonalnej. W tym celu zostaną zaproponowane niezbędne zmiany prawne oraz

zostanie podjęta współpraca z innymi państwami. Stanowić to będzie istotne wsparcie dla organów ścigania i służb odpowiedzialnych za bezpieczeństwo państwa, umożliwiając im skuteczniejsze wykrywanie, monitorowanie i przeciwdziałanie zagrożeniom terrorystycznym w cyberprzestrzeni.

Wypracowane zostaną rozwiązania pozwalające na ograniczenie nieprawidłowości związanych z rejestrowaniem kart SIM z wykorzystywaniem błędnych lub fikcyjnych danych osobowych przez zwiększenie efektywności weryfikacji danych identyfikacyjnych w procesie rejestracji kart SIM, z uwzględnieniem uregulowania rynku odsprzedaży, w tym w serwisach internetowych, oraz wtórnego użytkowania takich kart SIM wraz z możliwością ich blokowania przez operatora. Powyższe przyczyni się także do skuteczniejszego zwalczania innych rodzajów poważnych cyberprzestępstw niż cyberterroryzm i cyberszpiegostwo.

Polskie środowisko naukowe w ramach różnych projektów zostanie zaangażowane w rozwój i wdrażanie nowoczesnych rozwiązań technologicznych na potrzeby zwalczania terroryzmu, jak również w opracowanie rozwiązań informatycznych wspierających wykrywanie narzędzi cyberwywiadowczych wykorzystywanych przez obce służby specjalne m.in. w urządzeniach końcowych, służących pozyskiwaniu informacji od polskich obywateli, w szczególności osób zajmujących stanowiska publiczne.

Jednocześnie rosnące znaczenie technologii dla pozycji strategicznej państwa sprawia, że jednostki naukowo-badawcze i przemysł wysokich technologii są szczególnie narażone na zagrożenia hybrydowe, w tym działania cyberszpiegowskie. Dlatego będą podejmowane działania podnoszące poziom cyberbezpieczeństwa w sektorach naukowym i przemysłowym. W wymiarze cyfrowym państwo będzie podnosić poziom ochrony własności intelektualnej oraz ochronę przed szpiegostwem przemysłowym i technologicznym, szczególnie w zakresie nowych i przełomowych technologii oraz technologii o zastosowaniu w dziedzinie bezpieczeństwa i obronności państwa.

Służby specjalne będą kontynuować działalność ukierunkowaną na pozyskiwanie informacji mających wpływ na bezpieczeństwo zarówno w aspekcie politycznym, obronnym, jak i ekonomicznym. Realizowane będą działania w cyberprzestrzeni, których celem jest uzyskanie informacji o infrastrukturze sieciowej adwersarzy w celu przeciwdziałania i minimalizacji skutków wrogiej aktywności w cyberprzestrzeni wymierzonej w polskie instytucje i podmioty prywatne. Ważnym aspektem będzie także koordynacja działań i wymiana informacji z właściwymi partnerami krajowymi i zagranicznymi.

W powiązaniu z zagrożeniami cyberbezpieczeństwa będą kontynuowane zadania związane z analizowaniem, identyfikowaniem i ograniczaniem rozpowszechniania treści o charakterze propagandowo-dezinformacyjnym wymierzonych w polską przestrzeń informacyjną oraz będą realizowane działania w zakresie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym. Kampanie dezinformacyjne i operacje informacyjne tworzą zagrożenie dla polskiego społeczeństwa, interesów RP oraz jej pozycji na arenie międzynarodowej. W miarę identyfikacji potrzeb w tym zakresie będą wprowadzane odpowiednie zmiany w przepisach prawa. Realizacja zadań w tym obszarze będzie wspierana przez właściwe inne działy administracji rządowej w celu zapewnienia odpowiedniej wiedzy praktycznej i umiejętności oraz sił i środków na realizację nowych zadań. Ponadto będą zwiększane zdolności do wykrywania wykorzystania mechanizmów sztucznej inteligencji do tworzenia przekazów dezinformacyjnych opartych o treści tekstowe oraz audiowizualne.

6.6. Uzyskanie zdolności do prowadzenia pełnego spektrum działań w cyberprzestrzeni

Cyberprzestrzeń jest uznana za kolejną domenę, równorzędną w stosunku do domeny morskiej, lądowej, powietrznej i kosmicznej, w której mogą być prowadzone działania operacyjne. Powyższe znalazło odzwierciedlenie w zobowiązaniach, podjętych przez państwa członkowskie NATO w 2016 r., podczas

szczytu NATO w Warszawie, określanych jako Cyber Defence Pledge[24)]. Ich głównym celem jest wzmocnienie cyberodporności na poziomie krajowym, co jest zbieżne z kierunkiem zmian w obszarze cyberbezpieczeństwa państw UE. Zobowiązania te będą w dalszym ciągu wdrażane, przy uwzględnieniu rekomendacji wynikających z aktualnej oceny stanu cyberbezpieczeństwa na poziomie krajowym.

Cyberprzestrzeń RP jest poddawana licznym działaniom adwersarzy polegającym na rozpoznaniu, próbie przełamania zabezpieczeń aż do kompromitacji sieci i systemów teleinformatycznych podmiotów istotnych dla bezpieczeństwa i obronności państwa. W związku z powyższym SZ RP i służby specjalne będą w dalszym ciągu rozwijać swoje zdolności w zakresie proaktywnej ochrony oraz aktywnej obrony elementów i zasobów cyberprzestrzeni, co jest kluczowe w aspekcie zapewnienia cyberbezpieczeństwa na poziomie krajowym. Takie podejście do obrony wyprzedzającej pozwoli podejmować działania w cyberprzestrzeni, które będą zapobiegać cyberatakom jeszcze przed ich przeprowadzaniem przez zakłócenie wrogich działań.

Jednocześnie precyzyjnie zostaną uregulowane zasady stosowania ofensywnych cybernarzędzi wobec współcześnie wykorzystywanych narzędzi komunikacyjnych, w tym komunikacji interpersonalnej, jak również będzie rozwijany potencjał techniczny w tym zakresie.

Rozwijane i wdrażane będą nowe technologie (w tym sztucznej inteligencji i technologii kwantowych) oraz możliwości wykorzystania technologii podwójnego zastosowania, w celu rozbudowy potencjału SZ RP i służb specjalnych w cyberprzestrzeni. Priorytetowo będą traktowane technologie, rozwiązania i koncepcje, mające na celu identyfikację technik, taktyk i procedur, jakimi operują obecni i przyszli adwersarze, celem przeciwdziałania ich działaniom i ograniczeniu ich oddziaływania, a tym samym niwelowaniu możliwości realizacji przez nich określonych celów w cyberprzestrzeni lub za jej pośrednictwem. Rozbudowywane będą systemy umożliwiające realizację zadań w zakresie monitorowania i wykrywania cyberzagrożeń oraz reagowania na incydenty w systemach wykorzystywanych przez SZ RP i służby specjalne oraz współpracujące z nimi podmioty, zapewniając zarówno ochronę, jak i usuwanie skutków w odpowiednim czasie, tym samym zapewniając odpowiednią stabilność wykorzystywanej przestrzeni cyfrowej i zwiększając odporność na nowe zagrożenia.

W związku ze zmieniającymi się warunkami bezpieczeństwa w cyberprzestrzeni, w tym rosnącym zagrożeniem w domenie informacyjno-psychologicznej, w szczególności natężeniem operacji informacyjnych wymierzonych w obronność państwa, będą prowadzone działania mające na celu podniesienie zdolności SZ RP i służb specjalnych do identyfikacji, przeciwdziałania i reakcji na zagrożenia w tym obszarze.

Kontynuowane będą działania mające na celu rozwój systemu detekcji oraz budowę sieci wymiany informacji o zagrożeniach, co w konsekwencji w znaczącym stopniu zwiększy świadomość sytuacyjną w cyberprzestrzeni.

Rozwijany będzie potencjał osobowy SZ RP i służb specjalnych w obszarze IT, cyberbezpieczeństwa oraz kryptologii, w szczególności przez dostosowywanie istniejących struktur i tworzenie nowych odpowiadających zmieniającym się uwarunkowaniom w cyberprzestrzeni, oraz specjalistyczne

[24)] 1) Podjęcie zdecydowanych działań w kierunku wzmacniania ochrony krajowej infrastruktury teleinformatycznej;
2) Przydzielenie niezbędnych środków finansowych na organizację cyberobrony;
3) Wzmocnienie współpracy pomiędzy głównymi podmiotami krajowymi w celu pogłębiania kooperacji i wymiany najlepszych praktyk;
4) Dołożenie starań w kierunku poprawy zrozumienia istoty zagrożeń w cyberprzestrzeni, włączając w to wymianę doświadczeń i informacji oraz ocenę sytuacji;
5) Podjęcie działań ukierunkowanych na podniesienie świadomości wśród kluczowych dla bezpieczeństwa krajów decydentów, w zakresie podstawowych zasad, które muszą być przestrzegane w cyberprzestrzeni;
6) Położenie większego nacisku na edukację w obszarze cyberbezpieczeństwa;
7) Przyśpieszenie implementacji narodowych zobowiązań w zakresie wzmocnienia tych zdolności do cyberobrony, od realizacji których zależy bezpieczeństwo całego Sojuszu.

szkolenia. Docelowo działania będą zmierzać do zbudowania w ramach resortu obrony narodowej (RON) własnych zdolności do realizacji pełnego spektrum szkoleń w wyżej wymienionych obszarach.

Wdrażane będzie całościowe podejście do procesu zarządzania kompetencjami uwzględniające zdefiniowanie kompetencji dla ról zawodowych oraz szkoleń, zbudowanie ściśle dopasowanych ścieżek szkoleniowych i usystematyzowanie procesu szkolenia. Jako uzupełnienie systemu zarządzania kompetencjami będzie rozwijany projekt potwierdzania kompetencji i certyfikacji. Weryfikacja zdobytej wiedzy i umiejętności oraz zgrywanie zespołów cyberbezpieczeństwa będą prowadzone w ramach specjalistycznych ćwiczeń cyberbezpieczeństwa, zarówno na poziomie krajowym, jak i międzynarodowym. Powyższe przełoży się na efektywny rozwój kompetencji żołnierzy, funkcjonariuszy i pracowników RON oraz służb specjalnych, umożliwiając osiągnięcie zdolności do prowadzenia kompleksowych działań i operacji w domenie cyberprzestrzeni.

7. Cel szczegółowy 3. Podniesienie poziomu odporności systemów informacyjnych w sferze publicznej (w tym militarnej) oraz prywatnej

7.1. Podniesienie poziomu odporności systemów informacyjnych

W zamówieniach publicznych będą uwzględniane wymogi związane z cyberbezpieczeństwem w odniesieniu do produktów ICT, usług ICT i procesów ICT oraz specyfikacji tych wymogów na potrzeby takich zamówień, w tym w odniesieniu do certyfikacji cyberbezpieczeństwa, obowiązku zastosowania mechanizmów kryptograficznych wykorzystujących powszechnie uznawane normy oraz wykorzystywania produktów z zakresu cyberbezpieczeństwa opartych na otwartym oprogramowaniu.

Zaproponowane zostaną rozwiązania umożliwiające szybkie pozyskiwanie usług i produktów związanych z cyberbezpieczeństwem w pilnych przypadkach związanych z bezpieczeństwem państwa, przy jednoczesnym zachowaniu transparentności procesu zakupowego oraz określeniu szczególnego trybu zastosowania tego rodzaju procedury. Przemawia za tym w szczególności długi czas prowadzenia postępowań zakupowych w stosunku do potrzeby szybkiego reagowania na incydenty. Obejmować to będzie także możliwość zakupu pilnych usług i produktów związanych ze zwalczaniem cyberprzestępczości, w sytuacji uzasadnionej potrzeby szybkiego przeciwdziałania przestępstwu, jego wykrycia lub ścigania sprawców takiego przestępstwa, w przypadku gdy posiadane usługi lub narzędzia informatyczne są niewystarczające.

Wprowadzone zostaną rozwiązania dotyczące zarządzania podatnościami, obejmujące promowanie i ułatwianie skoordynowanego ujawniania podatności.

Podjęte zostaną działania na rzecz zwiększenia cyberbezpieczeństwa systemów i rejestrów państwowych oraz cyfrowych usług publicznych, aby zapewnić obywatelom, przedsiębiorcom i administracji publicznej dostęp do bezpiecznych systemów, rejestrów i usług. Podmioty utrzymujące tego rodzaju systemy, rejestry i usługi będą zapewniać monitorowanie bezpieczeństwa w trybie 24/7 przez zespoły cyberbezpieczeństwa, stałe podnoszenie zdolności do reagowania na incydenty oraz wdrażanie nowych rozwiązań technicznych, proceduralnych i systemowych, jak również przeprowadzanie cyklicznych testów ciągłości działania oraz włączenie aspektów cyberbezpieczeństwa na jak najwcześniejszym etapie rozwoju i utrzymania.

Nowe przepisy prawa regulujące różne dziedziny życia społecznego i gospodarczego będą uwzględniać na etapie projektowania standardy cyberbezpieczeństwa oraz ochrony danych osobowych (w tym użycia biometrii i systemów sztucznej inteligencji), wraz z oceną skutków w tym zakresie.

Kontynuowana i rozszerzana będzie ochrona przed atakami typu DDoS (rozproszona odmowa usługi, Distributed Denial of Service), polegającymi na przeciążeniu serwera, sieci lub usługi internetowej przez zalewanie ich ogromną liczbą zapytań, dla podmiotów realizujących zadania publiczne oraz podmiotów istotnych z punktu widzenia bezpieczeństwa narodowego.

Pełnomocnik będzie aktywnie wydawał rekomendacje i komunikaty z zaleceniami dla podmiotów KSC w związku z wykrytymi podatnościami, cyberatakami i kampaniami w cyberprzestrzeni, co pozwoli minimalizować ich skutki.

Prowadzone będą działania na rzecz wsparcia sektora prywatnego, w tym małych i średnich przedsiębiorstw, w podniesieniu odporności cyfrowej, szczególnie w zakresie bezpieczeństwa łańcuchów dostaw. Rozwijane będą narzędzia wzmacniające podstawowy poziom cyberodporności i higieny cyfrowej małych i średnich przedsiębiorstw przez certyfikację cyberbezpieczeństwa procesów ICT u tych przedsiębiorców. Powstaną mechanizmy wsparcia projektów, których celem jest wdrażanie i stosowanie standardów i systemów zarządzania, które bezpośrednio wpływają na utrzymanie ciągłości działania, bezpieczeństwo informacji i standardy zarządzania cyberbezpieczeństwem.

Większy nacisk zostanie położony na rozwój mechanizmów i narzędzi, które będą przede wszystkim koncentrować się na zapobieganiu incydentom, a nie tylko na ich wykrywaniu i zmniejszaniu skutków.

Realizowane będą działania na rzecz utrzymania ogólnej dostępności, integralności i poufności publicznego rdzenia otwartego internetu, w tym, w stosownych przypadkach, cyberbezpieczeństwa podmorskich kabli komunikacyjnych. Rozwijana będzie współpraca w grupach roboczych na forum

NATO i UE oraz we współpracy z instytucjami NATO i UE w celu przeprowadzenia m.in. skonsolidowanej oceny ryzyka, podatności na zagrożenia i zależności, obejmującej zarówno cyberbezpieczeństwo, jak i bezpieczeństwo fizyczne infrastruktury kabli podmorskich i ich łańcuchów dostaw.

Prowadzone działania na rzecz podnoszenia poziomu cyberbezpieczeństwa będą także uwzględniać newralgiczne kwestie systemów automatyki przemysłowej oraz urządzeń internetu rzeczy (IoT).

W celu zapewnienia cyberbezpieczeństwa odporności systemów informacyjnych będą realizowane działania przeciwdziałające zakłócaniu i podszywaniu się w spektrum elektromagnetycznym w odniesieniu do cyberbezpieczeństwa podmiotów publicznych, IK i innych newralgicznych dla bezpieczeństwa państwa podmiotów.

7.2. Rozwój krajowej kryptologii, w tym migracja do kryptografii postkwantowej oraz rozwój technologii kwantowych

W celu zwiększenia odporności systemów informacyjnych będzie rozwijany krajowy potencjał kryptograficzny, uwzględniający wyzwania kryptografii postkwantowej, w tym zdolność do projektowania i wytwarzania rozwiązań opartych na technikach kryptograficznych, zdolność do oceny ryzyka i działania w sytuacjach kryzysowych oraz zaplecze naukowo-badawcze przygotowane do rozwoju i walidacji technologii kryptograficznych niezależnie od organizacji i instytucji zagranicznych.

Konieczne jest wyselekcjonowanie i wdrożenie podstawowych komponentów kryptograficznych w takich obszarach jak identyfikacja elektroniczna (eID) dla osób fizycznych i prawnych, oparte o wieloskładnikowe źródła tożsamości i technologie tożsamości samodzielnie zarządzanej (Self-Sovereign Identity – SSI), narzędzia do pseudonimowego uwierzytelniania i identyfikacji, narzędzia do znakowania czasem nieoparte o zaufanie do wystawcy, narzędzia do szyfrowania w trybie end-to-end, narzędzia do ochrony obrotu danymi przez stworzenie mechanizmów potwierdzania integralności i pochodzenia dokumentów, zarówno cyfrowych jak i tradycyjnych, oraz ich bezpiecznej replikacji i rozproszenia. Mechanizmy te powinny być dostępne i łatwe do użycia przez osoby o niewielkich umiejętnościach cyfrowych.

Budowany system zaufania wymaga zidentyfikowania i stopniowej eliminacji pojedynczych komponentów typu pojedynczy punkt awarii (single-point-of failure). Konieczne jest rozpraszanie i duplikacja danych. Wymaga to m.in. stworzenia bezpiecznych mechanizmów przetwarzania w chmurze, w tym migracji kluczowych danych do zasobów chmurowych będących pod efektywną kontrolą podmiotów krajowych. Konieczne jest stworzenie rozproszonego ekosystemu zaufania, do którego z łatwością mogłyby wejść dane, które są w posiadaniu wielu niezależnych podmiotów.

Budowane będą mechanizmy zwiększające rozliczalność operacji wykonywanych na danych. Dotyczy to w szczególności rozwoju dostępnych mechanizmów typu technologia rozproszonego rejestru (DLT), ale i rozwoju oraz skali stosowania technik takich jak podpis elektroniczny i pieczęć cyfrowa czy doręczenie elektroniczne.

W obliczu postępu technik kryptoanalitycznych, w tym w szczególności kwantowej, rozwoju możliwości wrogiej kryptografii i możliwości zaszywania wrogich komponentów w produktach sprzętowych i oprogramowaniu, będą rozwijane techniki pozwalające na ograniczanie skuteczności ataków przez alternatywne zabezpieczenia pozwalające co najmniej na wykrycie danych będących rezultatem ataku. Ocenie zostaną poddane nowe standardy i algorytmy kryptograficzne przyjmowane przez zagraniczne gremia pod względem trybu ich wdrażania w RP.

