Możliwe zmiany w prawie

Cyberbezpieczeństwo w JST – analiza wyników kontroli NIK

Autor podejmuje problematykę poziomu cyberbezpieczeństwa w jednostkach samorządu terytorialnego (JST, samorządy) w Polsce, z wykorzystaniem wyników najnowszych kontroli Najwyższej Izby Kontroli oraz obowiązujących regulacji prawnych. Stawia tezę, że samorządy stanowią obecnie „miękkie podbrzusze" systemu bezpieczeństwa państwa, co wynika z niedostatku zasobów, braku świadomości decydentów, niewystarczających mechanizmów nadzoru oraz sankcji. W artykule nakreśla ramy prawne krajowego systemu cyberbezpieczeństwa, kluczowe obowiązki administracji samorządowej oraz najczęściej występujące nieprawidłowości i luki wskazane przez NIK. Na podstawie analizy empirycznej i przeglądu literatury formułuje rekomendacje *de lege lata* i *de lege ferenda*, wskazując na potrzebę centralizacji wybranych funkcji, wzmocnienia odpowiedzialności indywidualnej oraz rozwoju kompetencji cyfrowych. Podkreśla także znaczenie współpracy z zespołami reagowania na incydenty bezpieczeństwa komputerowego (ang. Computer Security Incident Response Team – CSIRT) i platformą ISAC-JST.

KAMIL SYLWESTER MROCZKA

Wstęp

Nie ulega wątpliwości, że w ostatnich latach istotna część procesów realizowanych przez podmioty administracji publicznej, w tym jednostki samorządu terytorialnego została przeniesiona do świata cyfrowego. Z roku na rok rośnie liczba dostępnych e-usług publicznych. Polskie państwo inwestuje środki finansowe, aby zwiększyć sprawność i efektywność działania administracji publicznej. Działania te bez wątpienia przynoszą wymierne korzyści obywatelom, a w przyszłości pozwolą również na wzrost standaryzacji sposobu świadczenia usług publicznych na rzecz wszystkich interesariuszy. Korzyści wynikające z informatyzacji nie podlegają dyskusji. Należy jednak mieć

na uwadze, że migracja ze świata „papierowego" do świata cyfrowego doprowadziła do powstania nowej kategorii zagrożeń i ryzyka dla państwa i jego instytucji.

W kontekście funkcjonowania podmiotów publicznych technologie informacyjno-komunikacyjne (ang. Information and Communications Technology – ICT) przyczyniają się do zwiększenia efektywności działania urzędów oraz usprawniają przepływ informacji między instytucjami i poprawiają kontakt z obywatelami, a także innymi interesariuszami organów władzy publicznej[1]. Należy jednak mieć świadomość, że „wraz ze wzrostem popularności usług cyfrowych i pojawianiem się nowych technologii rozwija się także cyberprzestępczość, co jest wyraźnie widoczne w statystykach zespołów zajmujących się reagowaniem na incydenty bezpieczeństwa komputerowego. Dodatkowo sytuacja międzynarodowa sprawia, że systematycznie rośnie liczba ataków na instytucje publiczne. W takich okolicznościach ważne jest – jak nigdy przedtem – zadbanie o cyberbezpieczeństwo podmiotów świadczących usługi publiczne i przetwarzających dane obywateli"[2]. W doktrynie podkreśla się, że „współcześnie cyberprzestrzeń (…) i jej ochrona stały się (…) elementem systemu ochrony bezpieczeństwa państwa i obronności"[3]. W rezultacie ochrona systemów IT jest obecnie kluczowa dla sprawnego działania administracji publicznej, w tym również samorządów.

O prawdziwości tego założenia świadczą dostępne dane empiryczne oraz skala incydentów w cyberprzestrzeni. Minister Cyfryzacji Krzysztof Gawkowski prezentując roczne sprawozdanie o cyberbezpieczeństwie w Polsce, poinformował, że w 2024 r. CSIRT poziomu krajowego zarejestrowały łącznie 111 660 incydentów cyberbezpieczeństwa, co było rekordowym wynikiem[4]. Wstępne dane za 2025 r. pokazują, że skala incydentów w cyberprzestrzeni niepokojąco rośnie i do października 2025 r. osiągnęła poziom ok. 170 000[5], z czego duża część dotyczyła właśnie administracji samorządowej. Zdaniem Ministra Cyfryzacji „ataki są prowadzone przez cyberprzestępców (chcą zarobić) oraz cyberterrorystów (chcą wyłączyć podstawowe usługi, np. wodę, kanalizację, energetykę)"[6].

Tezą przyjętą na potrzeby prowadzonych rozważań jest twierdzenie,

---

1 Zob. szerzej: M. Szczegielniak: *Dostęp do informacji w administracji publicznej a rozwój partycypacji obywatelskiej w Polsce*, Warszawa 2025, s. 125.

2 *Cyberbezpieczny samorząd. Poradnik*, Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy, Warszawa 2023, s. 16.

3 K. Chałubińska-Jentkiewicz, A. Brzostek: *Wstęp* [w:] *Modele rozwiązań prawnych w systemie cyberbezpieczeństwa RP. Rekomendacje*, K. Chałubińska-Jentkiewicz (red.), A. Brzostek, Warszawa 2021, s. 5.

4 *Wzrost cyberataków o ponad 20 proc. Gawkowski pokazuje liczby i wskazuje na rosyjskich hakerów. Czy jest tu drugie dno?*, wPolityce.pl, 16.4.2025 r., <https://wpolityce.pl/polityka/726831-wzrost-cyberatakow-gawkowski-pokazuje-liczby-drugie-dno> (dostęp: 30.11.2025).

5 *Gawkowski: miękkie podbrzusze systemu cyberbezpieczeństwa to samorząd*, Serwis Samorządowy PAP, <https://samorzad.pap.pl/kategoria/aktualnosci/gawkowski-miekkie-podbrzusze-systemu-cyberbezpieczenstwa-samorzad> (dostęp: 30.11.2025).

6 *Samorządowa platforma cyberbezpieczeństwa zwiększy cyfrową odporność JST*, Serwis Samorządowy PAP, <https://samorzad.pap.pl/kategoria/e-urzad/samorzadowa-platforma-cyberbezpieczenstwa-zwiekszy-cyfrowa-odpornosc-jst> (dostęp: 30.11.2025).

że jednostki samorządu terytorialnego stanowią „miękkie podbrzusze państwa" w wymiarze cyberbezpieczeństwa, dlatego że JST nie posiadają adekwatnych zasobów kadrowych i finansowych, a decydenci samorządowi nie mają odpowiedniej świadomości istotności kwestii związanych z bezpieczeństwem informacji. Czynnikiem, który negatywnie wpływa na ten stan rzeczy jest również brak adekwatnych mechanizmów sankcyjnych i kar indywidualnych nakładanych na osoby odpowiedzialne za zarządzanie cyberbezpieczeństwem samorządów. Co prawda istnieją mechanizmy odpowiedzialności porządkowej i pracowniczej, a także karnej (np. art. 231 kodeksu karnego[7]), lecz – w mojej ocenie – w praktyce nie funkcjonują skutecznie, a sankcje nie odnoszą się wystarczająco do naruszeń obowiązków w zakresie cyberbezpieczeństwa. Warto w tym miejscu wskazać, że prawodawca krajowy – implementując rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego (rozporządzenie DORA[8]) – zdecydował się na wprowadzenie takich kar m.in. dla osób odpowiadających za zarządzanie podmiotami finansowymi[9].

Na potrzeby weryfikacji założonej tezy sformułowano następujące pytania badawcze: jak definiowane jest cyberbezpieczeństwo w ujęciu prawa unijnego i krajowego? Jakie podmioty tworzą krajowy system cyberbezpieczeństwa? Jakie są zadania jednostek samorządu terytorialnego w tym zakresie? Jak przedstawia się ocena działań JST w kontekście wyników kontroli NIK? Jakie są najważniejsze wyzwania związane z cyberbezpieczeństwem administracji samorządowej?

Przyjęte założenia badawcze zdefiniowały warstwę metodologiczną artykułu. Na potrzeby prowadzonych rozważań wykorzystano analizę instytucjonalno-prawną oraz analizę danych empirycznych zawartych w wystąpieniach pokontrolnych i raportach wyspecjalizowanych podmiotów krajowego systemu cyberbezpieczeństwa. Uzupełnieniem są obserwacje autora wynikające z jego doświadczeń zawodowych oraz publikowanych wcześniej ustaleń[10].

---

[7] Ustawa z 6.7.1997 – Kodeks karny (t.j. Dz.U. z 2025 r. poz. 383, z późn. zm.).

[8] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14.12.2022 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 (Dz. U. UE. L. z 2022 r. nr 333, s. 1, z późn. zm.).

[9] Ustawa z 25.6.2025 o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji (Dz.U. poz. 1069).

[10] W artykule wykorzystano wcześniejsze ustalenia autora publikowane w ciągu ostatnich kilku lat m.in.: K. Mroczka, K. Maderak, K. Zieliński: *Nadzór nad cyberbezpieczeństwem rynku finansowego w Polsce: perspektywa nadzorcza,* [w:] *Finanse cyfrowe: informatyzacja, cyfryzacja i datafikacja,* L. Gąsiorkiewicz (red.), J. Monkiewicz, Warszawa 2021; K. Mroczka, P. Piekutowski: *Cyber Safe Place – ochrona cyberbezpieczeństwa rynku finansowego jako zyskujące na znaczeniu zadanie Komisji Nadzoru Finansowego* [w:] *Bezpieczeństwo terrorystyczne budynków użyteczności publicznej. Tom 4. Bezpieczeństwo w cyberprzestrzeni oraz praktyczny wymiar zabezpieczeń technicznych,* J. Stelmach (red.), Warszawa 2022; K. Mroczka, B. Biderman: *Uwarunkowania prawne nadzoru nad cyberbezpieczeństwem rynku finansowego w Polsce,* „Bezpieczny Bank" nr 2/2022; K. Mroczka, M. Szczegielniak, J. Brzozowski: *Kluczowe problemy i wyzwania w zakresie budowania odporności cyfrowej i cyberbezpieczeństwa jednostek samorządu terytorialnego w Polsce – analiza empiryczna w świetle wyników kontroli,* „Cybersecurity and Law" 2/2025; K. Mroczka, M. Groniewski: *Krajobraz*

Warto w tym miejscu podkreślić, że w styczniu 2026 r. Sejm Rzeczypospolitej Polskiej uchwalił nowelizację ustawy o krajowym systemie cyberbezpieczeństwa[11]. Na dzień finalizacji prac nad tekstem proces nie został zakończony. Wobec powyższego artykuł skupia się na regulacjach obowiązujących według stanu na 31 stycznia 2026 r. Należy jednak podkreślić, że nowelizacja wprowadza szereg istotnych zmian, które zostaną zasygnalizowane na marginesie prowadzonych rozważań związanych z analizą ustaleń Najwyższej Izby Kontroli.