W celu rozwoju krajowych kompetencji technologicznych i przemysłowych będą ustanawiane projekty i programy badawczo-rozwojowe w obszarze technologii kryptograficznych, z uwzględnieniem nowych technologii, takich jak kryptografia post-kwantowa, nowe techniki łączności (w tym rozwiązania kwantowej dystrybucji klucza (QKD)), ale również skoncentrowane na technologiach przydatnych w sytuacjach nadzwyczajnych, takich jak klęski żywiołowe, ataki terrorystyczne lub blokada o charakterze ekonomicznym. Cyberbezpieczeństwo RP będzie wzmacniane przez wykorzystanie potencjału, jakim dysponują podmioty krajowe, w tym służby specjalne. Rozwijane będą mechanizmy

współpracy cywilno-wojskowej oraz angażowanie polskiego przemysłu oraz świata nauki w zakresie rozwoju kryptografii i kryptoanalizy. W tym celu RP będzie także prowadzić aktywne działania na arenie międzynarodowej, w tym na forum UE i NATO oraz na płaszczyźnie dwustronnej z kluczowymi partnerami, jednakże przy zachowaniu pełnej kontroli i suwerenności w zakresie kryptografii wykorzystywanej na rzecz bezpieczeństwa narodowego.

7.3. Rozwiązania chmurowe dla wzmocnienia odporności systemów informacyjnych

W celu zwiększenia odporności systemów informacyjnych oraz rozwoju cyfrowego administracji rządowej będą podejmowane działania związane z rozwojem usług przetwarzania w chmurze obliczeniowej. Dotychczas obowiązująca uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”[25)] (Inicjatywa WIIP), regulująca korzystanie przez podmioty administracji rządowej z usług przetwarzania w chmurze obliczeniowej została zmieniona[26)] w taki sposób, aby jak najwięcej podmiotów mogło korzystać z usług przetwarzania w Publicznej Chmurze Obliczeniowej. Jest to niezwykle istotne z punktu widzenia bezpieczeństwa państwa, bezpieczeństwa danych i budowania państwa opartego na podejściu *Cloud First*. W związku z nowelizacją Inicjatywy WIIP zostaną zaktualizowane Standardy Cyberbezpieczeństwa Chmur Obliczeniowych, określone przez ministra właściwego do spraw informatyzacji w porozumieniu z ministrem właściwym do spraw wewnętrznych, Ministrem Obrony Narodowej oraz Ministrem – Członkiem Rady Ministrów, Koordynatorem Służb Specjalnych (MKSS).

Docelowo planuje się, że uchwała RM dotycząca Inicjatywy WIIP zostanie zastąpiona ustawą, która będzie kompleksowo regulowała możliwość korzystania z usług przetwarzania w chmurze przez administrację publiczną. Zapewnienie skutecznych przepisów pozwalających na przetwarzanie danych w chmurze obliczeniowej jest jednym z priorytetów nowoczesnego państwa cyfrowego, które czerpie z doświadczeń międzynarodowych opierających się o sytuację geopolityczną oraz uwzględnia kierunek, jaki obrały w tym zakresie pozostałe państwa członkowskie UE i nie tylko.

Wprowadzenie jednolitych, wysokich standardów ochrony systemów teleinformatycznych i wspieranie podmiotów administracji publicznej w utrzymaniu tych systemów oraz uzyskiwaniu usług niezbędnych do ich budowy, rozwoju i utrzymania przyczyni się do zapewnienia wysokiego poziomu usług świadczonych społeczeństwu przez administrację publiczną. Inicjatywa WIIP zakłada optymalizację istniejących zasobów teleinformatycznych i aplikacji w administracji publicznej przez dostarczanie nowoczesnych i optymalnych kosztowo technologii informatycznych. Wykorzystany model przetwarzania w chmurze może znacznie pomóc urzędom zmagającym się z potrzebą szybkiego dostarczania wysoce niezawodnych, innowacyjnych usług przy wykorzystaniu posiadanych zasobów oraz współpracy z sektorem prywatnym. W Inicjatywie WIIP będą dokonywane niezbędne zmiany zwiększające poziom cyberbezpieczeństwa oraz dostosowujące do nowych rozwiązań technologicznych, w tym szerszej możliwości wykorzystania rozwiązań chmurowych.

Powstanie także osobna chmura do przetwarzania informacji niejawnych (chmura niejawna), chroniona krajowymi rozwiązaniami kryptograficznymi, aby usprawnić dostęp do danych i oprogramowania dla podmiotów realizujących zadania w obszarze bezpieczeństwa i obronności państwa, co zwiększy odporność systemów informacyjnych wykorzystywanych przez te podmioty, jak również usprawni wymianę informacji niejawnych między nimi. W tym celu zostaną wprowadzone odpowiednie zmiany legislacyjne obejmujące odpowiednie zasady i reguły oraz ograniczenia, które pozwolą na zapewnienie odpowiedniego bezpieczeństwa przetwarzanych informacji i wprowadzą obowiązek ich bezwzględnego stosowania przez wszystkie podmioty i organy realizujące zadania związane z ochroną informacji niejawnych. Wszelkie działania związane z utworzeniem chmury niejawnej będą mieć źródło w decyzjach krajowej władzy bezpieczeństwa oraz będą uwzględniać potrzeby wszystkich jednostek objętych tą usługą. Ze względów bezpieczeństwa państwa wszelkie magazyny danych (w tym

[25)] M.P. z 2021 r. poz. 1006 oraz z 2024 r. poz. 908.

[26)] Uchwała nr 127 Rady Ministrów z dnia 23 października 2024 r. zmieniająca uchwałę w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa” (M.P. poz. 908).

infrastruktura) zgromadzone w chmurze niejawnej będą własnością RP. Ponadto chmura niejawna będzie organizowana w sposób uniemożliwiający uzależnienie się od jednego dostawcy.

Na bazie doświadczeń z ostatnich konfliktów zbrojnych systemy informatyczne budowane przez państwo będą opracowywane i modyfikowane z założeniem zapewnienia bezpieczeństwa i zachowania ciągłości dostępu do danych w przypadku wystąpienia istotnego zagrożenia bezpieczeństwa państwa lub wojny. Zostanie opracowany „Plan migracji kluczowych systemów informatycznych RP w przypadku wystąpienia kryzysu lub wojny", uwzględniający zasady bezpiecznego, a przede wszystkim poufnego przetwarzania danych w rozwiązaniach chmurowych.

7.4. Rozwój zdolności do skutecznego zapobiegania i reagowania na incydenty cyberbezpieczeństwa

Rozwijane i usprawniane będą mechanizmy koordynacji KSC i należytego zarządzania całym systemem. W tym zakresie będą realizowane przedsięwzięcia w zakresie Pełnomocnika oraz w ramach PCOC. Realizowane będą działania zwiększające zdolności operacyjne instytucji odpowiedzialnych za zapewnianie cyberbezpieczeństwa na poziomie krajowym oraz będą wspierane inicjatywy podnoszące odporność, w tym potencjał do zapobiegania i reagowania na incydenty cyberbezpieczeństwa, podmiotów KSC. Działania w tym zakresie obejmą m.in. środki do rozpoznawania zagrożeń w cyberprzestrzeni, rozwój ochrony przed atakami typu DDoS, oprogramowanie i rozwiązania sprzętowe zwiększające cyberbezpieczeństwo. Część z tych inicjatyw będzie realizowana centralnie przez Pełnomocnika – urząd obsługujący ministra właściwego do spraw informatyzacji na rzecz podmiotów KSC, co pozwoli w sposób bardziej efektywny i ekonomicznie opłacalny zapewniać niezbędne zasoby. Budowane będą wspólne skonsolidowane systemy cyberbezpieczeństwa na potrzeby całej administracji publicznej.

Zaproponowane będą odpowiednie regulacje prawne w zakresie stosowania aktywnej obrony w cyberprzestrzeni, jak również będą rozwijane zdolności operacyjne w tym zakresie. Zagrożenia ze strony państw-adwersarzy i grup przestępczych, często powiązanych z instytucjami wrogo nastawionych państw rodzi konieczność podejmowania działań określanych jako aktywna obrona. W tym celu zostaną wprowadzone regulacje umożliwiające, aby wybrane publiczne podmioty KSC w ramach obsługi incydentu posiadały uprawnienie blokowania ruchu sieciowego atakujących, np. przez czasowe ograniczenie tego ruchu z adresów IP lub URL, domen i systemów autonomicznych zidentyfikowanych jako przyczyna incydentu. Działania te pozwolą na zmniejszenie szkód spowodowanych cyberatakami przez dostarczanie narzędzi i usług oraz stosowanie odpowiednich taktyk w celu utrudnienia i uniemożliwienia przeprowadzenia cyberataków.

Rozwój zdolności operacyjnych podmiotów KSC będzie zwiększany przez wykorzystanie nowych i przełomowych technologii, w szczególności sztucznej inteligencji, kryptografii post-kwantowej, technologii blockchain, systemów zarządzania dużymi bazami danych, nowych środków łączności oraz rozwiązań chmurowych. Natomiast w wymiarze sprzętowym rozwój zdolności operacyjnych będzie wspierany przez stosowanie zaawansowanej mikroelektroniki, w szczególności przez inwestycje w rozwój kompetencji krajowej bazy technologicznej i przemysłowej, w tym przez działania badawczo-rozwojowe (B+R), aby mogła skutecznie zaspokajać potrzeby najważniejszych instytucji państwowych odpowiedzialnych za cyberbezpieczeństwo oraz sektora prywatnego. Polska będzie w tym celu wykorzystywać możliwości stwarzane przez współpracę międzynarodową (bilateralną oraz na forum UE i NATO).

7.5. Rozwój standaryzacji w cyberbezpieczeństwie

Utworzony zostanie krajowy ośrodek odpowiadający za standaryzację w cyberbezpieczeństwie. Za jego pośrednictwem zostanie wdrożony stały proces monitorowania i analiz stosowalności norm i dokumentów normatywnych (europejskich i międzynarodowych). Stan bieżący wydawanych przez Ministerstwo Cyfryzacji Narodowych Standardów Cyberbezpieczeństwa, będących zbiorem rekomendacji standaryzujących rozwiązania zabezpieczające w sieciach i systemach informacyjnych

wykorzystywanych przez podmioty KSC, oraz rekomendacji ramowych i branżowych, w tym rekomendacji dla podmiotów KSC, poddany zostanie przeglądowi i analizie. Podjęta zostanie inicjatywa zebrania, analizy i systematyzacji zaleceń dotyczących stosowania norm, standardów i przepisów technicznych oraz innych dokumentów o charakterze normatywnym bądź kierunkowym, jak rekomendacje i zalecenia. Na podstawie analizy zostanie podjęta decyzja o dalszym rozwoju krajowych norm standaryzacyjnych. Podjęte będą działania dające podstawy formalno-prawne dla wdrożenia zaleceń w podmiotach KSC. Zabezpieczone zostaną środki finansowe, które pozwolą zapewnić odpowiednie zasoby na rzecz wdrażania wyżej określonych zaleceń.

W celu zapewnienia bezpiecznej i optymalnej kosztowo infrastruktury przetwarzania systemów ICT/OT sektora publicznego, która wykorzystuje nowe formy przetwarzania i przechowywania informacji, m.in. przez wykorzystywanie usług chmury obliczeniowej, będą kontynuowane działania w zakresie przygotowania zaleceń i promowania dobrych praktyk, w tym certyfikacji newralgicznych systemów i urządzeń, podnoszących odporność na cyberzagrożenia. Przedstawiane zalecenia związane z najważniejszymi aspektami cyberbezpieczeństwa w krótkiej i powszechnie zrozumiałej formie pozwolą dostarczyć niezbędną wiedzę na temat standardów higieny cyfrowej i cyberbezpieczeństwa dla szerokiego kręgu użytkowników internetu, w tym zalecenia uwzględniające cyberbezpieczeństwo i ochronę danych w fazie projektowania oraz domyślne cyberbezpieczeństwo oraz ochronę danych.

7.6. Współpraca publiczno-prywatna w obszarze cyberbezpieczeństwa

Kontynuowana będzie współpraca w zakresie cyberbezpieczeństwa z sektorem prywatnym w ramach prowadzonego od 2019 r. Programu Współpracy w Cyberbezpieczeństwie (PWCyber) na rzecz KSC. Charakter współpracy w ramach programu jest publiczny, transparentny i pozafinansowy. Formuła programu partnerskiego jest otwarta dla wszystkich podmiotów, w tym także dla organizacji pozarządowych, które chciałyby pracować nad rozwojem systemu cyberbezpieczeństwa RP. Kluczowym obszarem współpracy w ramach partnerstwa jest podnoszenie kompetencji podmiotów KSC w zakresie świadomości zagrożeń, metod ataków w cyberprzestrzeni oraz prawnych, organizacyjnych i technicznych umiejętności przeciwdziałania zagrożeniom w systemach i sieciach teleinformatycznych, jak również wymiana informacji o cyberzagrożeniach.

8. Cel szczegółowy 4. Zwiększanie potencjału krajowej bazy technologiczno-przemysłowej oraz wzmocnienie suwerenności technologicznej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa

8.1. Wzmocnienie bezpieczeństwa łańcucha dostaw na poziomie krajowym i międzynarodowym

Pandemia COVID-19, wojny handlowe i technologiczne między mocarstwami, reperkusje agresji zbrojnej Federacji Rosyjskiej na Ukrainę pokazały znaczenie odporności gospodarczej na globalne zawirowania oraz posiadania w krytycznych obszarach niezależności technologicznej oraz możliwości zapewnienia bezpiecznych łańcuchów dostaw. Niestabilność światowego systemu politycznego i ekonomicznego jest związana m.in. z agresywną polityką Federacji Rosyjskiej, ryzykiem konfliktu w Azji Południowo-Wschodniej, która ma kluczowe znaczenie dla światowej gospodarki, szczególnie w zakresie półprzewodników i komponentów elektronicznych.

Podjęte zostaną działania zwiększające bezpieczeństwo łańcuchów dostaw w wymiarze krajowym i międzynarodowym, w tym przez wykorzystanie certyfikacji cyberbezpieczeństwa. Obejmie to zarówno wymiar sprzętowy, jak i oprogramowanie. Realizowane będą inicjatywy zarówno organizacyjno-formalne tworzące w RP sprzyjające środowisko dla tego rodzaju działalności biznesowej, jak i znacząco zwiększone zostaną wydatki na badania i rozwój oraz budowę przemysłowego potencjału produkcyjnego.

Wspierane będą wielkoskalowe inwestycje z państw sojuszniczych i partnerskich. Ma to fundamentalne znaczenie w wymiarze gospodarczym i zacieśnienia relacji z sojusznikami, choć ma ograniczone znaczenie, jeżeli chodzi o budowanie rodzimego potencjału technologicznego i suwerenności w tym zakresie. W związku z tym będą realizowane inwestycje w krajowe, suwerenne zdolności technologiczne i przemysłowe w zakresie m.in. półprzewodników i nowoczesnych technologii sprzętowych i programowych, informatycznych i kryptograficznych, ze szczególnym uwzględnieniem potrzeb bezpieczeństwa i obronności państwa. Będzie to także wnosić wkład w zwiększanie suwerenności UE. Tylko panując w pełni nad technologią w wymiarze sprzętowym i programowym, można zapewnić bezpieczeństwo w warstwie infrastrukturalnej i aplikacyjnej systemów teleinformatycznych, co będzie realizowane przez wprowadzenie obowiązku korzystania z certyfikowanych produktów przy tego typu sprzętach.

W celu zwiększenia odporności łańcucha dostaw oraz wzmocnienia krajowego potencjału technologicznego będzie wspierane wdrażanie prototypowych technologii cyberbezpieczeństwa opracowywanych przez krajowych producentów. Działania te obejmą m.in. ułatwienia zakupowe w zamówieniach publicznych, pilotażowe wdrożenia w instytucjach publicznych oraz wsparcie certyfikacyjne. Wdrożenie takich mechanizmów umożliwi praktyczną weryfikację skuteczności rozwiązań, przyspieszy ich komercjalizację oraz zwiększy udział polskich technologii w krajowym ekosystemie cyberbezpieczeństwa.

Z uwagi na rosnące znaczenie otwartego oprogramowania w infrastrukturze cyfrowej państwa będą wspierane inicjatywy zapewniające krajowe wsparcie techniczne, rozwój i utrzymanie kluczowych komponentów otwartoźródłowych wykorzystywanych w systemach administracji publicznej oraz podmiotów KSC. Wzmocnienie krajowego zaplecza oprogramowania otwartoźródłowego przyczyni się do zwiększenia niezależności technologicznej RP oraz odporności łańcucha dostaw na zagrożenia zewnętrzne.

Ważnym elementem zapewnienia bezpieczeństwa i jakości w łańcuchu dostaw jest ocena i certyfikacja produktów (w szczególności oprogramowania, urządzeń i usług) oraz procesów. KSCC umożliwia ustanowienie procedur niezbędnych do zapewnienia prawidłowości procesów certyfikacyjnych oraz określenie sposobu sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy.

W celu zwiększenia odporności KSC oraz wsparcia rozwoju krajowych kompetencji technologicznych będzie promowane wykorzystywanie przez podmioty objęte ustawą o KSCC prototypów krajowych

technologii cyberbezpieczeństwa. Takie podejście umożliwi testowanie i doskonalenie rozwiązań w rzeczywistym środowisku operacyjnym, wspierając jednocześnie rozwój krajowego rynku cyberbezpieczeństwa.

Wzmacniane będzie cyberbezpieczeństwo systemów teleinformatycznych oraz urządzeń i komponentów używanych w poszczególnych sektorach KSC. Organy właściwe i CSIRT-y sektorowe, we współpracy z innymi podmiotami KSC, będą wypracowywać rekomendacje mające na celu wzmocnienie cyberbezpieczeństwa, w tym np. co do wymogów cyberbezpieczeństwa, jakie powinny spełniać urządzenia i oprogramowanie stosowane w nowoczesnych systemach stosowanych w poszczególnych sektorach. W szczególności dotyczyłoby to nowych urządzeń ICT i OT (w tym nowe technologie typu smart, jak np. nowych typów źródeł energii oraz technologie wykorzystujące algorytmy sztucznej inteligencji), które mają stać się częścią instalacji technologicznych stosowanych w sektorze.

Dzięki uchwaleniu ustawy o KSCC system ten będzie wspierał procesy wydawania certyfikatów cyberbezpieczeństwa w europejskich programach certyfikacji cyberbezpieczeństwa, które będą uznawane na terenie całej UE. Jednostki oceniające zgodność oraz certyfikowane produkty ICT, usługi ICT i procesy ICT będą objęte nadzorem krajowego organu do spraw certyfikacji cyberbezpieczeństwa, którym będzie minister właściwy do spraw informatyzacji. W ramach tego nadzoru będzie możliwe prowadzenie niezależnych badań produktów pod kątem tego, czy stale spełniają one wymagania zawarte w programie certyfikacji. Dzięki takim certyfikatom podmioty kluczowe i podmioty ważne będą mogły zadbać o wybór właściwych produktów i usług zapewniających właściwy dla danego zastosowania poziom cyberbezpieczeństwa. Równocześnie ustawa o KSCC tworzy podstawy do tworzenia krajowych schematów certyfikacji cyberbezpieczeństwa, dzięki którym będzie możliwa promocja cyberbezpiecznych rozwiązań w obszarach nieobjętych przez europejskie programy certyfikacji. Co więcej, będą one również wspierać stosowanie bezpiecznych rozwiązań w obszarach uznanych za istotne przez ministra właściwego do spraw informatyzacji oraz inne organy właściwe.