Konceptualizacja terminu cyberbezpieczeństwo

Dorobek doktryny związany z konceptualizacją terminu „cyberbezpieczeństwo" znacząco powiększył się w ostatnich latach. Wynika to w dużej mierze z aktywności legislatorów poziomu zarówno unijnego, jak i krajowego oraz z dynamicznego rozwoju sektora usług ICT.

Z uwagi na ograniczenia objętości artykułu oraz zasadniczy cel badawczy przegląd definicji zostanie ograniczony do wybranych definicji prezentowanych w doktrynie oraz definicji legalnych.

Przedstawiciele doktryny prezentują różne perspektywy badawcze, co bez wątpienia wpływa na definiowanie terminu cyberbezpieczeństwo. Robert Siudak, reprezentujący nauki o polityce i administracji uważa, że cyberbezpieczeństwo to proces, który ma za zadanie „doprowadzenie do stanu, w którym możliwe niebezpieczeństwa nie przekraczają akceptowalnego poziomu ryzyka dla poszczególnych podmiotów bezpieczeństwa"[12]. Z kolei z perspektywy prawnej podkreśla się trudności interpretacyjne i nieostrość pojęcia cyberbezpieczeństwa (bezpieczeństwa w cyberprzestrzeni) oraz jego złożoność i wieloaspektowy, niejednoznaczny charakter[13].

Definicja terminu cyberbezpieczeństwo została zawarta w art. 2 pkt 4 ustawy z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Przepis ten stanowi, że jest to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy"[14]. Przywołana definicja zwraca uwagę na naruszenia konkretnych atrybutów, które wymagają szczególnej ochrony: poufność, integralność, dostępność

cyberbezpieczeństwa rynku finansowego w Polsce a poziom edukacji finansowej – perspektywa organu nadzoru nad rynkiem finansowym oraz jego interesariuszy, „Studia Politologiczne" 2025, vol. 77.

[11] Ustawa z 23.1.2026 o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, Sejm Rzeczypospolitej Polskiej, <https://orka.sejm.gov.pl/opinie10.nsf/nazwa/1955_u/$file/1955_u.pdf> (dostęp: 5.2.2026). Tekst ustawy Senat przyjął bez poprawek. Warto w tym miejscu podkreślić, że ustawa została podpisana przez Prezydenta RP i jednocześnie skierowana do Trybunału Konstytucyjnego w trybie kontroli następczej. Prezydent podał w wątpliwość: objęcie ustawą aż 18 branż gospodarki pogrupowanych w podmioty kluczowe i ważne, uregulowanie zasad uznawania podmiotów za dostawców wysokiego ryzyka oraz zasady wydawania tzw. poleceń.

[12] R. Siudak: *Cyberbezpieczeństwo w Polsce. Od dyskursów do polityk publicznych*, Kraków 2022, s. 280-281.

[13] C. Banasiński: *Pojęcie cyberbezpieczeństwa* [w:] *Cyberbezpieczeństwo. Zarys wykładu*, C. Banasiński (red.), Warszawa 2023, s. 31-37.

[14] Ustawa z 5.7.2018 o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077, z późn. zm., art. 2 pkt 4).

i autentyczność. Filip Radoniewicz precyzuje, że w kontekście ochrony systemów informacyjnych poufnością określa się dostęp do danych tylko przez osoby do tego uprawnione[15]. Integralność z kolei oznacza dokładność i kompletność danych i informacji wraz z utrzymaniem ich w takim stanie[16]. Dostępność jest tym atrybutem, który wiąże się z możliwością korzystania z informacji przez uprawnione osoby, ilekroć zajdzie taka potrzeba[17]. Autentyczność zdefiniowana jest w rozporządzeniu Rady Ministrów z 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (KRI) jako „właściwość polegająca na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie, jak deklarowane"[18].

Warto w tym miejscu podkreślić, że krajowy ustawodawca konstruując definicję w ustawie z lipca 2018 r., uwzględnił definicję przyjętą na poziomie dyrektywy NIS[19]. Co prawda dyrektywa nie definiuje wprost pojęcia cyberbezpieczeństwo, ale w art. 4 wprowadza pojęcie „bezpieczeństwa sieci i systemów informatycznych". Określa je jako „odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych, lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne"[20].

Samorząd terytorialny w Polsce

Na temat samorządu terytorialnego w Polsce powstały setki wartościowych prac, raportów i analiz. Ich przytaczanie w tym miejscu wykracza poza przyjęte założenia badawcze. Zamierzeniem autora jest przywołanie najważniejszych informacji dotyczących struktury jednostek samorządu terytorialnego w ujęciu liczbowym według stanu na 1 stycznia 2025 r.

Zgodnie z brzmieniem art. 163 Konstytucji Rzeczypospolitej Polskiej: „samorząd terytorialny wykonuje zadania publiczne nie zastrzeżone przez Konstytucję lub ustawy dla organów innych władz publicznych"[21]. W orzecznictwie i doktrynie podkreśla się, że powołany przepis stanowi „pewną generalną deklarację, która ma wzmocnić jego pozycję ustrojową. Polega ona na założeniu, że społeczności lokalne powinny mieć zapewnioną – w zakresie określonym prawem – pełną swobodę działania w każdej sprawie, która nie jest wyłączona z ich kompetencji lub nie wchodzi w zakres kompetencji innych

[15] F. Radoniewicz: *Objaśnienie pojęć* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, W. Kitler (red.), J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, s. 31.
[16] Tamże.
[17] Tamże.
[18] Rozporządzenie Rady Ministrów z 21.5.2024 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 r. poz. 773, §2, pkt 2).
[19] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.7.2016 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. UE L. z 2016 r., nr 194).
[20] Tamże, art. 4, pkt 2.
[21] Konstytucja Rzeczypospolitej Polskiej z 2.4.1997 (Dz.U. nr 78 poz. 483, z późn. zm.).

organów władzy”[22]. Przyjęta przez prawodawcę konstytucyjnego konstrukcja prawna jest określana w doktrynie mianem domniemania kompetencji (domniemania kompetencyjnego), domniemania zadań lub domniemania właściwości[23].

Od 1 stycznia 1999 r., na podstawie ustawy z 24 lipca 1998 r. wprowadzono zasadniczy trójstopniowy podział terytorialny państwa[24]. Zgodnie z art. 2 ust. 1 jego jednostkami są: gminy, powiaty i województwa. Ustawa określiła strukturę podziału terytorialnego, w ramach którego funkcjonują JST, natomiast same jednostki zostały powołane odrębnymi ustawami ustrojowymi[25]. Według danych Ministerstwa Spraw Wewnętrznych i Administracji na 1 stycznia 2025 r. Polska dzieli się na 16 województw, 314 powiatów i 2479 gmin (302 miejskie w tym 66 miast na prawach powiatu, 718 miejsko-wiejskich oraz 1459 wiejskich)[26].

Krajowy system cyberbezpieczeństwa

Zgodnie z intencją prawodawcy wyrażoną w art. 3 ustawy z lipca 2018 r. celem krajowego systemu jest „zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów”.

W ujęciu podmiotowym krajowy system cyberbezpieczeństwa (KSC) obejmuje szereg podmiotów: operatorów usług kluczowych; dostawców usług cyfrowych; CSIRT MON; CSIRT NASK; CSIRT GOV; sektorowe zespoły cyberbezpieczeństwa; wybrane jednostki sektora finansów publicznych; instytuty badawcze; Narodowy Bank Polski; Bank Gospodarstwa Krajowego; Urząd Dozoru Technicznego; Polską Agencję Żeglugi Powietrznej; Polskie Centrum Akredytacji; Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej; spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej; podmioty świadczące usługi z zakresu cyberbezpieczeństwa; organy właściwe do spraw cyberbezpieczeństwa; Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa; Pełnomocnika Rządu do spraw Cyberbezpieczeństwa; oraz Kolegium do spraw Cyberbezpieczeństwa.

---

[22] Wyrok Wojewódzkiego Sądu Administracyjnego we Wrocławiu z 26.5.2010, II SA/Wr 70/10, LEX nr 674616.

[23] Zob. szerzej: H. Izdebski: *Domniemanie zadań samorządu terytorialnego i domniemanie zadań gminy w obrębie samorządu terytorialnego – klauzule generalne dotyczące zadań samorządu*, „Samorząd Terytorialny” nr 1-2/2015, s. 69.

[24] Ustawa z 24.7.1998 o wprowadzeniu zasadniczego trójstopniowego podziału terytorialnego państwa (Dz.U. nr 96 poz. 603, z późn. zm.).

[25] Ustawa z 8.3.1990 o samorządzie gminnym (t.j. Dz.U. z 2025 r. poz. 1153, z późn. zm.), ustawa z 5.6.1998 o samorządzie powiatowym (t.j. Dz.U. z 2025 r. poz. 1684), ustawa z 5.6.1998 o samorządzie województwa. (t.j. Dz.U. z 2025 r. poz. 581, z późn. zm.).

[26] *Baza JST. Samorząd terytorialny w Polsce,* Ministerstwo Spraw Wewnętrznych i Administracji, <https://www.gov.pl/web/mswia/baza-jst> (dostęp: 19.10.2025).

Już pobieżna analiza tego katalogu prowadzi do wniosku, że krajowy system cyberbezpieczeństwa tworzą najważniejsze podmioty świadczące usługi na rzecz obywateli i innych interesariuszy systemu władzy publicznej. Co prawda JST nie stanowią odrębnej kategorii podmiotowej zdefiniowanej w art. 4 ustawy, lecz są objęte tą regulacją jako wybrane jednostki sektora finansów publicznych.