Dla zapewnienia skuteczności systemu certyfikacji cyberbezpieczeństwa będą rozwijane zdolności do certyfikacji oraz prowadzenia ocen bezpieczeństwa, odpowiednio, w jednostkach certyfikujących i laboratoriach badawczych znajdujących się w państwowych instytutach badawczych. Pierwszym krokiem w tym obszarze będzie dostosowanie obecnych programów certyfikacyjnych do europejskiego programu certyfikacji opartego na wspólnych kryteriach (EUCC). W dalszej kolejności będzie rozwijana zdolność do certyfikacji w ramach kolejnych europejskich i krajowych programów certyfikacji cyberbezpieczeństwa, w tym EUCS (Europejski system certyfikacji cyberbezpieczeństwa dla usług chmurowych) oraz EU5G (Europejski system certyfikacji cyberbezpieczeństwa dla 5G).

Certyfikacja jest istotnym elementem zapewnienia bezpiecznego łańcucha dostaw, w tym ograniczania ryzyka instalowania „tylnych wejść" (*backdoorów*), w szczególności w odniesieniu do sprzętu wykorzystanego na potrzeby bezpieczeństwa i obronności państwa, IK oraz podmiotów kluczowych i podmiotów ważnych. Jednocześnie konieczny jest także instrument umożliwiający wykluczanie produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawcy wysokiego ryzyka, według ściśle określonych kryteriów i w sytuacji gdy zajdą do tego uzasadnione powody. Odpowiedni mechanizm prawny pozwalający na uznanie określonego dostawcy sprzętu lub oprogramowania dla szczególnego rodzaju podmiotów gospodarczych i społecznych za dostawcę wysokiego ryzyka zostanie wprowadzony do krajowego porządku prawnego przez nowelizację ustawy o KSC. Rozwiązanie to pozwala na zapewnienie bezpieczeństwa narodowego w zakresie ochrony ważnego interesu państwowego.

Zaradzenie ryzyku wynikającemu z łańcucha dostaw danego podmiotu i jego powiązań z dostawcami jest szczególnie istotne z uwagi na częstość incydentów, w których podmioty są ofiarami cyberataków i w których agresorzy są w stanie złamać zabezpieczenia sieci i systemów informatycznych danego podmiotu, wykorzystując podatności występujące w produktach i usługach podmiotów trzecich (w tym małych i średnich przedsiębiorstwach). Wszystkie podmioty kluczowe i podmioty ważne będą musiały w ramach swoich systemów zarządzania bezpieczeństwem informacji uwzględnić kwestię bezpieczeństwa łańcucha dostaw. W związku z tym wypracowane zostaną narzędzia, które będą

wspierać podmioty kluczowe i podmioty ważne, zarówno publiczne, jak i prywatne, w realizacji tych obowiązków.

W celu ograniczenia ryzyka związanego z wykorzystaniem komponentów ICT pochodzących od dostawców wysokiego ryzyka będą rozwijane mechanizmy oceny bezpieczeństwa produktów i usług w całym łańcuchu dostaw. W szczególności będzie wspierane stosowanie krajowych i europejskich schematów certyfikacji cyberbezpieczeństwa, a także rozwój narzędzi do analizy pochodzenia, integralności i podatności komponentów sprzętowych i programowych. Działania te umożliwią podejmowanie świadomych decyzji zakupowych przez podmioty publiczne i prywatne oraz zwiększą przejrzystość i bezpieczeństwo infrastruktury cyfrowej RP.

Szerzej będzie wykorzystywany także mechanizm rekomendacji Pełnomocnika, w tym w zakresie konieczności aktualizacji bądź wykluczenia oprogramowania ze zidentyfikowanymi podatnościami. Podjęte zostaną działania mające na celu należyte i najbardziej efektywne stosowanie w polskim porządku prawnym rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności)[27]. Pozwoli to na ustanowienie standardów w zakresie zasad cyberbezpieczeństwa urządzeń łączących się z internetem, zwłaszcza w obszarze internetu rzeczy (IoT). Producenci sprzętu i oprogramowania zostaną zobowiązani do spełnienia szeregu kluczowych wymogów, m.in.:

1) zapewnienia, że ewentualne podatności na zagrożenia będą skutecznie usuwane przez okres przewidywanego użytkowania produktu lub przez 5 lat od wprowadzenia go na rynek;
2) niezwłocznego zgłaszania (w ciągu 24 godzin) zidentyfikowanych usterek produktów lub usług do Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA);
3) uwzględniania zasad cyberbezpieczeństwa na etapie projektowania towarów i usług.

Uregulowana zostanie kwestia związana z wykorzystaniem w zamówieniach publicznych certyfikatów cyberbezpieczeństwa. Na rynku obecne są bardzo liczne certyfikaty, których wartość potrafi diametralnie się różnić. Z tego względu ustawa o KSCC umożliwia wyróżnienie w tym procesie określonych certyfikatów, np. wydanych w ramach europejskiego programu certyfikacji cyberbezpieczeństwa EUCC czy certyfikatów wydanych w ramach innych europejskich programów certyfikacji cyberbezpieczeństwa, w szczególności przez wprowadzenie obowiązku posiadania tego typu certyfikatów w przypadku realizacji określonej kategorii zakupów dla podmiotów KSC.

Istotnym elementem wzmocnienia suwerenności technologicznej będzie wdrożenie systemu oceny zgodności urządzeń radiowych z zasadniczymi wymaganiami dotyczącymi cyberbezpieczeństwa określonymi w dyrektywie Parlamentu Europejskiego i Rady 2014/53/UE z dnia 16 kwietnia 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylającej dyrektywę 1999/5/WE[28] (Dyrektywa RED), tak aby zapewnić krajowym producentom możliwości konkurowania na rynku UE.

8.2. Stymulowanie badań, rozwoju i innowacji w obszarze cyberbezpieczeństwa

Wspierany i stymulowany będzie rozwój polskiego potencjału przemysłowego, technologicznego i naukowego w zakresie cyberbezpieczeństwa, w tym z udziałem spółek Skarbu Państwa. Realizowane będą programy oraz projekty badawczo-rozwojowe i innowacyjne w dziedzinie cyberbezpieczeństwa, które pozwolą na budowę krajowych kompetencji technologicznych i przemysłowych oraz zwiększenie technologicznej i cyfrowej suwerenności kraju, a także będą wnosić wkład w zwiększanie suwerenności

[27] Dz. Urz. UE L 2024/2847 z 20.11.2024, Dz. Urz. UE L 2025/327 z 05.03.2025, Dz. Urz. UE L 2025/90555 z 02.07.2025 oraz Dz. Urz. UE L 2025/90828 z 17.10.2025.

[28] Dz. Urz. UE L 153 z 22.05.2014, str. 62, Dz. Urz. UE L 212 z 22.08.2018, str. 1, Dz. Urz. UE L 315 z 07.12.2022, str. 30, Dz. Urz. UE L 223 z 11.09.2023, str. 1, Dz. Urz. UE L 2024/2839 z 07.11.2024 oraz Dz. Urz. UE L 2024/2749 z 08.11.2024.

UE. Jako główny wehikuł realizacji B+R posłuży Narodowe Centrum Badań i Rozwoju (NCBR), jednak działania w tym zakresie mogą być także realizowane w innych formatach, w tym w ramach poszczególnych ministerstw. Zwiększone zostaną także środki finansowe na realizację projektów B+R w dziedzinie cyberbezpieczeństwa, w tym na realizację projektów niejawnych.

W celu zapewnienia cybersuwerenności i stymulowania rozwoju sektora cyberbezpieczeństwa będą prowadzone prace nad stworzeniem polskich rozwiązań cyberbezpieczeństwa, zarówno sprzętowych, jak i programowych. Zintensyfikowane będą prace nad stworzeniem krajowego potencjału przemysłowego cyberbezpieczeństwa, pozwalającego m.in. na tworzenie mikroprocesorów i innego rodzaju układów scalonych, modułów pamięci, mikrokontrolerów, układów kryptograficznych programowalnych urządzeń sieciowych oraz algorytmów uczenia maszynowego, które zapewnią, że w przypadku technologicznego odcięcia będzie możliwe utrzymanie i rozwój technologii kluczowych z punktu cyberbezpieczeństwa i suwerenności państwa.

Na potrzeby cyberbezpieczeństwa będą przeprowadzane inwestycje w dalszy rozwój przełomowych technologii, w tym sztucznej inteligencji, technologii kwantowych, technologii blockchain, chmury obliczeniowej, dużych systemów bazodanowych, sieci i środków łączności nowych generacji (w tym 5G i 6G), IoT.

Organizacja współpracy instytucji odpowiedzialnych za bezpieczeństwo państwa z jednostkami naukowymi i badawczo-rozwojowymi, organizacjami komercjalizującymi wyniki badań naukowych i prac rozwojowych oraz ośrodków analitycznych będzie ukierunkowana na bezpośrednie wykorzystywanie technologii przełomowych na rzecz cyberbezpieczeństwa, w tym przez podmioty KSC.

W ramach krajowego systemu innowacji będą rozwijane rozwiązania na potrzeby cyberbezpieczeństwa. Wspierane będą też w różnych formach polskie startupy z branży cyberbezpieczeństwa. Wykorzystane zostaną parki technologiczne, akceleratory technologiczne, cyfrowe ośrodki innowacji oraz mechanizmy wsparcia finansowego, w tym fundusze venture capital, co umożliwi wsparcie rozwoju rodzimych start-upów działających w obszarze cyberbezpieczeństwa oraz zapewnienie ochrony przed ich przejęciem przez obcy kapitał, szczególnie z państw uznawanych jako nieprzyjazne. Działania wspierające stymulowanie rozwoju i innowacji w obszarze cyberbezpieczeństwa będą obejmować takie inicjatywy jak hackathony, wyzwania technologiczne, konkursy czy inicjatywy związane z wykrywaniem i ujawnianiem podatności (*bug bounty*). Wsparcie obejmie badania i wdrożenia w zakresie cyberbezpieczeństwa technologii przełomowych, nowych algorytmów, które mogą zbudować obecność polskich przedsiębiorców na rynkach światowych dla nowych produktów cyberbezpieczeństwa. Stymulowanie innowacji będzie skuteczne wyłącznie, gdy zaakceptuje się fakt, że część projektów nie osiągnie zakładanych celów. Działania wspierające będą uwzględniać istotne ryzyko związane z tworzeniem nowatorskich technologii.

Prowadzona będzie promocja sektora cyberbezpieczeństwa, aby stwarzać nowe możliwości rozwoju dla polskich firm z tego sektora.

Instytucje publiczne i spółki Skarbu Państwa, w ramach dopuszczonych prawem form, w tym przy poszanowaniu reguł rynku wewnętrznego UE, będą ukierunkowywać swoje działania, aby korzystać przede wszystkim z rozwiązań cyberbezpieczeństwa rodzimych polskich firm, w przypadku gdy są one konkurencyjne i spełniają wymagania zamawiającego. Pozwoli to zbudować w RP silne marki i sektor cyberbezpieczeństwa oraz będzie wspierać ekspansję zagraniczną polskich przedsiębiorstw z branży cyberbezpieczeństwa, a także przełoży się na wzmocnienie suwerenności państwa w zakresie technologii oraz strategicznej autonomii decyzyjnej. Przyczyni się to także do uniezależnienia od wielkich zagranicznych korporacji technologicznych. Jednocześnie będą podejmowane działania, aby przyciągać do RP zagraniczne inwestycje związane z cyberbezpieczeństwem.

Na potrzeby rozwoju krajowego potencjału w obszarze cyberbezpieczeństwa będzie wspierany udział polskich podmiotów przemysłowych i naukowo-badawczych w międzynarodowych programach badawczo-rozwojowych i innowacyjnych w zakresie cyberbezpieczeństwa, w szczególności w ramach UE i NATO (w dziedzinie cyfryzacji oraz bezpieczeństwa i obronności), jak również będą podejmowane działania na rzecz wykorzystania wyników tych inicjatyw na rzecz krajowego cyberbezpieczeństwa.

Działalność Europejskiego Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (ECCC) wraz z siecią krajowych ośrodków koordynacji (w tym polskim Krajowym Centrum Kompetencji Cyberbezpieczeństwa (NCC-PL)) będą prowadzić działania w celu zwiększenia unijnej suwerenności technologicznej przez wspólne inwestycje w strategiczne projekty w zakresie cyberbezpieczeństwa, co wpłynie pozytywnie na utrzymanie doskonałości badawczej i wzmocnienie konkurencyjności przemysłu UE w tej dziedzinie.

W ramach działalności NCC-PL tworzona jest Społeczność kompetentna, rozumiana jako duża, otwarta, interdyscyplinarna i zróżnicowana grupa europejskich interesariuszy, zaangażowanych w rozwój cyberbezpieczeństwa, o której mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2021/887 z dnia 20 maja 2021 r. ustanawiającym Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa oraz sieć krajowych ośrodków koordynacji[29)]. W skład Społeczności kompetentnej wchodzą interesariusze prowadzący badania naukowe, reprezentujący: sektory przemysłu, biznesu, akademicki i sektor publiczny, którzy mają przyczyniać się do utrzymywania i rozwoju zdolności technologicznych i przemysłowych w dziedzinie cyberbezpieczeństwa, niezbędnych do zabezpieczenia jednolitego rynku cyfrowego UE. Wzmocnione zostaną w ten sposób zdolności RP i UE. Będzie to również odpowiedź na wyzwania stojące przed Europą w obszarze cyberbezpieczeństwa dzięki transgranicznej i międzysektorowej współpracy podmiotów posiadających wiedzę specjalistyczną w obszarze cyberbezpieczeństwa.

9. Cel szczegółowy 5. Budowanie świadomości, wiedzy i kompetencji kadr podmiotów krajowego systemu cyberbezpieczeństwa oraz obywateli i przedsiębiorców

9.1. Zwiększenie świadomości i wiedzy oraz wzmocnienie kompetencji kadr podmiotów krajowego systemu cyberbezpieczeństwa

Niezbędne jest podejmowanie i kontynuowanie działań mających na celu zwiększenie świadomości i wiedzy oraz wzmocnienie kompetencji kadr podmiotów KSC. Prowadzone będą inicjatywy szkoleniowe dla podmiotów krajowego systemu cyberbezpieczeństwa, w tym w ramach PWCyber. Szkolenia zapewnią wzrost kompetencji cyfrowych z obszaru cyberbezpieczeństwa kadr podmiotów KSC i zwiększą świadomość oraz kulturę cyberbezpieczeństwa jako integralnego elementu funkcjonowania w cyfrowej rzeczywistości. Inicjatywy szkoleniowe podniosą poziom wiedzy i umiejętności uczestników zarówno w wymiarze ogólnym, jak i specjalistycznym, co jest kluczowe dla skutecznego przeciwdziałania zagrożeniom w cyberprzestrzeni. Działania szkoleniowe będą obejmować też implikacje prawnomiędzynarodowe w odniesieniu do działań w cyberprzestrzeni.

Administracja publiczna jako jeden z filarów KSC wymaga stałego podnoszenia świadomości cyberzagrożeń. Dlatego będą organizowane szkolenia z higieny cyfrowej dla kadr administracji publicznej mające na celu zwiększenie ich wiedzy na temat zagrożeń oraz sposobów ich unikania, co jest niezbędne w kontekście zabezpieczania informacji publicznych. Realizowane będą także działania prewencyjno-edukacyjne skierowane do najważniejszych osób w państwie, w tym parlamentarzystów oraz osób sprawujących wysokie funkcje publiczne, aby zapewnić odpowiedni poziom ochrony na najwyższych szczeblach władzy.

Równie ważne jest podnoszenie wiedzy i świadomości wśród kadr administracji samorządowej, ponieważ to na poziomie lokalnym często dochodzi do pierwszego kontaktu z cyberzagrożeniami. Z tego powodu będą organizowane projekty i przedsięwzięcia edukacyjne, które mają na celu zwiększenie ich kompetencji w zakresie cyberbezpieczeństwa. Zarówno w przypadku przedstawicieli władzy wykonawczej, ustawodawczej, jak i JST, zakłada się kontynuację działań prewencyjno-edukacyjnych z zakresu cyberbezpieczeństwa prowadzonych jako projekt SecureV dotyczący szkoleń cyberbezpieczeństwa dla najważniejszych osób w państwie oraz budowania kompetencji w zakresie tworzenia kultury cyberbezpieczeństwa w JST. Projekt ten będzie rozwijany

[29)] Dz. Urz. UE L 202 z 08.06.2021, str. 1.

m.in. o kolejne grupy odbiorców, aby zwiększyć odporność Rzeczypospolitej Polskiej na zagrożenia w przestrzeni cyfrowej.

Podejmowane przedsięwzięcia na rzecz podnoszenia świadomości cyberzagrożeń będą dotyczyć nie tylko działań edukacyjnych i szkoleniowych, ale obejmować będą również symulowane testy socjotechniczne, które będą mogły być wspierane przed podmioty KSC na rzecz zainteresowanych jednostek sektora publicznego i przedsiębiorstw.

Równolegle do szkoleń przeznaczonych dla szerokiego grona odbiorców, w tym przede wszystkim podmiotów KSC, zostanie rozwinięty system certyfikacji kompetencji oraz przygotowujących do tej certyfikacji szkoleń przeznaczonych także dla kadry zarządzającej podmiotów kluczowych i podmiotów ważnych. Jednocześnie zostanie przygotowany program certyfikacji dla pracowników administracji publicznej i JST.

Jednym z elementów wpisujących się w powyższe cele będzie również zbudowanie systemu certyfikacji kompetencji z zakresu cyberbezpieczeństwa, służącego weryfikacji wiedzy i umiejętności osób realizujących zadania z zakresu cyberbezpieczeństwa, przede wszystkim w podmiotach publicznych.

W celu ograniczenia odpływu specjalistów do spraw cyberbezpieczeństwa z sektora publicznego zostaną utrzymane rozwiązania, które zapewniają konkurencyjne wynagrodzenia w stosunku do sektora prywatnego oraz szkolenia specjalistyczne. W ramach realizacji tego celu do polskiego porządku prawnego wprowadzono ustawę z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa[30)], której głównym celem jest wsparcie działań zmierzających do zapewnienia ochrony systemów teleinformatycznych przed cyberzagrożeniami przez finansowanie świadczeń teleinformatycznych, które są dodatkami do wynagrodzenia za pracę, a w przypadku funkcjonariuszy i żołnierzy zawodowych świadczeniem pieniężnym. Jednakże, aby ograniczyć uznaniowy charakter świadczenia teleinformatycznego finansowanego ze środków Funduszu Cyberbezpieczeństwa, zostaną podjęte prace nad zmodyfikowaniem formuły tego Funduszu.

Prowadzona będzie ścisła współpraca w tym obszarze z ECCC, ENISA i innymi instytucjami, organami i agencjami UE (EUIBA) w związku z prowadzonymi działaniami tych podmiotów mającymi na celu wzmocnienie i rozwój kompetencji wśród osób realizujących zadania w obszarze cyberbezpieczeństwa.

9.2. Rozwój świadomości i wiedzy obywateli i przedsiębiorców z zakresu cyberbezpieczeństwa

W obliczu dynamicznie zmieniającej się sytuacji w cyberprzestrzeni oraz rosnącej liczby zagrożeń niezwykle ważne jest podnoszenie kompetencji w zakresie cyberbezpieczeństwa wśród wszystkich użytkowników internetu. Realizowane będą działania w zakresie kształcenia i szkolenia w dziedzinie cyberbezpieczeństwa, podnoszenia umiejętności oraz świadomości z zakresu cyberbezpieczeństwa, włączając w to dobre praktyki oraz higienę cyfrową, jak również kwestie prywatności i ochrony danych osobowych w internecie. Kampanie społeczne mające na celu zwiększenie świadomości cyberzagrożeń oraz promowanie bezpiecznych praktyk cyfrowych są niezbędne, aby dotrzeć do jak najszerszego grona odbiorców. Działania edukacyjne będą dopasowane do różnych grup użytkowników internetu, uwzględniając ich specyfikę.