Obowiązki JST w zakresie cyberbezpieczeństwa

Nie ulega wątpliwości, że dynamiczny rozwój technologii ICT oraz rosnące zagrożenia w cyberprzestrzeni wymuszają na podmiotach publicznych, w tym jednostkach samorządu terytorialnego, wdrażanie skutecznych mechanizmów ochrony danych i systemów teleinformatycznych. Ustawa o krajowym systemie cyberbezpieczeństwa jest najważniejszym aktem prawnym określającym kompetencje, obowiązki i zadania w tym zakresie. Przywołana regulacja obejmuje szeroki katalog podmiotów realizujących zadania publiczne, w tym gminy, powiaty, województwa, związki JST, związki metropolitalne oraz samorządowe zakłady budżetowe[27]. Bez wątpienia ustawa z lipca 2018 r. ma charakter kompleksowy – określa zarówno obowiązki związane z zarządzaniem incydentami, jak i inne wymogi dotyczące kształtowania odporności cyfrowej administracji samorządowej.

Obowiązki jednostek samorządu terytorialnego obejmują kilka obszarów. Na podstawie art. 21 ustawy mają obowiązek wyznaczenia osoby odpowiedzialnej za utrzymanie kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa. Ustawodawca nie precyzuje szczegółowych kompetencji tej osoby, co w praktyce rodzi problemy interpretacyjne. Dodatkowo powołany przepis nie precyzuje, jakie wymagania musi spełniać taka jednostka kontaktowa, jak również nie jest powiedziane, że wyznaczona musi być osobą fizyczną. W praktyce jednak takie jednostki wskazują właśnie osoby fizyczne o właściwych kompetencjach[28]. Podstawowym obowiązkiem osoby wyznaczonej jest utrzymywanie kontaktu z właściwym zespołem CSIRT oraz założenie „punktu kontaktowego", w terminie 14 dni od daty jej wyznaczenia. Obejmuje ono przedstawienie konkretnych danych wymienionych w artykule 22 ust. 1 pkt 5 ustawy[29]. Informację o wskazaniu osoby kontaktowej w odniesieniu do JST przekazuje się do CSIRT NASK (wysyłając na adres ksc@cert.pl), który jest właściwy dla jednostek samorządu terytorialnego, z wyjątkiem przypadku wynikającego z art. 27 ustawy, czyli w zakresie incydentów związanych ze zdarzeniami o charakterze terrorystycznym, przedstawiając niezbędne dane wskazane w ustawie[30].

---

[27] F. Radoniewicz: *Objaśnienie pojęć* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, W. Kitler (red.), J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, s. 58-59.

[28] W. Dziomdziora: *Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik*, Warszawa 2021, s. 31.

[29] Ustawa z 5.7.2018 o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2024 r. poz. 1077, z późn. zm., art. 22, ust. 1, pkt 5).

[30] W. Dziomdziora: *Cyberbezpieczeństwo*…, op.cit., s. 35.

Na JST nałożono również obowiązki i zadania związane z właściwym zarządzaniem incydentami. Obejmują one m.in.: zgłaszanie incydentów, w tym krytycznych, ich obsługę i dokumentowanie, podejmowanie działań naprawczych i zapobiegawczych oraz dzielenie się wiedzą o zagrożeniach z właściwymi CSIRT[31]. Należy podkreślić, że obowiązki te mają charakter nie tylko informacyjny, lecz także operacyjny – wymagają przywrócenia pełnej sprawności systemu informacyjnego oraz wdrożenia procedur minimalizujących ryzyko powtórzenia incydentu. W doktrynie podkreśla się, że JST powinny również „umieć zaimplementować procedury i narzędzia chroniące podmiot publiczny w przyszłości przed zaistnieniem analogicznego incydentu" oraz dokumentować wszystkie, które miały miejsce w przeszłości[32].

Przepis art. 24 ustawy daje podstawę jednostkom samorządowym do przekazywania informacji o możliwych zagrożeniach w przyszłości. Procedura nie została sformalizowana, co może prowadzić do niejednolitości praktyki. Informacje powinny być przekazywane w formie elektronicznej i bez zbędnej zwłoki, aby umożliwić CSIRT odpowiednią reakcję. Wymagania te należy jednak doprecyzować, aby obowiązywał wspólny standard zarządzania informacjami o incydentach. Warto podkreślić, że zgodnie z art. 25 wobec podmiotu publicznego może zostać również wydana decyzja o uznaniu go za operatora usługi kluczowej, co nakłada na podmiot dodatkowe obowiązki określone w art. 8-16 ustawy[33].

Podmioty wykonujące zadania publiczne są również zobowiązane do korzystania z systemów teleinformatycznych spełniających minimalne wymagania oraz zapewniających interoperacyjność, zgodnie z zasadami określonymi w Krajowych Ramach Interoperacyjności[34]. Oznacza to, że wykorzystywane przez JST systemy teleinformatyczne oraz prowadzone przez nie publiczne rejestry danych muszą spełnić odpowiednie wymagania techniczne określone w rozporządzeniu Rady Ministrów w sprawie Krajowych Ram Interoperacyjności[35]. Nakłada ono m.in. obowiązek zapewnienia właściwych standardów dotyczących bezpieczeństwa, dostępności oraz integralności danych, a także stosowania uzgodnionych standardów komunikacji, które pozwalają na współpracę z systemami innych instytucji publicznych.