Edukacja w tym zakresie musi rozpoczynać się już na etapie przedszkolnym, dlatego programy kształcenia w szkołach będą obejmować edukację w zakresie cyberbezpieczeństwa, w tym także w zakresie prywatności i ochrony danych osobowych w internecie, w odpowiednio dostosowanej formie. Programy nauczania informatyki w szkołach podstawowych i ponadpodstawowych zostaną zmodyfikowane tak, aby uwzględniały podstawowe zasady zapobiegania oraz reagowania na różnego rodzaju cyberzagrożenia.

Zapewnione zostanie również kształcenie w zakresie cyberbezpieczeństwa przez wprowadzenie nowego zawodu w systemie kształcenia zawodowego, tj. technika cyberbezpieczeństwa. Technik cyberbezpieczeństwa będzie odpowiedzialny za ochronę systemów informatycznych, sieci

[30)] Dz. U. z 2024 r. poz. 1662, z 2025 r. poz. 1017 oraz z 2026 r. poz. 252.

komputerowych oraz usług i aplikacji, przed zagrożeniami cyfrowymi. Jego zadaniem będzie zapewnienie poufności, integralności i dostępności danych oraz ciągłości działania systemów informatycznych w organizacjach publicznych i prywatnych.

Realizowane będą również dodatkowe projekty edukacyjne skierowane do dzieci i młodzieży, a także nauczycieli, pedagogów, psychologów, rodziców i opiekunów, ze szczególnym uwzględnieniem aktualnych trendów, które zagrażają dzieciom i młodzieży, pełniące bardzo istotną rolę w przygotowaniu dziecka do bezpiecznego uczestnictwa w świecie cyfrowym. Informacje dotyczące cyberbezpieczeństwa będą również przekazywane osobom młodym objętym oceną kompetencji cyfrowych realizowaną przez urzędy pracy.

Wzmocnieniu ulegnie kształcenie akademickie w zakresie cyberbezpieczeństwa, co zapewni przyszłym specjalistom solidne podstawy teoretyczne i praktyczne. Instytucje akademickie i naukowe otrzymają wsparcie w opracowywaniu, usprawnianiu i propagowaniu wprowadzania narzędzi z zakresu cyberbezpieczeństwa oraz bezpiecznej infrastruktury sieciowej. W kształceniu akademickim podmioty KSC będą wspierały wiedzą i doświadczeniem budowanie świadomości w zakresie odporności na cyberzagrożenia przez wykłady przedstawiające realne i praktyczne wyzwania stojące w tym obszarze przed studentami w ich życiu prywatnym, akademickim, jak i przyszłym życiu zawodowym. Wspierany będzie potencjał jednostek naukowo-badawczych, aby skuteczniej opracowywały nowe technologie i je komercjalizowały oraz efektywnie współpracowały z przedsiębiorstwami.

Kampanie informacyjno-edukacyjne będą adresowane również do seniorów, którzy wymagają podniesienia świadomości na tematy związane z różnego rodzaju oszustwami internetowymi, m.in. wyłudzaniem danych wrażliwych (tzw. phishing), podszywaniem się pod zaufane podmioty (tzw. spoofing), a które także będą uczulać seniorów na stosowane przez oszustów socjotechniki i manipulacje. W tym zakresie będą realizowane również kampanie edukacyjne uwzględniające potrzeby osób z niepełnosprawnościami. Realizowane kampanie edukacyjne będą dostosowane do specyfiki poszczególnych grup docelowych (w tym młodzieży, seniorów, osób z niepełnosprawnościami, przedsiębiorców) oraz będą uwzględniały wymogi dostępności komunikacyjnej dla osób ze specjalnymi potrzebami.

Realizowane będą działania wspierające rozwój kadr w polskich firmach z branży cyberbezpieczeństwa. Realizowane będą kampanie docierające do polskich przedsiębiorców i ich pracowników upowszechniające wiedzę o technologiach cyberbezpieczeństwa. Planowanym rezultatem kampanii będzie podniesienie wśród przedsiębiorców kompetencji cyberbezpieczeństwa. Działania skierowane do małych i średnich przedsiębiorców będą podzielone na wiele warstw i będą dotyczyły problemów zarówno mikroprzedsiębiorców, jak i małych i średnich firm. Zostaną przygotowane również usługi cyfrowe mające na celu sprawdzenie poziomu dojrzałości cyfrowej i cyberbezpieczeństwa dla małych i średnich przedsiębiorstw, wsparcie producentów technologii informacyjnych we wdrożeniu wymagań wynikających z CRA oraz ocena, czy działalność firmy podlega regulacjom NIS2, które zostaną wdrożone przez nowelizację ustawy o KSC.

Prowadzone będą działania wzmacniające cyberbezpieczeństwo i promujące higienę cyfrową wśród przedsiębiorstw. Rozwijane będą już istniejące programy certyfikacji cyberbezpieczeństwa, w tym Firma Bezpieczna Cyfrowo, które mają na celu podniesienie poziomu ochrony w sektorze małych i średnich przedsiębiorstw, jak i podniesienie stabilności obrotu gospodarczego w kraju, a także upowszechnienie i wdrożenie nowego standardu cyberbezpieczeństwa w firmach. Prowadzone będą również kampanie edukacyjne mające na celu zwiększenie poziomu świadomości polskich przedsiębiorstw na temat cyberbezpieczeństwa. Działania w tym obszarze będą też wspierane przez rozwój kierunków na uczelniach wyższych, formy partnerstwa publiczno-prywatnego, rozwój ISAC i ośrodków kompetencji cyberbezpieczeństwa, współpracę ze szkołami ponadpodstawowymi, tak aby zainteresować młodzież potencjałem branży cyberbezpieczeństwa. Dostępna baza wiedzy o cyberbezpieczeństwie na rządowym portalu gov.pl będzie stale rozwijana, oferując wsparcie i informacje z zakresu cyberbezpieczeństwa, co umożliwi użytkownikom internetu szybki dostęp do potrzebnych zasobów edukacyjnych. Realizacja tych inicjatyw jest niezbędna, aby skutecznie budować kompetencje, wiedzę oraz świadomość zagrożeń i wyzwań w cyberprzestrzeni, co jest kluczowe dla bezpieczeństwa całego kraju. W ramach rozwoju bazy wiedzy o cyberbezpieczeństwie na portalu gov.pl,

będą publikowane informacje z obszaru cyberbezpieczeństwa, w tym ostrzeżenia o bieżących zagrożeniach, poradniki, rekomendacje i standardy cyberbezpieczeństwa. Ponadto będą zamieszczane tam również informacje o realizowanych szkoleniach online wraz z możliwością zapisów na nie.

10. Cel szczegółowy 6. Wzmocnienie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa

10.1. Aktywna współpraca międzynarodowa na poziomie strategiczno-politycznym i prawnym

Z uwagi na fakt, że cyberprzestrzeń jest obszarem strategicznej konkurencji, zagrożenie dla bezpieczeństwa i obrony wzrasta w czasie pogłębiających się geopolitycznych napięć i coraz większej zależności od technologii cyfrowych. Znaczące pogorszenie się sytuacji bezpieczeństwa w wymiarze globalnym i europejskim, rosnąca skala cyberataków ze strony państw nieprzyjaznych, grup powiązanych ze strukturami państwowymi (APT) i haktywistycznych oraz międzynarodowych grup cyberprzestępczych, prowadzone w cyberprzestrzeni działania hybrydowe i terrorystyczne, sprawiają, że współpraca międzynarodowa, zwłaszcza wśród państw sojuszniczych oraz podzielających podobne wartości, jest ważna, jak nigdy dotąd.

Partnerzy podzielający wspólne wartości odgrywają istotną rolę w utrzymywaniu globalnej, otwartej, stabilnej i bezpiecznej cyberprzestrzeni i mogą zwiększyć zdolność RP, NATO i UE do przeciwdziałania szkodliwym zachowaniom w cyberprzestrzeni, zniechęcania do takich zachowań, ich powstrzymywania oraz reagowania na nie. Polska pozostaje otwarta na szeroko zakrojoną, ambitną i korzystną dla wszystkich zaangażowanych stron współpracę w obszarze bezpieczeństwa i obrony, w tym cyberobrony, z partnerami. RP będzie brać udział w pracach mających na celu redefinicję norm prawa międzynarodowego – zarówno prawa wojny, jak i prawa konfliktów zbrojnych – do nowego środowiska walki, jakim stała się cyberprzestrzeń lub tworzenie w tym obszarze nowych norm konwencyjnych. Ponadto będzie dążyć do zwiększenia polskiej obecności w strukturach międzynarodowych, w tym międzynarodowych strukturach wojskowych.

UE i jej państwa członkowskie muszą jeszcze bardziej wzmocnić swoją odporność na zagrożenia cyberbezpieczeństwa i zwiększyć wspólne cyberbezpieczeństwo i cyberobronę przed szkodliwymi zachowaniami w cyberprzestrzeni. RP będzie aktywnie uczestniczyć w pracach UE podnoszących cyberbezpieczeństwo w Europie, w szczególności w wymiarze legislacyjnym. W ramach NATO RP będzie podejmować działania służące wzmacnianiu zdolności obronnych, skuteczności i spójności Sojuszu, w szczególności w obszarach obrony kolektywnej i odstraszania. Ponadto zintensyfikowana zostanie współpraca z organizacjami międzynarodowymi w celu wzmocnienia bezpieczeństwa międzynarodowego i stabilności w cyberprzestrzeni oraz promowania przestrzegania prawa międzynarodowego, w tym ochrony praw człowieka i podstawowych wolności w cyberprzestrzeni. RP będzie się także angażować na rzecz bezpieczeństwa cyfrowego w ramach prac prowadzonych w ONZ, Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE), Organizacji Współpracy Gospodarczej i Rozwoju (OECD) oraz innych organizacji międzynarodowych i formatów współpracy międzynarodowej.

RP będzie współpracować na rzecz cyberbezpieczeństwa w ramach współpracy wielostronnej i dwustronnej. Szczególnie istotnymi partnerami będą Stany Zjednoczone Ameryki, Wielka Brytania, inne pozaeuropejskie państwa podzielające wspólne wartości dotyczące cyberbezpieczeństwa i państwa członkowskie UE oraz państwa kandydujące do UE (w tym Ukraina). RP będzie dążyła do zawiązywania dostosowanych do indywidualnych potrzeb partnerstw w obszarze cyberbezpieczeństwa, jeżeli będą one przynosiły partnerom wzajemne korzyści. W celu zwiększenia naszych możliwości odstraszania przez zapewnienie silnej wspólnej reakcji społeczności międzynarodowej na cyberataki, RP będzie aktywnie poszukiwać, w ramach działalności dyplomatycznej, możliwości wzmocnienia międzynarodowej koordynacji wspólnych działań, w tym kolektywnej atrybucji oraz sankcji.

RP będzie współpracowała na rzecz promowania przestrzegania prawa międzynarodowego w cyberprzestrzeni. W szczególności będzie uczestniczyć w istotnych z punktu prawa międzynarodowego dyskusjach na forum ONZ, OBWE, NATO i UE. Ponadto będzie włączać się w wymianę poglądów na temat relacji prawa międzynarodowego do cyberprzestrzeni przez publiczne prezentowanie swojego stanowiska oraz dialog bilateralny z innymi państwami.

Wspólnie ze swoimi partnerami na szczeblu międzynarodowym RP będzie w dalszym ciągu wspierała Ukrainę, w tym również w ramach dialogu w sprawach cyberprzestrzeni. Biorąc pod uwagę doświadczenie Ukrainy w zwiększaniu zdolności w zakresie cyberodporności i cyberobrony, wymiana najlepszych praktyk w dziedzinie cyberobrony, w tym informacji na temat krajobrazu zagrożeń i świadomości sytuacyjnej, a także wymiana informacji na temat istotnych zmian polityki, leży we wspólnym interesie Ukrainy i RP, dlatego też będzie kontynuowana i poszerzana.

Wspierane będzie umacnianie się pozycji międzynarodowej polskich firm z sektora cyberbezpieczeństwa. Prowadzone będą działania na rzecz wzmocnienia ich potencjału eksportowego, a rozwiązania cyberbezpieczeństwa polskich firm będą promowane na arenie międzynarodowej.

Wzmocnienie pozycji międzynarodowej RP będzie możliwe tylko na drodze wewnętrznej ścisłej kooperacji między instytucjami i agencjami odpowiadającymi w RP za zapewnienie cyberbezpieczeństwa, w tym szczególnie między ministrem właściwym do spraw informatyzacji oraz ministrem właściwym do spraw zagranicznych odpowiadającym za całokształt polskiej polityki zagranicznej.

Dodatkowo ważne są znaczne inwestycje, zarówno indywidualne, jak i wspólne na poziomie unijnym, w zwiększenie odporności i wdrażanie zdolności w zakresie cyberobrony o pełnym spektrum. W tym kontekście kluczowe znaczenie mogą mieć unijne ramy współpracy i zachęty finansowe, a także wprowadzenie wspólnych standardów i uznawanie wzajemne certyfikowanych urządzeń.

Eksperci krajowi będą nadal aktywnie uczestniczyli w dyskusjach prowadzonych na forach oraz w ramach inicjatyw regionalnych i globalnych, a także będą aspirowali do pełnienia kluczowych ról w organizacjach międzynarodowych, przyczyniając się w ten sposób do skutecznej realizacji polityki zagranicznej w zakresie cyberbezpieczeństwa.

Budowanie odporności w cyberprzestrzeni jest globalnym wyzwaniem. RP, włączając się w inicjatywy organizacji międzynarodowych i prowadząc bilateralne działania, będzie przyczyniać się do wzmacniania zdolności partnerów, z którymi współpraca będzie wynikać z celów polityki zagranicznej.

10.2. Aktywna współpraca międzynarodowa na poziomie operacyjnym i technicznym

Współpraca międzynarodowa na poziomie operacyjnym i technicznym będzie realizowana m.in. w ramach NATO, ENISA, Sieci CSIRT (art. 15 dyrektywy NIS 2) oraz Stowarzyszenia INHOPE i INSAFE na poziomie UE oraz na innych forach wymiany informacji i współpracy, takich jak sieć FIRST czy TF-CSIRT, zrzeszające CSIRT-y, Forum Zespołu CSIRT TF-CSIRT, platformy wymiany informacji typu platforma udostępniania informacji o zagrożeniach MISP czy n6 oraz w ramach współpracy dwu- i wielostronnej. Kluczowe dla efektywnej współpracy międzynarodowej na poziomie operacyjnym i technicznym jest, aby w pracach Sieci CSIRT aktywnie uczestniczyły wszystkie CSIRT-y poziomu krajowego. Docelowo w aspekcie europejskiej sieci komunikacji o zagrożeniach cyberbezpieczeństwa (European Cybersecurity Alert System), o której jest mowa w Cyber Solidarity Act, stworzony zostanie NCH. Kolejnym krokiem będzie jego współpraca z wybranymi NCH w co najmniej 3 innych krajach członkowskich w formie Transgranicznego Cyber Hubu (Cross Boarder Cyber Hub).

RP będzie aktywnie włączać się w ćwiczenia prowadzone przez podmioty UE, NATO i inne podmioty międzynarodowe, jak również organizować specjalistyczne szkolenia i ćwiczenia z zakresu cyberbezpieczeństwa w wymiarze międzynarodowym. Pozwoli to m.in. na weryfikację wiedzy i nabytych umiejętności oraz wzmacnianie interoperacyjności zespołów cyberbezpieczeństwa oraz cyberwojsk.

Doskonalenie współpracy międzynarodowej będzie również kontynuowane przez uczestnictwo podmiotów publicznych zaangażowanych w zapewnienie cyberbezpieczeństwa w oficjalnych międzynarodowych forach wymiany informacji o zagrożeniach i podatnościach, a także w ramach międzynarodowych instytucji normalizacyjnych odpowiedzialnych za przygotowywanie i publikację standardów dotyczących cyberbezpieczeństwa.

Doskonalenie współpracy międzynarodowej w obszarze cyberbezpieczeństwa będzie odbywało się na płaszczyźnie uprawnionych organów państwowych i posiadanych przez nie bilateralnych systemów łączności ze służbami partnerskimi NATO.

RP będzie się włączać w europejskie inicjatywy na rzecz wzrostu cyberbezpieczeństwa przez ochronę przemysłu nowych technologii i zapewnienie mu suwerennej konkurencyjności w technologiach przełomowych w wymiarze regionalnym i globalnym. Te wspólne europejskie inicjatywy obejmują już technologie kwantowe o zastosowaniu w cyberbezpieczeństwie.

Współpraca międzynarodowa na poziomie operacyjnym i technicznym obejmie też poszerzenie i wspieranie międzynarodowej współpracy naukowej oraz badawczo-rozwojowej w obszarze cyberbezpieczeństwa.

10.3. Koordynacja działań na arenie międzynarodowej w zakresie współpracy cywilno-wojskowej w obszarze cyberbezpieczeństwa

Pełnomocnik, realizując swoje ustawowe zadania koordynowania działań i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa, będzie prowadził działania RP na arenie międzynarodowej w zakresie współpracy cywilno-wojskowej w obszarze cyberbezpieczeństwa w porozumieniu z ministrem właściwym do spraw informatyzacji, ministrem właściwym do spraw zagranicznych oraz Ministrem Obrony Narodowej, jak również innymi organami administracji rządowej w zakresie ich właściwości. Pozwoli to zwiększyć efektywność działań w stosunkach międzynarodowych i należycie zsynchronizować aktywności w obszarze cyberbezpieczeństwa podejmowane w ramach zarówno relacji wojskowych, jak i cywilnych, a przez to efektywniej realizować narodowe cele strategiczne.

11. Zarządzanie Strategią Cyberbezpieczeństwa Rzeczypospolitej Polskiej

Strategia przyjmowana jest przez RM w drodze uchwały na okres 5 lat.

Koordynatorem wdrażania Strategii jest minister właściwy do spraw informatyzacji.

Po dwóch latach od przyjęcia oraz w czwartym roku obowiązywania dokument podlega przeglądowi i ocenie efektów jego oddziaływania. Wyniki przeglądu są przedstawiane RM. W wyniku dokonanego przeglądu minister właściwy do spraw informatyzacji opracowuje propozycję działań korygujących lub projekt dokumentu na kolejny okres pięcioletni. W przypadku wystąpienia uzasadnionych okoliczności Strategia może być aktualizowana w innych terminach niż te, o których mowa powyżej.

Plan działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej (Plan działań) stanowi załącznik do Strategii. Plan działań określa zadania Koordynatora, członków RM, kierowników urzędów centralnych, dyrektora Rządowego Centrum Bezpieczeństwa (RCB) oraz innych organów właściwych określonych w ustawie o KSC, zgodnie z ich ustawowymi kompetencjami.

Plan działań obejmuje:

1) obszar działania;
2) nr zadania;
3) nazwę zadania;
4) harmonogram;
5) instytucję właściwą / instytucje właściwe;
6) oczekiwane efekty;
7) miernik.

Plan działań obejmuje działania o charakterze projektowym, charakteryzujące się początkiem i końcem okresu realizacji oraz produktami powstałymi w wyniku realizacji danego działania.