Specyfika działania jednostek samorządu terytorialnego sprawia, że uznaje się je za administratorów danych

---

[31] K. Czaplicki: *Obowiązki w zakresie zgłaszania i obsługi incydentu w podmiocie publicznym* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, G. Szpor (red.), A. Gryszczyńska, Warszawa 2019, s. 199.

[32] Tamże.

[33] *Cyberbezpieczny samorząd…..*, op.cit., s. 19.

[34] Ustawa z 17.2.2005 o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2024 r. poz. 1557, 1717, art. 13 ust. 1).

[35] Rozporządzenie Rady Ministrów z 21.5.2024 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 r. poz. 773).

w rozumieniu RODO[36]. Nakłada to na nie obowiązek przeprowadzenia analizy ryzyka i wdrażania środków technicznych i organizacyjnych, które owo ryzyko minimalizują[37]. Samorządy muszą więc nieustannie chronić systemy teleinformatyczne przed zagrożeniami, zapewniać integralność, poufność i dostępność danych, a także wdrażać procedury zarządzania incydentami, mechanizmy kontroli dostępu oraz regularne szkolenia dla pracowników w zakresie bezpiecznego przetwarzania informacji zawierających dane osobowe.

Cyberbezpieczeństwo JST w świetle kontroli NIK

W kwietniu 2025 r. NIK opublikowała wyniki kontroli: „Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego"[38]. Izba ujawniła wiele problemów i wyzwań. Kontrolę przeprowadzono w 24 samorządach – w 17 gminach i 7 powiatach. Czynności kontrolne obejmowały okres od 1 stycznia 2023 r. do 24 września 2024 r. Na potrzeby głównego celu kontroli zdefiniowano pytanie: „Czy prawidłowo, rzetelnie i skutecznie realizowano zadania związane z zapewnieniem bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego?"[39].

W ujęciu szczegółowym zdefiniowano następujące pytania:
1. Czy podjęto prawidłowe, rzetelne i skuteczne działania dla zapewnienia organizacji bezpieczeństwa informacji oraz dla zapewnienia ciągłości działania systemów informatycznych, tj. czy przeprowadzono odpowiednie analizy oraz czy opracowano i przyjęto do stosowania właściwe procedury, polityki, instrukcje oraz określono i zapewniono niezbędne zasoby osobowe i techniczne?
2. Czy prawidłowo, rzetelnie i skutecznie wdrożono przyjęte rozwiązania organizacyjne i techniczne, tj. czy są one faktycznie stosowane i egzekwowane?
3. Czy są cyklicznie podejmowane prawidłowe działania mające na celu zapobieganie incydentom bezpieczeństwa informacji (szkolenia, analiza incydentów, audyty, analiza ryzyka)?

Kluczowe ustalenia

Ocena ogólna sformułowana przez NIK jednoznacznie wskazuje, że w skontrolowanych jednostkach poziom cyberbezpieczeństwa jest niewystarczający. Co prawda wyników ustaleń nie można automatycznie uogólniać w odniesieniu do wszystkich JST, jednak wskazują one na ryzyko systemowe istotne z perspektywy państwa. Jak stwierdzono w analizowanym wystąpieniu pokontrolnym, „zadania w zakresie zapewnienia bezpieczeństwa informacji

[36] *Cyberbezpieczny samorząd….*, op.cit., s. 17.
[37] Rozporządzenie Parlamentu Europejskiego i Rady 2016/679 z 27.4.2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. U. UE z 2016 r. L 119/1, art. 24 i 25).
[38] Informacja o wynikach kontroli NIK, nr ewid. 123/2024/P/24/004/KAP, Warszawa 2025.
[39] Tamże, s. 7.

Tabela 1. **Najczęściej stwierdzane nieprawidłowości w 24 kontrolowanych podmiotach**

Lp.	Rodzaj nieprawidłowości	Liczba jednostek
1	Brak ustanowionej polityki ciągłości działania	17
2	Brak planów zapewnienia ciągłości działania oraz planów odtworzeniowych	12
3	Niepełna identyfikacja aktywów informacyjnych lub brak przypisania poziomu ochrony zbiorom danych	12
4	Niewystarczające zabezpieczenia fizyczne serwerowni	12
5	Nieprawidłowości w zakresie tworzenia, przechowywania lub testowania kopii zapasowych	12
6	Brak zapisów dotyczących bezpieczeństwa informacji w umowach zakupu lub serwisu sprzętu komputerowego/oprogramowania	11
7	Brak szkoleń dla pracowników zaangażowanych w proces przetwarzania informacji	10
8	Nieprzestrzeganie wymogów dotyczących haseł dostępu do systemów informatycznych	9
9	Brak obowiązkowego audytu bezpieczeństwa informacji w 2023 r. lub jego nierzetelne przeprowadzenie	9
10	Brak opracowanego i wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	8

Źródło: Opracowanie własne na podstawie Informacji o wynikach kontroli NIK: *Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów*…, op.cit.

nie były skutecznie, rzetelnie i prawidłowo wykonywane w większości skontrolowanych urzędów jednostek samorządu terytorialnego, a NIK negatywnie oceniła przygotowanie do zapewnienia ciągłości działania systemów informatycznych w 71% tych urzędów. Istotne nieprawidłowości ujawniono w 23 z 24 objętych kontrolą jednostek, w tym w przypadku dwóch urzędów sformułowano negatywną ocenę ogólną”[40].

Co szczególnie niepokojące – zdaniem Izby – działania jednostek samorządu terytorialnego w kontekście organizacji zasad i mechanizmów zapewnienia bezpieczeństwa informacji nie były w pełni skutecznie, należycie i prawidłowo realizowane. Jak wynika z ustaleń kontroli, w 50% skontrolowanych jednostek nie podjęto odpowiednich analiz i nie zidentyfikowano części posiadanych zbiorów danych i ich wagi pod kątem zapewnienia odpowiedniej ochrony, co NIK oceniła jako działanie nierzetelne.

Katalog najczęściej występujących nieprawidłowości w kontrolowanych podmiotach prezentuje tabela powyżej.

Z ustaleń kontrolerów wynikają szokujące wręcz ustalenia w obszarze zarządzania ciągłością działania JST. W ponad 70% badanych urzędów nie opracowano związanej z tym polityki – dokumentu

[40] Tamże, s. 8.

kluczowego z perspektywy zarządzania ryzykiem w sytuacjach kryzysowych. Brak takich polityk należy rozpatrywać łącznie z kolejną nieprawidłowością, polegającą na niewdrożeniu planów zapewnienia ciągłości działania oraz planów odtworzeniowych, co stwierdzono w połowie kontrolowanych jednostek. Warto w tym miejscu przywołać wyjaśnienia osób, o których mowa w art. 40 ustawy o Najwyższej Izbie Kontroli. Przykładowo, Starostwo Powiatowe w Sochaczewie wskazało, że plany zapewnienia ciągłości i plany odtworzeniowe nie zostały sporządzone w formie pisemnej. Nie przeprowadzono również testów. Stwierdzono, że „taki stan rzeczy jest wynikiem braku posiadania sprzętu, jaki można do takiej symulacji wykorzystać, braku urządzeń zapasowych o parametrach takich samych jak posiadane lub lepszych". W dalszej części wyjaśnień podkreślono, że „akceptowalny czas przywrócenia ciągłości działania systemów informatycznych nie został określony w sposób dokładny z powodu braku możliwości przetestowania takiej sytuacji, z uwagi na brak sprzętu zapasowego. W przybliżeniu takie działanie zajęłoby ok. 24 h w momencie posiadania identycznego lub lepszego sprzętu, jaki jest obecnie na wyposażeniu Urzędu"[41].

W połowie badanych jednostek nie dokonano pełnej identyfikacji aktywów informacyjnych wymagających ochrony lub nie przypisano im odpowiedniego poziomu zabezpieczeń. Jak ustalili kontrolerzy NIK, „pomijano na ogół informacje wymagające ochrony – inne niż dane osobowe, takie jak powierzone przez kontrahentów tajemnice przedsiębiorstwa, zasady bezpieczeństwa fizycznego i informatycznego w jednostce, informacje finansowe z deklaracji podatkowych". Wicestarosta ostrołęcki wskazał, że przyczyną nieprawidłowości były braki kadrowe i finansowe w obszarze bezpieczeństwa informacji.

Informacja o kontroli NIK ujawnia również, że wdrożone rozwiązania w zakresie bezpieczeństwa informacji nie były właściwie stosowane ani egzekwowane. W 20 jednostkach (83%) stwierdzono nieprawidłowości dotyczące m.in. zabezpieczenia serwerowni, sporządzania kopii zapasowych oraz braku w umowach na zakup usług IT zapisów gwarantujących bezpieczeństwo informacji, co naruszało przepisy rozporządzenia KRI. W skrajnych przypadkach aż 5% pracowników miało możliwość instalowania dowolnego oprogramowania na komputerach służbowych, a w jednym z urzędów wszyscy użytkownicy systemów informatycznych – niebędący pracownikami działu IT – posiadali uprawnienia administratora, w związku z czym mogli samodzielnie instalować dowolne oprogramowanie[42]. Kontrola objęła również proces blokowania lub odbierania dostępu do systemów informatycznych. Na próbie 240 osób stwierdzono, że 52 byłym pracownikom (22%) konta nie zostały zablokowane. Ponadto jedynie w trzech urzędach wdrożono rozwiązania umożliwiające monitorowanie oprogramowania na urządzeniach mobilnych,

[41] Tamże, s. 22.
[42] Tamże, s. 23-24.

co stanowi poważne ryzyko dla bezpieczeństwa danych.

Kolejne ustalenie NIK również odnosiło się do kwestii umów na zakup usług informatycznych, zakup lub serwis sprzętu komputerowego/oprogramowania. W wyniku przeprowadzonych czynności ustalono, że w 11 urzędach (46%) w umowach stwierdzono brak zapisów gwarantujących zabezpieczenie poufności informacji uzyskanych przez wykonawców w związku z ich realizacją. Na 101 zbadanych umów w 30 nie zawarto takich zapisów. Działanie to istotnie obniża poziom bezpieczeństwa jednostek samorządowych. Zabezpieczenie interesów JST na poziomie umowy na zakup usług informatycznych lub oprogramowania jest fundamentem budowania cyfrowej odporności zarówno w ujęciu jednostkowym, jak i systemowym.