Koordynator będzie corocznie przygotowywał sprawozdanie o postępach wdrażania Strategii za rok poprzedni na podstawie informacji otrzymywanych od podmiotów zaangażowanych w jej realizację. Sprawozdania będą przedkładane RM w terminie do dnia 30 września.

12. Finansowanie

Skutki finansowe dla budżetu państwa z tytułu podejmowanych działań zostaną sfinansowane w ramach limitu wydatków zaplanowanych na dany rok budżetowy we właściwych częściach budżetu państwa. Podjęcie działań opisanych w Strategii, a rodzących skutki finansowe, będzie wymagać korzystania z obecnie dostępnych instrumentów z zaplanowanymi środkami finansowymi albo przyjęcie nowych aktów prawa powszechnie obowiązującego. W drugim z wymienionych przypadków na etapie przygotowania projektu przepisów prawa wdrażających postanowienia Strategii zostaną określone skutki finansowe i odpowiednio zabezpieczone środki finansowe.

Na mocy obowiązujących przepisów podmioty realizujące zadania publiczne są obowiązane do ujmowania w swoich planach finansowych nakładów na cyberbezpieczeństwo. Planowanie środków finansowych powinno objąć także zadania ujęte w Planie działań. Strategia nie wywołuje dodatkowych skutków finansowych dla budżetu państwa. Środki finansowe na rzecz realizacji zadań ujętych w Planie działań powinny zostać zabezpieczone przez wiodące lub współpracujące instytucje w ramach swoich planów finansowych.

Źródłami finansowania realizacji działań opisanych w dokumencie będą w szczególności:

1) budżet państwa i plany finansowe poszczególnych jednostek zaangażowanych we wdrażanie Strategii Cyberbezpieczeństwa;
2) środki finansowe pochodzące z Funduszu Cyberbezpieczeństwa;
3) środki pochodzące z NCBR;
4) środki europejskie, w tym w ramach programów i funduszy:
    a) DEP,
    b) Horyzont Europa,
    c) Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC),
    d) Krajowy Plan Odbudowy i Zwiększania Odporności (KPO),
    e) Fundusze Europejskie dla Nowoczesnej Gospodarki (FENG) 2021–2027,
    f) inne programy regionalne.

Plan działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
Cel szczegółowy 1 – Rozwój krajowego systemu cyberbezpieczeństwa								
1.1 Doskonalenie krajowego systemu cyberbezpieczeństwa	1.1.1	Przyjęcie nowelizacji ustawy o KSC wdrażającej dyrektywę NIS 2	2025 (zadanie kontynuowane)	2026	MC	Pozostałe instytucje administracji rządowej	Wdrożenie dyrektywy NIS 2, usprawnienie KSC	Uchwalenie ustawy
	1.1.2	Utworzenie PCOC jako komórki organizacyjnej MC	2026	2027	MC	–	Utworzenie komórki organizacyjnej w MC	Zmiana Regulaminu organizacyjnego MC
	1.1.3	Utworzenie PCOC jako centralnej instytucji państwowej	2027	2029	MC	NASK, ABW, MON, AW, SKW, SWW, RCB, Policja	Utworzenie instytucji	Nadanie statutu
	1.1.4	Dostosowanie przepisów krajowych do zapisów Kodeksu Sieci	2028	2029	ME	MC	Zapewnienie podstaw prawnych do efektywnej realizacji Kodeksów Sieci	Uchwalenie ustawy
	1.1.5	Zapewnienie stosowania rozporządzenia 2022/2554	2025 (zadanie kontynuowane)	2026	MF	KNF	Zwiększenie cyberbezpieczeństwa w sektorze finansowym	Uchwalenie ustawy
	1.1.6	Wdrożenie dyrektywy 2022/2556	2025 (zadanie kontynuowane)	2026	MF	KNF	Zwiększenie cyberbezpieczeństwa w sektorze finansowym	Uchwalenie ustawy
	1.1.7	Dostosowanie systemu cyberbezpieczeństwa RON do wymagań nowelizacji ustawy o KSC (wdrażającej dyrektywę NIS 2)	2025 (zadanie kontynuowane)	2026	MON	DKWOC	Wdrożenie wymagań nowelizacji ustawy o KSC	Zmiana decyzji w sprawie organizacji i funkcjonowania systemu cyberbezpieczeństwa w RON
	1.1.8	Dostosowanie struktur RON odpowiedzialnych za cyberbezpieczeństwo do realizacji nowych zadań	2025 (zadanie kontynuowane)	2026	MON	DKWOC, jednostki podległe Ministrowi Obrony Narodowej i przez niego nadzorowane	Osiągnięcie zdolności do realizacji zadań	Nadanie/zmiana etatu i zakresu kompetencyjnego
	1.1.9	Dostosowanie struktur RON na potrzeby wczesnego wykrywania kryzysów w cyberbezpieczeństwie,	2025 (zadanie kontynuowane)	2027	MON	DKWOC/CSIRT MON, Dowództwo Wojsk Obrony Terytorialnej	Osiągnięcie zdolności do realizacji zadań	Nadanie/zmiana etatu i zakresu kompetencyjnego

[31)] Przy wskazaniu skrótu nazwy danego ministerstwa należy przez to rozumieć ministra właściwego dla danego działu administracji rządowej.

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
		reagowania kryzysowego w cyberbezpieczeństwie i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę w wymiarze militarnym						
	1.1.10	Rozbudowa kompetencji i uprawnień ABW przez nowelizację ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, realizowaną pod nadzorem MKSS oraz dostosowanie struktur ABW odpowiedzialnych za cyberbezpieczeństwo do realizacji nowych zadań wraz z rozbudową zaplecza instytucjonalnego ABW	2025 (zadanie kontynuowane)	2029	ABW	MKSS	Rozbudowa kompetencji i uprawnień ABW w zakresie cyberbezpieczeństwa	Uchwalenie ustawy
1.2 Podniesienie efektywności krajowego systemu cyberbezpieczeństwa	1.2.1	Podłączenie nowych podmiotów do systemu S46 oraz rozwój tego systemu	2024 (zadanie kontynuowane)	2026	MC, NASK	–	Zwiększenie liczby podmiotów KSC podłączonych do systemu S46 i wdrożenie nowych funkcjonalności tego systemu	Osiągnięcie wartości wskaźników określonych we wniosku o objęcie przedsięwzięcia wsparciem
	1.2.2	Dostosowanie systemu S46 do realizacji zadań wynikających w wdrożenia dyrektywy CER	2024 (zadanie kontynuowane)	2026	NASK	RCB	Prowadzenie w systemie S46 wykazu podmiotów krytycznych, o których mowa w dyrektywie CER	Objęcie usługą wszystkich podmiotów krytycznych
	1.2.3	Uruchomienie portalu Cyber.gov.pl	2025 (zadanie kontynuowane)	2026	MC	NASK	Zapewnienie wsparcia dla obywateli, przedsiębiorstw i instytucji publicznych w korzystaniu usług cyberbezpieczeństwa zapewnianych przez administrację rządową	Udostępnienie portalu Cyber.gov.pl
	1.2.4	Utworzenie lub rozwój CSIRT sektorowych	2024 (zadanie kontynuowane)	2027	Organy właściwe	MC, CSIRT poziomu krajowego	Utworzenie nowych CSIRT sektorowych lub rozwój potencjału już istniejącego	Osiągnięcie wartości wskaźników określonych we wniosku o objęcie przedsięwzięcia wsparciem

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
	1.2.5	Utworzenie Centrum Cyberbezpieczeństwa NASK (CCN)	2023 (zadanie kontynuowane)	2029	NASK	MC	Wzmocnienie KSC przez utworzenie centrum, na które złożą się jakościowo nowe tematyczne specjalistyczne centra, ośrodki i laboratoria oraz rozwój potencjału NASK	Osiągnięcie wartości wskaźników określonych we wniosku o dofinansowanie projektu
	1.2.6	Utworzenie wojewódzkich zespołów specjalistów cyberbezpieczeństwa	2024 (zadanie kontynuowane)	2026	MC	NASK, Policja	Utworzenie wojewódzkich zespołów specjalistów cyberbezpieczeństwa działających lokalnie i wspierających podmioty publiczne w obsłudze incydentów i odzyskiwaniu danych oraz prowadzeniu działań podnoszących świadomość o cyberbezpieczeństwie	Osiągnięcie wartości wskaźników określonych we wniosku o objęcie przedsięwzięcia wsparciem
	1.2.7	Realizacja projektu „Cyberbezpieczny Samorząd”	2023 (zadanie kontynuowane)	2027	CPPC	MC, NASK	Zwiększenie poziomu bezpieczeństwa informacji JST przez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych	Osiągnięcie wartości wskaźników określonych we wniosku o dofinansowanie projektu
	1.2.8	Utworzenie Lokalnych Centrów Cyberbezpieczeństwa na poziomie samorządu terytorialnego	2025 (zadanie kontynuowane)	2029	MC, JST	CPPC	Utworzenie Lokalnych Centrów Cyberbezpieczeństwa, działających jako Centra Usług Wspólnych w obszarze IT, które zapewnią wysoki poziom bezpieczeństwa dla instytucji działających na poziomie samorządu terytorialnego	Osiągnięcie wartości wskaźników określonych we wniosku o dofinansowanie projektu
	1.2.9	Wsparcie podmiotów krajowego systemu cyberbezpieczeństwa, w tym wykorzystujących technologie operacyjne (OT)	2024 (zadanie kontynuowane)	2026	MC	CPPC, NASK	Wsparcie podmiotów KSC w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT, w tym wsparcie podmiotów wykorzystujących IT oraz OT stosowane w ICS	Osiągnięcie wartości wskaźników określonych we wniosku o objęcie przedsięwzięcia wsparciem

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
	1.2.10	Opracowanie i przyjęcie Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę	2025 (zadanie kontynuowane)	2029	MC	RCB, CSIRT poziomu krajowego oraz inne ministerstwa i urzędy centralne	Efektem funkcjonowania „Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę" będzie podejmowanie właściwych działań oraz bieżąca analiza zdarzeń	Opracowanie corocznego raportu z zakresu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę oraz opracowywanie rekomendacji mitygującej potencjalne zdarzenia w przyszłości
	1.2.11	Utworzenie zespołów specjalistów cyberbezpieczeństwa działających na rzecz wybranych spółek Skarbu Państwa i wspierających spółki we wdrażaniu bezpieczeństwa informacji, obsłudze incydentów oraz prowadzeniu działań podnoszących świadomość o cyberbezpieczeństwie, czyli wykorzystanie wiedzy z ISAC-MAP	2025 (zadanie kontynuowane)	2029	MAP	–	Podniesienie poziomu cyberbezpieczeństwa w spółkach Skarbu Państwa	Liczba funkcjonujących zespołów specjalistów cyberbezpieczeństwa działających na rzecz wybranych spółek Skarbu Państwa
	1.2.12	Utworzenie ISAC Energia	2025 (zadanie kontynuowane)	2029	ME	CSIRT GOV, CSIRT NASK	Zapewnienie możliwości wymiany informacji pomiędzy OUK sektora energii	Utworzenie ISAC Energia
	1.2.13	Utworzenie ISAC Telko	2025 (zadanie kontynuowane)	2028	UKE	CSIRT GOV, CSIRT NASK	Zapewnienie możliwości wymiany informacji pomiędzy OUK podsektora komunikacji elektronicznej oraz producentami urządzeń i oprogramowania telekomunikacyjnego	Utworzenie ISAC Telko
	1.2.14	Opracowanie i przyjęcie Krajowej Oceny Ryzyka	2025 (zadanie kontynuowane)	2026	RCB	ministerstwa i urzędy centralne	Wdrożenie Unijnego Mechanizmu Ochrony Ludności – Union Civil Protection Mechanism w zakresie Krajowej Oceny Ryzyka w zakresie zidentyfikowanych	Przyjęcie przez RM w drodze uchwały Krajowej Oceny Ryzyka

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
							istotnych zagrożeń m.in. cyberbezpieczeństwa	
	1.2.15	Opracowanie i przyjęcie Strategii w zakresie odporności podmiotów krytycznych	2025 (zadanie kontynuowane)	2026	RCB	ABW, ministerstwa i urzędy centralne	Zwiększenie odporności podmiotów krytycznych przez zapewnienie niezakłóconego świadczenia usług kluczowych przez podmioty krytyczne oraz niezakłóconego funkcjonowania IK	Przyjęcie Strategii w zakresie odporności podmiotów krytycznych, o której mowa w dyrektywie CER
	1.2.16	Ustanowienie National Cyber Hub zgodnie z Cyber Solidarity Act	2026	2029	NASK	–	Powstanie krajowego centrum wymiany informacji o cyberzagrożeniach zgodnie z założeniami CSoA	Osiągniecie wskaźników określonych we wnioskach o finansowanie z DEP
	1.2.17	Organizacja specjalistycznych ćwiczeń i warsztatów cyberbezpieczeństwa z wykorzystaniem nowoczesnych platform typu CyberRange, w szczególności dla podmiotów KSC	2024 (zadanie kontynuowane)	2029	MON	ECSC, MC, ABW	Podniesienie kompetencji i zgrywanie zespołów cyberbezpieczeństwa, weryfikacja nabytych umiejętności w bezpośrednich działaniach/ współzawodnictwie	Liczba zorganizowanych ćwiczeń/warsztatów, liczba uczestników
	1.2.18	Wsparcie przedsiębiorców realizujących zadania na rzecz SZ RP w zakresie ochrony systemów informacyjnych wykorzystywanych do ich realizacji	2025 (zadanie kontynuowane)	2029	MON	DKWOC/CSIRT MON, ABW	Zwiększenie cyberbezpieczeństwa przedsiębiorców realizujących zadania na rzecz SZ RP	Liczba podmiotów objętych wsparciem
1.3 Rozwój zintegrowanego systemu wymiany informacji na potrzeby zapewnienia ciągłości funkcjonowania	1.3.1	Utworzenie SBŁP	2025 (zadanie kontynuowane)	2028 (planowane kontynuowanie)	MSWiA	Policja, KG PSP, KG SG, Służba Ochrony Państwa, ABW, MC, IŁ, RCB, Lotnicze Pogotowie Ratunkowe	Niezawodne, bezpieczne i solidne systemy telekomunikacyjne zapewniające usługi przepływu informacji w czasie pokoju, kryzysu i konfliktu	Liczba podmiotów objętych SBŁP oraz liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
administracji państwowej, bezpieczeństwa narodowego i ochrony ludności	1.3.2	Rozwój i utrzymanie systemu łączności mobilnej do informacji niejawnych do klauzuli „zastrzeżone" (SKR-Z)	2022 (zadanie kontynuowane)	2025 (planowana kontynuacja umowy)	MC, NASK	–	Wsparcie podmiotów administracji publicznej i KSC, podmiotów terenowych i służb mundurowych w komunikacji niejawnej o klauzuli „zastrzeżone"	Osiągnięcie wartości wskaźników określonych we wniosku o dofinansowanie projektu
	1.3.3	Rozwój Komunikatora	2022 (zadanie kontynuowane)	2025 (planowane przedłużenie współpracy na 3 lata)	MC	Operator Chmury Krajowej (OChK)	Wsparcie podmiotów KSC, w tym administracji publicznej oraz służb mundurowych, w jawnej, bezpłatnej i bezpiecznej komunikacji służbowej	Liczba podmiotów i użytkowników
	1.3.4	Komunikator narodowy	2025 (zadanie kontynuowane)	2029	MC	MSWiA, ABW, NASK, MON, DKWOC	Wsparcie podmiotów administracji publicznej przez dostarczenie dostępnego komunikatora do bezpiecznej jawnej łączności	Liczba użytkowników
1.4 Zwiększanie cyberbezpieczeństwa podmiotów nadzorowanych przez organy właściwe do spraw cyberbezpieczeństwa	1.4.1	Realizacja zadań nadzorczych organu właściwego do spraw cyberbezpieczeństwa w sektorze energii	2025 (zadanie kontynuowane)	2029	ME	–	Podniesienie poziomu cyberbezpieczeństwa w sektorze	Liczba podmiotów, w stosunku do których zastosowano środki nadzoru
	1.4.2	Realizacja zadań nadzorczych organu właściwego do spraw cyberbezpieczeństwa w sektorze transportu z wyłączeniem podsektora transportu wodnego	2025 (zadanie kontynuowane)	2029	MI	–	Podniesienie poziomu cyberbezpieczeństwa w sektorze	Liczba podmiotów, w stosunku do których zastosowano środki nadzoru
	1.4.3	Realizacja zadań nadzorczych organu właściwego do spraw cyberbezpieczeństwa w podsektorze transportu wodnego	2025 (zadanie kontynuowane)	2029	MI	–	Podniesienie poziomu cyberbezpieczeństwa w sektorze	Liczba podmiotów, w stosunku do których zastosowano środki nadzoru
	1.4.4	Realizacja zadań nadzorczych organu właściwego do spraw cyberbezpieczeństwa w sektorze bankowym i	2025 (zadanie kontynuowane)	2029	KNF	–	Podniesienie poziomu cyberbezpieczeństwa w sektorze	Liczba podmiotów, w stosunku do których zastosowano środki nadzoru

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
		infrastruktury rynków finansowych						
	1.4.5	Realizacja zadań nadzorczych organu właściwego do spraw cyberbezpieczeństwa w sektorze ochrony zdrowia z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 ustawy o KSC	2025 (zadanie kontynuowane)	2029	MZ	–	Podniesienie poziomu cyberbezpieczeństwa w sektorze	Liczba podmiotów, w stosunku do których zastosowano środki nadzoru
	1.4.6	Realizacja zadań nadzorczych organu właściwego do spraw cyberbezpieczeństwa w sektorze ochrony zdrowia obejmującego podmioty, o których mowa w art. 26 ust. 5 ustawy o KSC	2025 (zadanie kontynuowane)	2029	MON	–	Podniesienie poziomu cyberbezpieczeństwa w sektorze	Liczba podmiotów, w stosunku do których zastosowano środki nadzoru
	1.4.7	Realizacja zadań nadzorczych organu właściwego do spraw cyberbezpieczeństwa w sektorze zaopatrzenia w wodę pitną i jej dystrybucji	2025 (zadanie kontynuowane)	2029	MI	–	Podniesienie poziomu cyberbezpieczeństwa w sektorze	Liczba podmiotów, w stosunku do których zastosowano środki nadzoru
	1.4.8	Realizacja zadań nadzorczych organu właściwego do spraw cyberbezpieczeństwa w sektorze infrastruktury cyfrowej z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 ustawy o KSC	2025 (zadanie kontynuowane)	2029	MC	–	Podniesienie poziomu cyberbezpieczeństwa w sektorze	Liczba podmiotów, w stosunku do których zastosowano środki nadzoru
	1.4.9	Realizacja zadań nadzorczych organu właściwego do spraw cyberbezpieczeństwa w sektorze infrastruktury cyfrowej obejmującego podmioty, o których mowa w art. 26 ust. 5 ustawy o KSC	2025 (zadanie kontynuowane)	2029	MON	–	Podniesienie poziomu cyberbezpieczeństwa w sektorze	Liczba podmiotów, w stosunku do których zastosowano środki nadzoru

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
	1.4.10	Realizacja zadań nadzorczych organu właściwego do spraw cyberbezpieczeństwa dla DUC z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 ustawy o KSC	2025 (zadanie kontynuowane)	2029	MC	–	Podniesienie poziomu cyberbezpieczeństwa w sektorze	Liczba podmiotów, w stosunku do których zastosowano środki nadzoru
	1.4.11	Realizacja zadań nadzorczych organu właściwego do spraw cyberbezpieczeństwa dla DUC obejmujących podmioty, o których mowa w art. 26 ust. 5 ustawy o KSC	2025 (zadanie kontynuowane)	2029	MON	–	Podniesienie poziomu cyberbezpieczeństwa w sektorze	Liczba podmiotów, w stosunku do których zastosowano środki nadzoru
	1.4.12	Realizacja zadań organu właściwego, o którym mowa w Kodeksie Sieci	2026	2029	ME	–	Objęcie podmiotów w sektorze regulacjami wynikającymi z Kodeksu Sieci	Zidentyfikowanie podmiotów o dużym wpływie oraz krytycznym wpływie
1.5 Wypracowanie i wdrożenie metodyki szacowania ryzyka na poziomie krajowym	1.5.1	Opracowanie nowej metodyki szacowania ryzyka	2025 (zadanie kontynuowane)	2026	MC	NASK, IŁ	Analiza ryzyka w ramach KSC	Opracowanie metodyki
Cel szczegółowy 2 – Przeciwdziałanie i zwalczanie cyberprzestępczości oraz uzyskanie zdolności do prowadzenia pełnego spektrum działań w cyberprzestrzeni								
2.1 Wprowadzenie regulacji skuteczniej pozwalających zwalczać cyberprzestępczość	2.1.1	Nowelizacja przepisów dotyczących tajemnicy bankowej	2025 (zadanie kontynuowane)	2026	MS	MF, MSWiA, KNF, MC, ABW, SKW, Policja	Efektywniejsze zwalczanie cyberprzestępczości	Uchwalenie ustawy
	2.1.2	Wprowadzenie obowiązków dla banków i innych instytucji finansowych wspierających zwalczanie cyberprzestępczości	2025 (zadanie kontynuowane)	2029	MF	MS, MSWiA, KNF, MC, ABW, SKW Policja	Efektywniejsze zwalczanie cyberprzestępczości	Uchwalenie ustawy
	2.1.3	Wdrożenie rozwiązań legislacyjnych, organizacyjnych i technicznych służących zwiększeniu ochrony użytkowników internetu przed szkodliwymi i	2025 (zadanie kontynuowane)	2029	MC, NASK	MC, UKE, Policja	Utworzenie systemu zaufanych podmiotów zgłaszających; automatyczne systemy ochrony dzieci przed treściami szkodliwymi i nielegalnymi	Bieżąca analiza treści szkodliwych dla dzieci i młodzieży oraz wydawanie ostrzeżeń; utworzenie jednej struktury w Policji zajmującej się przestępstwami związanymi z CSAM

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
		niebezpiecznymi treściami, w tym w szczególności ochrona dzieci i młodzieży (zwalczanie treści CSAM, patostreamów, grooming itp.)						
	2.1.4	Przegląd rozwiązań zawartych w ustawie o zwalczaniu nadużyć w komunikacji elektronicznej	2026	2027	MC	NASK, UKE, Policja	Analiza skuteczności rozwiązań zawartych w ustawie	Określenie potrzeb zmian w ustawie
	2.1.5	Dostosowywanie do zmian technologicznych przepisów przeciwdziałających kradzieży tożsamości	2025 (zadanie kontynuowane)	2029	MC	MSWiA, MS, ABW, Policja	Ograniczenie zjawiska kradzieży tożsamości w internecie	Uchwalenie ustawy
	2.1.6	Przegląd prawodawstwa i urealnienie odpowiedzialności karnej za cyberprzestępstwa	2025 (zadanie kontynuowane)	2029	MS	MSWiA, MC, ABW, SKW, Policja	Skuteczniejsze odstraszanie przed dokonywaniem cyberprzestępstw	Nowelizacja aktów prawnych
	2.1.7	Nowelizacja ustaw pragmatycznych poszczególnych służb specjalnych oraz Kodeksu karnego w zakresie zwalczania cyberprzestępczości, w tym cyberterroryzmu i cyberszpiegostwa	2025 (zadanie kontynuowane)	2029	MS, MSWiA, ABW, AW, SKW, SWW, Centralne Biuro Antykorupcyjne, Policja	–	Usprawnienie zwalczania cyberprzestępczości	Uchwalenie ustawy
	2.1.8	Nowelizacja przepisów ustawowych w kierunku wprowadzenia kontratypów działań operacyjnych i analitycznych	2026	2029	MSWiA, PK	ABW, Policja, SKW	Usprawnienie zwalczania cyberprzestępczości oraz zapewnienie bezpieczeństwa prawnego funkcjonariuszy	Uchwalenie ustawy
	2.1.9	Rozwój i wdrożenie scentralizowanych narzędzi informatycznych wspierających zwalczanie cyberprzestępczości	2025 (zadanie kontynuowane)	2029	MC	MKSS, ABW, Policja, Prokuratura Krajowa (PK), MS	Skuteczniejsze zwalczanie cyberprzestępczości	Wprowadzenie do użytku narzędzi
2.2 Wzmocnienie wyspecjalizowanych	2.2.1	Tworzenie i rozwijanie wyspecjalizowanych	2025	2029	PK, Policja, ABW	MS	Skuteczniejsze zwalczanie cyberprzestępczości	–

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
struktur zwalczania cyberprzestępczości		zasobów kadrowych wraz z zapleczem instytucjonalnym i technicznym na potrzeby zwalczenia cyberprzestępczości	(zadanie kontynuowane)					
	2.2.2	Rozwój wyspecjalizowanych komórek organizacyjnych do spraw cyberprzestępczości w prokuraturze oraz Policji	2025 (zadanie kontynuowane)	2029	PK, ABW, Policja	–	Skuteczniejsze zwalczanie cyberprzestępczości	Liczba powstałych wyspecjalizowanych komórek organizacyjnych do spraw cyberprzestępczości w prokuraturze oraz Policji
	2.2.3	Rozwój specjalizacji w zakresie ścigania cyberprzestępczości	2025 (zadanie kontynuowane)	2029	PK	MS	Skuteczniejsze zwalczanie cyberprzestępczości	Wprowadzenie specjalizacji w prokuraturze
2.3 Podnoszenie zdolności analitycznych organów ścigania, służb specjalnych i wymiaru sprawiedliwości przy wykorzystaniu nowych technologii	2.3.1	Podnoszenie zdolności analitycznych w zakresie walki z cyberprzestępczością	2025 (zadanie kontynuowane)	2029	PK, Policja, ABW		Skuteczniejsze zwalczanie cyberprzestępczości przy wykorzystaniu zaawansowanych technologii	Wdrożenie nowoczesnych systemów analizy danych
	2.3.2	Szkolenia dla funkcjonariuszy organów ścigania oraz przedstawicieli wymiaru sprawiedliwości i prokuratury z zakresu nowych technologii	2025 (zadanie kontynuowane)	2029	MS	PK, ABW, Policja, MSWiA	Skuteczniejsze zwalczanie cyberprzestępczości przy wykorzystaniu nowych technologii	Liczba zorganizowanych szkoleń
2.4 Podniesienie skuteczności organów ścigania przez wymianę wiedzy i doświadczeń z zakresu cyberbezpieczeństwa oraz metod wykorzystywanych przez sprawców cyberprzestępstw	2.4.1	Szkolenia przedstawicieli wymiaru sprawiedliwości, prokuratury i organów ścigania z zakresu zwalczania cyberprzestępczości	2025 (zadanie kontynuowane)	2029	MS	PK, ABW, Policja	Skuteczniejsze zwalczanie cyberprzestępczości	Liczba zorganizowanych szkoleń
	2.4.2	Współpraca z Interpolem i Europolem w zakresie zwalczania cyberprzestępczości	2025 (zadanie kontynuowane)	2029	Policja	MS	Skuteczniejsze zwalczanie cyberprzestępczości	–
	2.4.3	Szkolenia dotyczące uzyskania danych od podmiotów zagranicznych wykorzystywanych przy	2025 (zadanie kontynuowane)	2029	MS, Policja	ABW, PK	Liczba zorganizowanych szkoleń	Liczba przeszkolonych funkcjonariuszy i prokuratorów

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
		zwalczaniu cyberprzestępczości						
2.5 Zwalczanie cyberterroryzmu i cyberszpiegostwa	2.5.1	Zmiana ustaw regulujących funkcjonowanie służb specjalnych w sposób umożliwiający skuteczne prowadzenie działań operacyjnych w cyberprzestrzeni	2025 (zadanie kontynuowane)	2029	MKSS	ABW, AW, SKW, SWW	Zwiększenie skuteczności w zwalczaniu cyberterroryzmu i cyberszpiegostwa	Uchwalenie ustawy
	2.5.2	Wzmocnienie wyspecjalizowanych struktur zwalczania cyberterroryzmu i cyberszpiegostwa w ABW	2025 (zadanie kontynuowane)	2029	ABW	–	Zwiększenie skuteczności w zwalczaniu cyberterroryzmu i cyberszpiegostwa	Wprowadzenie zmian organizacyjnych w ABW
	2.5.3	Opracowanie systemu utrwalania treści generowanych przez osoby zaangażowane w działalność terrorystyczną wykorzystujące komunikatory internetowe i inne środki komunikacji	2025 (zadanie kontynuowane)	2029	ABW	MS, MSWiA, SKW, Policja	Zwiększenie skuteczności w zwalczaniu cyberterroryzmu i cyberszpiegostwa	Wdrożenie systemu
	2.5.4	Wdrożenie rozwiązań ograniczających nieprawidłowości związane z rejestrowaniem kart SIM	2025 (zadanie kontynuowane)	2029	MC	ABW, Policja, UKE, MS	Zwiększenie skuteczności w zwalczaniu cyberterroryzmu i cyberszpiegostwa oraz innych cyberprzestępstw	Dokonanie zmian w aktach prawnych
	2.5.5	Budowa potencjału zespołów CTI instytucji odpowiedzialnych za cyberbezpieczeństwo na poziomie krajowym w kontekście zwiększania możliwości dystrybuowania informacji do odbiorców krajowych i zagranicznych	2025 (zadanie kontynuowane)	2029	CSIRT poziomu krajowego, AW, ABW, SKW, SWW, MC, Policja	–	Zwiększenie możliwości podmiotów współpracujących w przedmiotowym obszarze działania	Liczba dostarczonych informacji
2.6 Uzyskanie zdolności do prowadzenia pełnego	2.6.1	Organizacja specjalistycznych ćwiczeń oraz szkoleń z	2024 (zadanie kontynuowane)	2029	MON	ECSC, DKWOC, ABW, AW, SKW, SWW	Podniesienie umiejętności oraz wiedzy personelu SZ RP oraz służb	Liczba zorganizowanych ćwiczeń i szkoleń, liczba uczestników

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
spektrum działań w cyberprzestrzeni		obszaru cyberbezpieczeństwa z wykorzystaniem nowoczesnych platform typu CyberRange					specjalnych w zakresie cyberbezpieczeństwa, zgrywanie zespołów cyberbezpieczeństwa oraz weryfikacja nabytych umiejętności w bezpośrednich działaniach	
	2.6.2	Rozwijanie kompetencji personelu w oparciu o zdefiniowane ścieżki szkolenia	2024 (zadanie kontynuowane)	2029	MON	ECSC, DKWOC	Usystematyzowanie sposobu zarządzania kompetencjami i procesem szkolenia personelu cyberbezpieczeństwa RON	Liczba zdefiniowanych ról zawodowych oraz ścieżek rozwoju
	2.6.3	Certyfikacja osób w zakresie cyberbezpieczeństwa w oparciu o posiadane i przyszłe programy certyfikacji	2024 (zadanie kontynuowane)	2029	MON	ECSC, DKWOC	Wprowadzenie standaryzacji oraz ujednolicenie oceny kompetencji personelu cyberbezpieczeństwa RON	Liczba akredytowanych programów certyfikacji oraz wydanych certyfikatów
	2.6.4	Koordynacja wdrażania zobowiązań w ramach Cyber Defence Pledge	2025 (zadanie kontynuowane)	2029	MON	DKWOC, MC, RCB, inne podmioty administracji publicznej	Wzmocnienie cyberodporności na poziomie krajowym	Ankieta – samoocena
	2.6.5	Rozwój systemu detekcji SZ RP (pozyskiwanie telemetrii z systemów istotnych dla obronności państwa) i budowa sieci wymiany informacji o zagrożeniach	2026	2029	DKWOC	SKW	Zwiększenie świadomości sytuacyjnej w cyberprzestrzeni	Liczba podmiotów objętych detekcją
	2.6.6	Aktywne działania w cyberprzestrzeni ukierunkowane na uzyskanie informacji o infrastrukturze sieciowej adwersarzy oraz informacji mających wpływ na bezpieczeństwo RP	2025 (zadanie kontynuowane)	2029	AW, ABW, SKW, SWW, CBA	Organy administracji rządowej	Uzyskanie i przekazanie do właściwych organizacji istotnych dla bezpieczeństwa RP informacji	Liczba i jakość dostarczonych informacji
	2.6.7	Aktywne działania w cyberprzestrzeni ukierunkowane na neutralizację lub ograniczenie funkcjonowania	2025 (zadanie kontynuowane)	2029	Wywiadowcze i kontrwywiadowcze służby specjalne	MON, CSIRT poziomu krajowego	Neutralizacja cyberzagrożeń ze strony infrastruktury adwersarzy	Liczba zneutralizowanych serwerów

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
		poszczególnych elementów struktury (podmioty, narzędzia, schematy) angażowanej przez adwersarza do działań wobec RP						
Cel szczegółowy 3 – Podniesienie poziomu odporności systemów informacyjnych w sferze publicznej (w tym militarnej) oraz prywatnej								
3.1 Podniesienie poziomu odporności systemów informacyjnych	3.1.1	Wprowadzenie wymogów cyberbezpieczeństwa w PZP	2025 (zadanie kontynuowane)	2027	MC	Organy administracji rządowej	Stworzenie jednolitego, efektywnego podejścia dotyczącego cyberbezpieczeństwa zamawianych produktów i usług	Uchwalenie ustawy
	3.1.2	Wprowadzenie procedury pozyskiwania usług i produktów związanych z cyberbezpieczeństwem w pilnych przypadkach związanych z bezpieczeństwem państwa	2026	2027	MC	Organy administracji rządowej	Usprawnienie procesu realizacji pilnych zamówień na potrzeby cyberbezpieczeństwa	Uchwalenie ustawy
	3.1.3	Skoordynowane ujawnianie podatności	2025 (zadanie kontynuowane)	2026	NASK	ABW, MON	Zapewnienie jednego punktu, w którym dowolna osoba może zgłosić w bezpieczny sposób podatność	Wdrożony proces przyjmowania i obsługi zgłoszeń podatności
	3.1.4	Rozwój programu szkoleń oraz narzędzi do praktycznej weryfikacji odporności na zagrożenia phishingowe w RON	2024 (zadanie kontynuowane)	2027	MON	DKWOC, ECSC	Wzrost świadomości żołnierzy i pracowników	Liczba przeprowadzonych symulowanych kampanii phishingowych, liczba szkoleń
	3.1.5	Wdrożenie polityki etykietowania danych w RON	2025 (zadanie kontynuowane)	2027	MON	Sztab Generalny Wojska Polskiego, DKWOC	Zwiększenie bezpieczeństwa informacji przetwarzanych w systemach informatycznych RON	Realizacja harmonogramu
	3.1.6	Opracowanie/aktualizacja standardów i wytycznych z zakresu cyberbezpieczeństwa w ramach RON	2025 (zadanie kontynuowane)	2026	MON	DKWOC	Zwiększenie bezpieczeństwa systemów informatycznych	Liczba opracowanych/zaktualizowanych dokumentów

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
	3.1.7	Przeprowadzenie testów bezpieczeństwa systemów teleinformatycznych eksploatowanych w SZ RP, w tym aktywne testowanie systemów w celu weryfikacji procedur reagowania na incydenty komputerowe oraz sposobów przeciwdziałania atakom na systemy teleinformatyczne RON	2025 (zadanie kontynuowane)	2029	MON, DKWOC/CSIRT MON, SKW	Jednostki podległe Ministrowi Obrony Narodowej i przez niego nadzorowane	Zwiększenie bezpieczeństwa systemów informatycznych	Liczba przeprowadzonych testów bezpieczeństwa
3.2 Rozwój krajowej kryptologii, w tym migracja do kryptografii postkwantowej oraz rozwój technologii kwantowych	3.2.1	Opracowanie Planu migracji do kryptografii postkwantowej	2025 (zadanie kontynuowane)	2029	MC	ABW, MON, MRiT, SKW, NASK, IŁ, DKWOC	Zapewnienie RP bezpiecznej migracji do kryptografii postkwantowej i zabezpieczenie poufności danych w sektorze publicznym i prywatnym	Przyjęcie Planu
	3.2.2	Budowa krajowej sieci komunikacji kwantowej opartej o mechanizm QKD – PIONIER-Q (udział w sieci EURO-QCI)	2023 (zadanie kontynuowane)	2029	Uczestnicy konsorcjum PIONIER-Q	MC, MNiSW, MRiT	Budowa sieci do kwantowej wymiany kluczy szyfrujących wewnątrz kraju i we współpracy międzynarodowej z wykorzystaniem sieci optycznych oraz komunikacji satelitarnej	Liczba linków międzynarodowych; liczba podmiotów mających dostęp do sieci QKD
	3.2.3	Opracowanie i udostępnienie obywatelom, organizacjom oraz przedsiębiorcom nowoczesnych, krajowych narzędzi kryptograficznych (takich jak np. pseudonimy, podpisy domenowe, anonimowe certyfikaty atrybutów, tokeny jednorazowe)	2025 (zadanie kontynuowane)	2029	NASK	MC, MRiT, ośrodki akademickie	Wprowadzenie i rozpowszechnienie nowoczesnych metod uwierzytelniania kryptograficznego, stosowania cyfrowej tożsamości i odporności na ataki na cyfrową tożsamość w oparciu o m.in. DLT	Dostępność cyfrowej tożsamości dla osób prawnych opartej na kluczu publicznym, dostępność pseudonimowego uwierzytelniania dla osób fizycznych, dostępność mechanizmów generowania poświadczeń atrybutów osób fizycznych, dostępność znakowania czasem oparta o DLT, dostępność mechanizmów chroniących przed nieuprawnionym użyciem kluczy do składania podpisu i

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
								uwierzytelniania i zewnętrznymi atakami kryptoanalitycznymi
3.3 Rozwiązania chmurowe dla wzmocnienia odporności systemów informacyjnych	3.3.1	Wspólna Infrastruktura Informatyczna Państwa	2025 (zadanie kontynuowane)	2026	MC	–	Zwiększenie odporności systemów informacyjnych oraz rozwoju cyfrowego administracji publicznej, podejmowane będą działania związane z rozwojem usług przetwarzania w chmurze obliczeniowej	Wprowadzenie Inicjatywy WIIP w drodze ustawy
	3.3.2	Chmura niejawna	2026	2029	MC	ABW, MON, NASK, SKW, DKWOC	Zwiększenie dostępności systemów niejawnych i podniesienie poziomu ich odporności	Liczba podmiotów mających dostęp do niejawnej chmury
	3.3.3	Opracowanie Planu migracji kluczowych systemów informatycznych RP w przypadku wystąpienia kryzysu lub wojny	2026	2029	MC	ABW, MON, SKW, NASK, DKWOC	Zapewnienie możliwości bezpiecznej migracji kluczowych systemów informatycznych RP w przypadku wystąpienia kryzysu lub wojny	Przyjęcie Planu
3.4 Rozwój zdolności do skutecznego zapobiegania i reagowania na incydenty cyberbezpieczeństwa	3.4.1	Rozpoznawanie zagrożeń w cyberprzestrzeni (CTI)	2025 (zadanie kontynuowane)	2029	MC	Podmioty zapewniające cyberbezpieczeństwo na poziomie krajowym	Podniesienie poziomu cyberbezpieczeństwa na poziomie krajowym	Liczba podmiotów KSC wyposażonych w systemy CTI
	3.4.2	Zapewnienie ochrony AntyDDOS dla podmiotów publicznych oraz istotnych z punktu widzenia cyberbezpieczeństwa kraju	2025 (zadanie kontynuowane)	2029	NASK	MC	Zapewnienie ochrony AntyDDOS dla podmiotów publicznych oraz istotnych z punktu widzenia cyberbezpieczeństwa kraju	Liczba podmiotów, dla których zapewniana jest ochrona AntyDDOS
	3.4.3	Prowadzenie ćwiczeń i stress testów w obszarze operatorów IK	2025 (zadanie kontynuowane)	2029	RCB	ministerstwa i urzędy centralne, ABW, AW CSIRTy i organy właściwe ds. IK	Wzmocnienie odporności operatorów IK na zagrożenia antagonistyczne a w szczególności w obszarze cyberbezpieczeństwa	Liczba przeprowadzonych ćwiczeń i stress testów
3.5 Rozwój standaryzacji w cyberbezpieczeństwie	3.5.1	Rekomendacje i standardy cyberbezpieczeństwa	2025 (zadanie kontynuowane)	2029	MC	Partnerzy PWCyber	Wzmocnienie odporności systemów informacyjnych w sektorze publicznym oraz prywatnym przez wdrażanie standardów oraz rekomendacji w	Liczba opracowanych rekomendacji i standardów

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
							zakresie cyberbezpieczeństwa	
	3.5.2	Przygotowanie zaleceń i promowanie dobrych praktyk podnoszących odporność na cyberzagrożenia	2025 (zadanie kontynuowane)	2029	MC	NASK	Zwiększenie świadomości i umiejętności w zakresie cyberbezpieczeństwa	Liczba wdrożonych zaleceń oraz liczba uczestników szkoleń i warsztatów
	3.5.3	Wprowadzenie obowiązku stosowania przez operatorów IK minimalnych standardów w zakresie cyberbezpieczeństwa	2025 (zadanie kontynuowane)	2026	RCB	Organy właściwe ds. IK	RM określi, w drodze rozporządzenia, minimalne wymagania dla operatorów IK m.in. w zakresie cyberbezpieczeństwa, mających na celu wdrażanie adekwatnych do wyników przeprowadzonej analizy zagrożeń rozwiązań	Liczba raportów o stanie ochrony IK przekazanych ministrom właściwym ds. IK
	3.5.4	Utworzenie krajowego ośrodka odpowiadającego za standaryzację w cyberbezpieczeństwie	2026	2027	NASK	MC	Ustalenie wspólnych standardów stosowanych przez podmioty KSC	Liczba wydanych standardów, wytycznych
3.6 Współpraca publiczno-prywatna w obszarze cyberbezpieczeństwa	3.6.1	PWCyber	2025 (zadanie kontynuowane)	2029	MC	–	Propagowanie świadomości i podnoszenie kompetencji podmiotów KSC w zakresie cyberbezpieczeństwa i nowoczesnych technologii	Liczba inicjatyw realizowanych wspólnie z partnerami
	3.6.2	Organizowanie cyklicznych seminariów cyberbezpieczeństwa dla operatorów IK	2023 (zadanie kontynuowane)	2029	RCB	MC, NASK, ABW, MON, SKW	Zwiększenie świadomościi umiejętności w zakresie cyberbezpieczeństwa	Liczba przeprowadzonych seminariów oraz liczba uczestników seminariów
	3.6.3	Organizacja Krajowych forów ochrony infrastruktury krytycznej	2023 (zadanie kontynuowane)	2029	RCB	MC, NASK, ABW, MON, SKW	Propagowanie świadomości w zakresie cyberbezpieczeństwa i nowoczesnych technologii	Liczba przeprowadzonych forów oraz liczba uczestników forów
Cel szczegółowy 4 – Zwiększanie potencjału krajowej bazy technologiczno-przemysłowej oraz wzmocnienie suwerenności technologicznej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa								

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
4.1 Wzmocnienie bezpieczeństwa łańcucha dostaw na poziomie krajowym i międzynarodowym	4.1.1	Uzyskanie zdolności przez krajową jednostkę certyfikującą NASK do wydania certyfikatów w ramach programu EUCC	2024 (zadanie kontynuowane)	2026	NASK	MC, IŁ, Sieć Badawcza Łukasiewicz – Instytut Sztucznej Inteligencji i Cyberbezpieczeństwa	Akredytacja i notyfikacja do certyfikacji w ramach EUCC dla krajowej jednostki certyfikującej NASK	Liczba przeprowadzonych procesów certyfikacji
	4.1.2	Uzyskanie zdolności laboratorium oceny bezpieczeństwa w IŁ do realizacji oceny bezpieczeństwa produktów ICT w ramach programu EUCC, na poziomie uzasadnienia zaufania „wysoki” w pełnym zakresie programu EUCC	2025 (zadanie kontynuowane)	2026	IŁ	NASK	Akredytacja i notyfikacja do certyfikacji w ramach EUCC	Liczba przeprowadzonych procesów certyfikacji
	4.1.3	Wprowadzenie zmian w ustawie – Prawo zamówień publicznych ułatwiających zamówienia z zakresu cyberbezpieczeństwa	2025 (zadanie kontynuowane)	2026	MC	Organy administracji rządowej	Przyjęcie nowelizacji ustawy	–
	4.1.4	Uzyskanie zdolności do certyfikacji w ramach europejskiego programu certyfikacji usług chmurowych (EUCS)	2026	2026	NASK	MC, IŁ, MON, WIŁ	Autoryzacja i notyfikacja dla jednostek oceniających zgodność	Liczba przeprowadzonych procesów certyfikacji
	4.1.5	Przyjęcie pierwszego krajowego schematu certyfikacji cyberbezpieczeństwa	2025 (zadanie kontynuowane)	2026	MC	NASK	Wdrożenie krajowego systemu certyfikacji cyberbezpieczeństwa	Przyjęcie rozporządzenia określającego schemat certyfikacji
	4.1.6	Uzyskanie zdolności do certyfikacji zgodnej z wymogami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany	2025 (zadanie kontynuowane)	2026	NASK	MC, IŁ, MON, WIŁ	Możliwość certyfikacji zgodnej z AI Act w jednostce certyfikującej w NASK	Liczba programów certyfikacji

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
		rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji)						
	4.1.7	Uzyskanie zdolności do certyfikacji zgodnej z wymaganiami aktu o cyberodporności	2025 (zadanie kontynuowane)	2026	NASK	MC, IŁ, ŁUKASIEWICZ-EMAG	Możliwość oceny zgodności do wymagań aktu o cyberodporności w jednostkach oceniających zgodność	Liczba przeprowadzonych ocen
	4.1.8	Uzyskanie zdolności do certyfikacji w ramach europejskiego programu certyfikacji rozwiązań 5G (EU5G) – przygotowanie krajowych zdolności technicznych	2025 (zadanie kontynuowane)	2029	MC	NASK, IŁ	Uzyskanie zdolności do certyfikacji	Liczba przeprowadzonych procesów certyfikacji
	4.1.9	Uzyskanie zdolności krajowego systemu oceny zgodności urządzeń radiowych z wymaganiami cyberbezpieczeństwa określonymi w Dyrektywie RED	2025 (zadanie kontynuowane)	2026	IŁ	MC	Uzyskanie zdolności do certyfikacji	Liczba przeprowadzonych procesów certyfikacji
	4.1.10	Opracowanie i wdrożenie polityki bezpieczeństwa RON dotyczącej przeciwdziałania cyberzagrożeniom w łańcuchu dostaw na rzecz SZ RP	2025 (zadanie kontynuowane)	2027	MON	DKWOC, Inspektorat Wsparcia SZ, Agencja Uzbrojenia	Zwiększenie cyberbezpieczeństwa łańcucha dostaw	Przyjęcie polityki bezpieczeństwa RON dotyczącej przeciwdziałania cyberzagrożeniom w łańcuchu dostaw, liczba jednostek RON, które zaimplementowały politykę
4.2 Stymulowanie badań, rozwoju i innowacji w obszarze cyberbezpieczeństwa	4.2.1	Inicjatywy B+R+I w obszarze cyberbezpieczeństwa	2025 (zadanie kontynuowane)	2029	NCBR	MNiSW, MC, MON, MRiT	Budowa krajowych kompetencji technologicznych i przemysłowych oraz suwerenności technologicznej	Liczba uruchomionych projektów B+R+I w obszarze cyberbezpieczeństwa

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
	4.2.2	Wsparcie dla polskich podmiotów w międzynarodowych inicjatywach B+R+I w obszarze cyberbezpieczeństwa	2025 (zadanie kontynuowane)	2029	MC	MNiSW, NCBR, MON, MRiT	Budowa krajowych kompetencji technologicznych i przemysłowych oraz suwerenności technologicznej	Liczba międzynarodowych projektów B+R+I w obszarze cyberbezpieczeństwa ze wsparciem instytucji rządowych
	4.2.3	Budowa Społeczności kompetentnej w zakresie cyberbezpieczeństwa	2024 (zadanie kontynuowane)	2029	MC		Zwiększenie zdolności i konkurencyjności RP, w tym Europy, w zakresie oferowanych rozwiązań mających na celu zapewnienie cyberbezpieczeństwa, co wpłynie na zwiększenie autonomii strategicznej UE	Liczba wniosków o dołączenie do Społeczności kompetentnej
	4.2.4	Zapewnienie mechanizmów bezpieczeństwa, niezaprzeczalności, integralności i prywatności danych - budowa, utrzymanie i rozwój zastosowań węzła europejskiej sieci EBSI Europeum (blockchain) w RP	2024 (zadanie kontynuowane)	2029	NASK, MC	MS, MF, UNKF, MNiSW, MS, Narodowy Fundusz Zdrowia, Zakład Ubezpieczeń Społecznych	Budowa i utrzymanie odpornej infrastruktury blockchain dla świadczenia usług transgranicznych sektora publicznego	Liczba przypadków użycia w usługach sektora publicznego, liczba transgranicznych przypadków użycia
Cel szczegółowy 5 – Budowanie świadomości, wiedzy i kompetencji kadr podmiotów krajowego systemu cyberbezpieczeństwa oraz obywateli i przedsiębiorców								
5.1 Zwiększenie świadomości i wiedzy oraz wzmocnienie kompetencji kadr podmiotów krajowego systemu cyberbezpieczeństwa	5.1.1	Szkolenia dla podmiotów KSC	2025 (zadanie kontynuowane)	2029	MC	NASK, Partnerzy PWCyber	Podniesienie świadomości i wiedzy oraz wzmocnienie kompetencji kadr podmiotów KSC w zakresie cyberbezpieczeństwa	Liczba zorganizowanych szkoleń
	5.1.2	Szkolenia dla administracji publicznej	2025 (zadanie kontynuowane)	2029	MC	NASK, Partnerzy PWCyber	Podniesienie świadomości i wiedzy oraz wzmocnienie kompetencji kadr administracji publicznej w zakresie cyberbezpieczeństwa	Liczba zorganizowanych szkoleń
	5.1.3	Szkolenia dla administracji samorządowej	2025 (zadanie kontynuowane)	2029	MC	NASK, Partnerzy PWCyber	Podniesienie świadomości i wiedzy oraz wzmocnienie kompetencji kadr administracji	Liczba zorganizowanych szkoleń

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
							samorządowej w zakresie cyberbezpieczeństwa	
	5.1.4	Rozwój programu szkoleń oraz narzędzi do weryfikacji wiedzy i świadomości pracowników MC w zakresie cyberhigieny i cyberzagrożeń	2024 (zadanie kontynuowane)	2029	MC	–	Wzrost świadomości pracowników	Procent pracowników objętych szkoleniami oraz testami weryfikującymi wiedzę
	5.1.5	Wsparcie finansowe dla osób realizujących zadania z zakresu cyberbezpieczeństwa, w ramach funkcjonowania Funduszu Cyberbezpieczeństwa	2024 (zadanie kontynuowane)	2030	MC	–	Ograniczenie odpływu specjalistów do spraw cyberbezpieczeństwa z sektora publicznego oraz wyrównanie poziomu wynagrodzeń w stosunku do sektora prywatnego	Liczba podjętych inicjatyw (udzielonego wsparcia)
	5.1.6	Działania prewencyjno-edukacyjne. Certyfikacja kompetencji w oparciu o Europejskie Ramy Umiejętności w zakresie Cyberbezpieczeństwa w administracji publicznej i w jednostkach samorządu terytorialnego	2025 (zadanie kontynuowane)	2029	MC, NASK	NASK	Podniesienie poziomu wiedzy oraz wzmocnienie kompetencji najważniejszych osób w państwie oraz pracowników urzędów centralnych, JST i innych. Ujednolicenie oceny kompetencji kadr zarządzających podmiotów KSC	Liczba zrealizowanych szkoleń / wydanych certyfikatów
	5.1.7	Utworzenie instytucji odpowiadającej za harmonizację i walidację procesu kształcenia kadr w obszarze cyberbezpieczeństwa	2026	2028	NASK	–	Powołanie i zoperacjonalizowanie jednostki odpowiedzialnej za harmonizację i walidację procesu kształcenia w zakresie cyberbezpieczeństwa	Liczba zwalidowanych programów kształcenia
	5.1.8	Rozwój umiejętności kadry technicznej przez prowadzenie ćwiczeń i zawodów na bazie doświadczeń zawodów ECSC	2025 (zadanie kontynuowane)	2029	NASK, MC	–	Zainteresowanie młodych adeptów cyberbezpieczeństwa – uczniów i studentów udziałem w wymagających wiedzy technologicznej zawodach i ćwiczeniach, w tym konkursach i olimpiadach przedmiotowych z zakresu cyberbezpieczeństwa	–

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
	5.1.9	Tworzenie strategii komunikacyjnych związanych z reagowaniem na skutki incydentów cyberbezpieczeństwa	2025 (zadanie kontynuowane)	2029	NASK	MC	Uspójnienie sposobu reagowania na incydenty z obszaru cyberbezpieczeństwa, tak żeby kluczowe informacje docierały do wszystkich interesariuszy	Bieżące informowanie o aktualnych trendach widocznych w incydentach – propagowanie wiedzy
	5.1.10	Prowadzenie Programów Współpracy z podmiotami KSC służących wymianie doświadczeń, przekazywaniu wiedzy i podejmowaniu wspólnych inicjatyw – jako kontynuacja Programu PdC (Partnerstwo dla Cyberbezpieczeństwa)	2025 (zadanie kontynuowane)	2029	NASK	MC	Podniesienie świadomości i wiedzy oraz wzmocnienie kompetencji z obszaru cyberbezpieczeństwa wśród kadr podmiotów tworzących krajowy system cyberbezpieczeństwa, będących uczestnikami PdC	Liczba zorganizowanych spotkań
	5.1.11	Przeciwdziałanie cyberzagrożeniom i wzmocnienie systemu cyberbezpieczeństwa przez Zespół Zagrożeń Hybrydowych powołany przy Rządowym Zespole Zarządzania Kryzysowego	2025 (zadanie kontynuowane)	2029	RCB	Podmioty administracji publicznej, służby i operatorzy IK	Wczesna identyfikacja zagrożeń hybrydowych oraz wsparcie koordynacji działań w obszarze cyberbezpieczeństwa	Liczba posiedzeń zespołu
	5.1.12	Koordynacja wymiany informacji między administracją, służbami i operatorami IK	2025 (zadanie kontynuowane)	2029	RCB	Podmioty administracji publicznej, służby i operatorzy IK	Bieżąca koordynacja wymiany informacji pomiędzy	–
	5.1.13	Tworzenie cyklicznych raportów o stanie realizacji zadań wynikających z wprowadzonych stopni CRP. Tworzenie raportów o zdarzeniach i incydentach mających miejsce podczas obowiązywania stopni alarmowych CRP	2025 (zadanie kontynuowane)	2029	RCB	Podmioty administracji publicznej i operatorzy IK	Koordynacja działań i tworzenie raportów związanych z wprowadzaniem stopni CRP	Liczba raportów

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
	5.1.14	Zbudowanie systemu certyfikacji osób, w tym wdrożenie programów certyfikacji osób, w tym w oparciu o profile kompetencyjne Europejskich Ram Umiejętności w zakresie Cyberbezpieczeństwa oraz NIST Framework w administracji publicznej, jednostkach samorządu terytorialnego oraz resorcie obrony narodowej	2025 (zadanie kontynuowane)	2029	MC, MON	ECSC, NASK	Podniesienie poziomu wiedzy oraz wzmocnienie kompetencji najważniejszych osób w państwie oraz pracowników urzędów centralnych, JST i innych. Ujednolicenie oceny kompetencji kadr zarządzających podmiotów KSC	Liczba akredytowanych programów certyfikacji oraz wydanych certyfikatów
	5.1.15	Organizacja specjalistycznych, technicznych szkoleń z obszaru cyberbezpieczeństwa z wykorzystaniem nowoczesnych platform typu CyberRange	2024 (zadanie kontynuowane)	2029	MON	ECSC, MC	Podniesienie umiejętności oraz wiedzy personelu podmiotów KSC w zakresie cyberbezpieczeństwa, w szczególności podmiotów administracji publicznej	Liczba zorganizowanych szkoleń oraz przeszkolonych osób
	5.1.16	Organizacja szkoleń/konferencji dotyczących cyberbezpieczeństwa (upowszechnianie dobrych praktyk w zakresie cyberbezpieczeństwa) skierowanych do podmiotów KSC w zakresie kompetencyjnym Ministra Obrony Narodowej	2025 (zadanie kontynuowane)	2029	MON	Jednostki podległe Ministrowi Obrony Narodowej i przez niego nadzorowane	Podniesienie świadomości i wiedzy podmiotów KSC w zakresie cyberbezpieczeństwa	Liczba przedsięwzięć o charakterze informacyjno-edukacyjnym, liczba uczestników
5.2 Rozwój świadomości i wiedzy obywateli i przedsiębiorców z zakresu cyberbezpieczeństwa	5.2.1	Ogólnodostępne szkolenia z cyberbezpieczeństwa i higieny cyfrowej	2025 (zadanie kontynuowane)	2029	MC	NASK, Partnerzy PWCyber (firmy komercyjne), CPPC	Podniesienie świadomości i wiedzy oraz wzmocnienie kompetencji obywateli w zakresie cyberbezpieczeństwa i higieny cyfrowej	Liczba zorganizowanych szkoleń
	5.2.2	Szkolenia z cyberbezpieczeństwa i	2025	2029	MC	MEN, NASK, UKE	Podniesienie świadomości i wiedzy dzieci i	Liczba szkół, przedstawicieli kadry pedagogicznej

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
		higieny cyfrowej dla dzieci i młodzieży oraz kadry pedagogicznej	(zadanie kontynuowane)				młodzieży w zakresie cyberbezpieczeństwa i higieny cyfrowej przez kontynuację wspólnego z NASK i MEN, projektu Cyberlekcje 3.0	(nauczycieli, pedagogów, psychologów) i uczniów objętych projektem
	5.2.3	Kampania informacyjno-edukacyjna – Cyberbezpieczeństwo i higiena cyfrowa dla seniorów	2025 (zadanie kontynuowane)	2029	MC	NASK, CPPC, UKE	Podniesienie świadomości i wiedzy seniorów w zakresie higieny cyfrowej przez prowadzenie kampanii informacyjno-edukacyjnej	Liczba zorganizowanych kampanii informacyjno-edukacyjnych
	5.2.4	Kampania edukacyjno-informacyjna dla przedsiębiorców, upowszechniająca korzyści płynące z wykorzystywania technologii cyfrowych (KEI MŚP)	2025 (zadanie kontynuowane)	2029	MRiT	NASK	Podniesienie świadomości i wiedzy oraz wzmocnienie kompetencji wśród MŚP w zakresie cyberbezpieczeństwa i higieny cyfrowej przez prowadzenie szkoleń	Wskaźniki produktu końcowego: Liczba kampanii edukacyjno-informacyjnych dotyczących TIK –3 Liczba kampanii internetowych – 3 Liczba kampanii PR – 3 Liczba akcji specjalnych – 20 Wskaźniki rezultatu końcowego: Zasięg działań/ kampanii edukacyjno-informacyjnych – ok. 8 mln (osób) Liczba wysłanych wniosków łącznie dla e-usług dotyczących założenia i prowadzenia działalności gospodarczej – min. 7,8 mln Liczba wejść na stronę kampanii dotyczącej cyberbezpieczeństwa dla firm – 1,5 mln
	5.2.5	Baza wiedzy o cyberbezpieczeństwie na rządowym portalu gov.pl	2025 (zadanie kontynuowane)	2029	MC	–	Rozwijanie bazy wiedzy o cyberbezpieczeństwie na rządowym portalu gov.pl	Liczba opublikowanych nowych artykułów na portalu gov.pl
	5.2.6	Rozwój rozwiązań edukacyjnych służących zwiększeniu ochrony użytkowników internetu przed szkodliwymi i niebezpiecznymi treściami, w tym w szczególności ochrona dzieci i młodzieży	2025 (zadanie kontynuowane)	2029	MC, NASK	–	Upowszechnienie wiedzy o szkodliwości określonych treści – dotyczy zarówno CSAM, jak i innych treści szkodliwych dla dzieci i młodzieży. Ograniczenie dostępu dzieci i młodzieży do szkodliwych treści	Liczba akcji informacyjnych oraz uświadamiających, uruchomienie w NASK w ramach Dyżurnet.pl zespołu dedykowanego do identyfikacji i zwalczania treści szkodliwych innych niż CSAM

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
		(zwalczanie treści CSAM, patostreamów, grooming itp.)						
	5.2.7	Wykłady na uczelniach wyższych podnoszące świadomość w zakresie odporności na aktualne cyberzagrożenia	2025 (zadanie kontynuowane)	2029	AW	–	Wzrost świadomości studentów i kadry akademickiej w obszarze cyberbezpieczeństwa. Wzrost liczby studentów wiążących swoją karierę zawodową z cyberbezpieczeństwem, zainteresowanych tematem – większa liczba dostępnych specjalistów na rynku	Liczba przeprowadzonych wykładów
	5.2.8	Przeprowadzanie symulowanych testów socjotechnicznych na rzecz zainteresowanych jednostek sektora publicznego i przedsiębiorstw	2025 (zadanie kontynuowane)	2029	AW	–	Wzrost świadomości pracowników w oparciu o wyniki przeprowadzonych testów. Diagnoza realnej skali zagrożeń wynikających z ataków socjotechnicznych	Liczba przeprowadzonych testów
	5.2.9	Komunikacja na stronach internetowych i publikowanie na profilach mediów społecznościowych kampanii informacyjnych na temat cyberbezpieczeństwa	2024 (zadanie kontynuowane)	2029	RCB	NASK, MC	Wzrost świadomości obywateli. Kampanie informacyjne dotyczące cyberzagrożeń prowadzone na szczeblu krajowym przynoszą wymierne korzyści, które przynoszą wzrost świadomości na temat cyberzagrożeń. Działaniom towarzyszy publikacja infografik związanych z zagrożeniami cybernetycznymi oraz obowiązkami administracji i obywateli w związku z wprowadzanymi stopniami alarmowymi CRP	Liczba publikowanych wiadomości i liczba wyświetleń
	5.2.10	Realizacja projektu Akademia CYBER.MIL	2025 (zadanie kontynuowane)	2029	MON	DKWOC, ECSC	Zwiększenie zainteresowania służbą w SZ RP/ pracą w RON w obszarze	Liczba uczelni biorących udział w projekcie

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
							cyberbezpieczeństwa i informatyki	
	5.2.11	Realizacja warsztatów CyberMil z klasą	2025 (zadanie kontynuowane)	2029	Centralne Wojskowe Centrum Rekrutacji	DKWOC, Akademia Marynarki Wojennej. Wojskowa Akademia Techniczna, Akademia Wojsk Lądowych	Zainteresowanie tematyką cyberbezpieczeństwa w sferze militarnej, wzrost wiedzy uczestników projektu w obszarze cyberbezpieczeństwa i informatyki	Liczba szkół biorących udział w projekcie
	5.2.12	Organizacja konkursu o nagrodę im. Mariana Rejewskiego za najlepszą pracę inżynierską, licencjacką, magisterską i rozprawę doktorską poświęconą cyberbezpieczeństwu i kryptologii	2025 (zadanie kontynuowane)	2029	MON	–	Liczba laureatów zatrudnionych w SZ RP	Liczba prac zgłoszonych do konkursu
	5.2.13	Zwiększenie dojrzałości cyfrowej i cyberbezpieczeństwa firm przez udostępnienie usług cyfrowych na Biznes.gov.pl	2025 (zadanie kontynuowane)	2026	MRiT	NASK	Zwiększenie dojrzałości cyfrowej i cyberbezpieczeństwa firm	Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych – 30 000. Zakończenie procesu opracowywania nowych lub udoskonalania istniejących e-usług – 3. Zakończenie procesu opracowywania nowych lub rozwijania istniejących publicznych systemów informatycznych – 1. Odsetek firm, które wdrożyły otrzymane rekomendacje, spośród tych, które zrealizowały e-usługi – 15%
Cel szczegółowy 6 – Wzmocnienie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa								
6.1 Aktywna współpraca międzynarodowa na poziomie strategiczno-politycznym i prawnym	6.1.1	Udział w Mechanizmie Tallińskim – prowadzenie Back Office	2023 (zadanie kontynuowane)	-	MC	MSZ, organy właściwe	Wsparcie Ukrainy w obszarze cyberbezpieczeństwa	Liczba zrealizowanych działań
	6.1.2	Udział w wydarzeniach międzynarodowych z obszaru cyberbezpieczeństwa oraz prawa	2025 (zadanie kontynuowane)	2029	MC	MSZ, organy właściwe, NASK	Podniesienie świadomości i kompetencji kadr, wzmocnienie obecności polskich ekspertów w	Liczba wydarzeń oraz charakter uczestnictwa

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
		międzynarodowego w tym zakresie					przestrzeni międzynarodowej	
	6.1.3	Wsparcie przy organizacji wydarzeń z obszaru cyberbezpieczeństwa, w których uczestniczą podmioty zagraniczne	2025 (zadanie kontynuowane)	2029	MC	MSZ, organy właściwe, CSIRT-y	Wzmocnienie wizerunku Rzeczypospolitej Polskiej jako ważnego i aktywnego podmiotu w obszarze cyberbezpieczeństwa, wzmocnienie obecności polskich ekspertów w przestrzeni międzynarodowej	Liczba wspólnych działań
	6.1.4	Konceptualizacja i realizacja wybranych projektów w ramach istniejących porozumień G2G	2025 (zadanie kontynuowane)	2029	MC	–	Pogłębianie współpracy międzynarodowej, wymierne korzyści zgodnie z założeniami projektów lub podejmowanych działań	Liczba wspólnych działań
	6.1.5	Ustanawianie dwustronnego dialogu i współpracy na podstawie Protokołów Ustaleń (Memorandum of Understanding)	2025 (zadanie kontynuowane)	2029	MC	MSZ	Bilateralne zacieśnianie współpracy międzynarodowej, przede wszystkim w obszarach wymiany informacji na temat zagrożeń, dzielenia się dobrymi praktykami i współpracy w zakresie reagowania na incydenty i ataki	Liczba wypracowanych porozumień lub konsultacji w ramach podpisanych Protokołów Ustaleń
	6.1.6	Udział w pracach legislacyjnych z obszaru cyberbezpieczeństwa na poziomie UE	2025 (zadanie kontynuowane)	2029	MC	Organy właściwe	Monitorowanie procesów legislacyjnych i reagowanie zgodnie z krajowymi priorytetami	-
	6.1.7	Udział w grupach roboczych oraz eksperckich na poziomie unijnym i międzynarodowym w obszarze cyberbezpieczeństwa oraz prawa międzynarodowego w tym zakresie	2025 (zadanie kontynuowane)	2029	MSZ, organy właściwe	MC	Wzmocnienie wizerunku RP jako ważnego i aktywnego podmiotu w obszarze cyberbezpieczeństwa	-
	6.1.8	Opracowywanie stanowisk do	2025	2029	MSZ, organy właściwe	MC	Wzmocnienie wizerunku RP jako ważnego i	-

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
		prezentowania przez przedstawicieli RP na posiedzeniach lub opracowywanie i przekazywanie stanowisk na piśmie w obszarze cyberbezpieczeństwa oraz prawa międzynarodowego w tym zakresie	(zadanie kontynuowane)				aktywnego podmiotu w obszarze cyberbezpieczeństwa	
	6.1.9	Udział w ćwiczeniach z obszaru cyberbezpieczeństwa oraz prawa międzynarodowego w tym zakresie	2025 (zadanie kontynuowane)	2029	Organy właściwe	MSZ, MC, NASK, CSIRT poziomu krajowego	Polepszenie koordynacji i komunikacji na poziomie krajowym i międzynarodowym	Liczba ćwiczeń
	6.1.10	Prowadzenie konsultacji międzyrządowych w sprawie polityki cyberbezpieczeństwa oraz prawa międzynarodowego w tym zakresie	2025 (zadanie kontynuowane)	2029	MC	MSZ, organy właściwe	Bilateralne zacieśnianie współpracy międzyrządowej	Liczba wspólnych działań lub konsultacji
	6.1.11	Promowanie polskich kandydatur na kluczowe stanowiska w grupach roboczych oraz w organizacjach międzynarodowych w obszarze cyberbezpieczeństwa	2025 (zadanie kontynuowane)	2029	MSZ	MC, MON	Wzmocnienie wizerunku Rzeczypospolitej Polskiej jako kraju o wysokim poziomie profesjonalizmu i kompetencji kadr w obszarze cyberbezpieczeństwa	-
	6.1.12	Wspieranie rozwoju odporności państw trzecich	2025 (zadanie kontynuowane)	2029	MSZ, MC	NASK, organy właściwe, ośrodki akademickie i organizacje pozarządowe	Zwiększenie poziomu bezpieczeństwa otoczenia strategicznego RP	Liczba zrealizowanych projektów pomocowych
	6.1.13	Ustanawianie dwustronnego i multilateralnego dialogu i współpracy na podstawie porozumień w wymiarze militarnym	2025 (zadanie kontynuowane)	2029	MON	DKWOC	Bilateralne/ multilateralne zacieśnianie współpracy międzynarodowej, przede wszystkim w obszarach wymiany informacji na temat zagrożeń, dzielenia	Liczba wypracowanych porozumień lub konsultacji w ramach istniejących porozumień

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
							się dobrymi praktykami i współpracy w zakresie reagowania na incydenty i ataki	
	6.1.14	Organizacja wydarzeń z obszaru cyberbezpieczeństwa w wymiarze militarnym, w których uczestniczą podmioty zagraniczne	2025 (zadanie kontynuowane)	2029	MON	DKWOC, ECSC	Wzmocnienie wizerunku Rzeczypospolitej Polskiej jako ważnego i aktywnego podmiotu w obszarze cyberbezpieczeństwa, wzmocnienie obecności polskich ekspertów w przestrzeni międzynarodowej	Liczba przedsięwzięć
6.2 Aktywna współpraca międzynarodowa na poziomie operacyjnym i technicznym	6.2.1	Działalność przy organizacjach międzynarodowych jako punkt kontaktowy w obszarze cyberbezpieczeństwa	2025 (zadanie kontynuowane)	2029	MSZ, organy właściwe	–	Wymiana informacji na temat zagrożeń, dzielenia się dobrymi praktykami i współpracy w zakresie reagowania na incydenty i ataki	–
	6.2.2	Wymiana informacji i współpraca w ramach międzynarodowych forów technicznych w obszarze cyberbezpieczeństwa	2025 (zadanie kontynuowane)	2029	MC, CSIRT-y	MSZ	Podniesienie poziomu cyberbezpieczeństwa RP oraz budowa zaufania pomiędzy partnerami międzynarodowymi	–
	6.2.3	Udział w inicjatywach i projektach międzynarodowych oraz sieciach współpracy, takich jak EBSI/Europeum (blockchain), rozwój eIDAS, EuroQCI, IRIS2 i innych	2024 (zadanie kontynuowane)	2029	NASK, MC	–	Pogłębianie współpracy międzynarodowej w zakresie standaryzacji i kształtowania bezpiecznych rozwiązań technicznych, prawnych, usługowych wspólnych dla całej UE	Liczba przypadków użycia wskazanych jako wskaźniki w projektach międzynarodowych
	6.2.4	Współpraca w europejskiej sieci komunikacji o zagrożeniach cyberbezpieczeństwa (European Cybersecurity Alert System)	2026	2029	NASK	CSIRT-y poziomu krajowego, CSIRT-y sektorowe, Lokalne Centra Cyberbezpieczeństwa, ISAC	Stworzenie transgranicznego węzła wymiany informacji o cyberzagrożeniach zgodnie z założeniami CSoA	Osiągniecie wskaźników określonych we wnioskach o finansowanie z DEP
	6.2.5	Koordynacja działań i wsparcie w zakresie organizacyjno-	2025 (zadanie kontynuowane)	2029	AW, ABW, SKW, SWW	Organy administracji rządowej	Zwiększenie efektywności i skuteczności działań przez koordynację działań	Liczba i skuteczność przedsięwzięć realizowanych we współpracy z partnerami

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
		technicznym współpracy z partnerskimi służbami specjalnymi						
	6.2.6	Nawiązanie współpracy w domenie cyber z większą liczbą podmiotów zagranicznych	2025 (zadanie kontynuowane)	2029	Podmioty KSC zgodnie z właściwością	Uprawnione organy zagraniczne	Zwiększenie potencjału informacyjnego w domenie cyber właściwej dla służby wywiadowczej	Liczba dostarczonych informacji
	6.2.7	Udział w międzynarodowych ćwiczeniach PACE	2025 (zadanie kontynuowane)	2029	RCB	Ministerstwa i urzędy centralne, ABW, AW CSIRTy i organy właściwe ds. IK	Planowanie, przygotowanie i koordynacja ćwiczeń w wymiarze krajowym oraz w relacjach pomiędzy interesariuszami międzynarodowymi	–
	6.2.8	Organizacja specjalistycznych, technicznych szkoleń z obszaru cyberbezpieczeństwa z wykorzystaniem nowoczesnych platform typu CyberRange, przeznaczonych dla współpracujących podmiotów z państw UE/NATO/Ukrainy	2024 (zadanie kontynuowane)	2029	MON	ECSC, MC	Budowanie rozpoznawalności oraz silnej pozycji Polski na arenie międzynarodowej. Podniesienie poziomu wiedzy i umiejętności personelu odpowiedzialnego za utrzymanie bezpieczeństwa powierzonej im infrastruktury	Liczba przeprowadzonych szkoleń oraz liczba uczestników
	6.2.9	Organizacja międzynarodowych specjalistycznych ćwiczeń cyberbezpieczeństwa z wykorzystaniem nowoczesnych platform typu CyberRange	2024 (zadanie kontynuowane)	2029	MON	ECSC, MC	Sprawdzenie wiedzy i weryfikacja nabytych umiejętności oraz zgrywanie zespołów cyberbezpieczeństwa w bezpośrednich działaniach – zarówno defensywnych, jak i ofensywnych	Liczba przeprowadzonych ćwiczeń oraz liczba uczestników
	6.2.10	Prowadzenie Narodowego Punktu Kontaktowego do współpracy z NATO	2025 (zadanie kontynuowane)	2029	DKWOC/MON	SZ RP	Wzmocnienie współpracy w obszarze z właściwymi organami NATO oraz państwami członkowskimi sojuszu w obszarze cyberbezpieczeństwa	Liczba wspólnych przedsięwzięć /działań
	6.2.11	Aktywny udział w Sieci CSIRT, w szczególności w zakresie wymiany informacji	2025 (zadanie kontynuowane)	2029	CSIRT-y poziomu krajowego	MC, MSZ, organy właściwe	Efektywna i aktywna wymiana informacji na temat zagrożeń, dzielenia się dobrymi praktykami i	–

Obszar działania	Nr zadania	Nazwa zadania	Harmonogram		Instytucja właściwa/instytucje właściwe[31)]		Oczekiwane efekty	Miernik
			Termin rozpoczęcia	Termin zakończenia	wiodąca	współpracujące		
							współpracy w zakresie reagowania na incydenty i ataki	
	6.2.12	Udział w grupach roboczych oraz eksperckich na poziomie unijnym i międzynarodowym w obszarze cyberbezpieczeństwa	2025 (zadanie kontynuowane)	2029	MC, MSZ	CSIRT-y poziomu krajowego, organy właściwe	Efektywna i aktywna współpraca ekspercka w różnych obszarach cyberbezpieczeństwa, zagrożeń, dzielenia się dobrymi praktykami i współpracą w zakresie reagowania na incydenty i ataki	–
6.3 Koordynacja działań na arenie międzynarodowej w zakresie współpracy cywilno-wojskowej w obszarze cyberbezpieczeństwa	6.3.1	Działania koordynacyjne Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa w zakresie międzynarodowej współpracy cywilno-wojskowej w obszarze cyberbezpieczeństwa	2025 (zadanie kontynuowane)	2029	Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa	MC, MSZ, MON	Skoordynowanie działań na arenie międzynarodowej w zakresie współpracy cywilno-wojskowej w obszarze cyberbezpieczeństwa na poziomie krajowym	–
	6.3.2	Koordynacja działań i wymiana informacji z partnerskimi służbami specjalnymi	2025 (zadanie kontynuowane)	2029	AW, ABW, SKW, SWW	Organy administracji rządowej	Zwiększenie efektywności działań przez koordynację działań	Liczba i skuteczność przedsięwzięć realizowanych we współpracy z partnerami
	6.3.3	Udział w międzynarodowych ćwiczeniach CMX	2025 (zadanie kontynuowane)	2029	MC, RCB, organy właściwe, CSIRT-y poziomu krajowego	Ministerstwa i urzędy centralne, AW, organy właściwe ds. IK	Planowanie, przygotowanie i koordynacja ćwiczeń w wymiarze krajowym oraz w relacjach pomiędzy interesariuszami międzynarodowymi	–