Nieprawidłowości dotyczyły także tworzenia i przechowywania kopii zapasowych. W połowie kontrolowanych urzędów stwierdzono naruszenia § 19 ust. 2 pkt 12 lit. b rozporządzenia KRI, polegające m.in. na przechowywaniu kopii w serwerowniach – miejscach wytwarzania danych – co zwiększa ryzyko ich utraty w wypadku zdarzeń losowych. W kilku urzędach kopie nie były sporządzane zgodnie z procedurami, a w sześciu nie przeprowadzano testów ich skuteczności[43]. Istotnym problemem jest również brak szkoleń dla pracowników odpowiedzialnych za przetwarzanie informacji – w 10 urzędach (42%) nie zapewniono wymaganych szkoleń, co narusza § 19 ust. 2 pkt 6 rozporządzenia KRI.

Wnioski pokontrolne

W wyniku przeprowadzonych czynności kontrolnych NIK sformułowała szereg wniosków zaadresowanych do różnych podmiotów odpowiedzialnych za cyberbezpieczeństwo. Wniosek skierowany do Ministra Cyfryzacji dotyczył konieczności wspierania przez administrację rządową jednostek samorządu terytorialnego w zakresie wdrażania rozwiązań organizacyjnych i technicznych dotyczących bezpieczeństwa informacji oraz zapewnienia ciągłości działania urzędów. W stanowisku Ministra Cyfryzacji do wystąpienia pokontrolnego (*vide* art. 64 ust. 2 ustawy o Najwyższej Izbie Kontroli) wskazano, że „konsekwentnie buduje i rozwija krajowy system cyberbezpieczeństwa, aby zapewnić ochronę cyberprzestrzeni RP na właściwym poziomie", a „zapewnienie cyberbezpieczeństwa jest jednym z głównych priorytetów ministra cyfryzacji"[44]. Zwrócono również uwagę, że w 2024 r. uruchomiono program grantowy „Cyberbezpieczny Samorząd", który obejmuje wszystkie JST. Jego celem jest „zwiększenie bezpieczeństwa informacji poprzez wzmacnianie odporności jednostek samorządu terytorialnego oraz ich zdolności do skutecznego zapobiegania incydentom bezpieczeństwa teleinformatycznego, wykrywania ich i reagowania na nie"[45].

[43] Tamże, s. 11.
[44] Pismo Ministra Cyfryzacji do Prezesa Najwyższej Izby Kontroli, sygn.: BM.WN.0810.8.2025, Warszawa, 12.3.2025.
[45] Tamże.

Minister Cyfryzacji zakłada, że realizacja projektu przyczyni się do osiągnięcia wymiernych efektów m.in.:
a) wdrożenia lub aktualizacji w jednostkach samorządu terytorialnego polityk bezpieczeństwa informacji w ramach SZBI;
b) wprowadzenia w JST środków zarządzania ryzykiem w cyberbezpieczeństwie;
c) wdrożenia w samorządach mechanizmów i środków zwiększających odporność na ataki z cyberprzestrzeni;
d) podniesienia poziomu wiedzy i kompetencji personelu w jednostkach samorządu terytorialnego, kluczowego z punktu widzenia SZBI wdrożonego w urzędzie;
e) przeprowadzenia w JST audytów SZBI potwierdzających uzyskanie wyższego poziomu odporności na cyberzagrożenia.

Minister Cyfryzacji podkreślił również znaczenie podnoszenia kwalifikacji zawodowych przez pracowników szeroko pojętej administracji publicznej. Zwrócił uwagę na działania związane z opracowaniem pakietu edukacyjnego, który zawiera praktyczne wskazówki dotyczące rozpoznawania i unikania najczęstszych zagrożeń, takich jak wiadomości phishingowe, złośliwe oprogramowanie czy dezinformacja. Zebrano w nim również konkretne porady dotyczące codziennych praktyk cyberhigieny, takich jak zarządzanie hasłami, regularne aktualizacje oprogramowania czy bezpieczne korzystanie z Internetu.

Do wójtów, burmistrzów, prezydentów miast i starostów zaadresowano łącznie 12 wniosków. Dotyczyły one:
a) opracowania i wdrożenia SZBI, zgodnie z § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI;
b) zapewnienia dokonywania okresowego przeglądu i aktualizacji Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z § 19 ust. 2 pkt 1 rozporządzenia KRI;
c) ustanowienia polityk ciągłości działania oraz opracowania i wdrożenia planów zapewnienia ciągłości funkcjonowania urzędów, planów odtworzeniowych oraz ich okresowego testowania;
d) zagwarantowania pracownikom zaangażowanym w proces przetwarzania informacji odpowiednich szkoleń w tym zakresie, zgodnie z § 19 ust. 2 pkt 6 rozporządzenia KRI;
e) prowadzenia okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji zgodnie z § 19 ust. 2 pkt 3 rozporządzenia KRI;
f) wdrożenia rozwiązań zapewniających odpowiednie zabezpieczenie pomieszczeń serwerowni zgodnie z § 19 ust. 2 pkt 9 rozporządzenia KRI;
g) regularnego testowania kopii zapasowych oraz przechowywania ich poza miejscem wytworzenia;
h) zapewnienia prowadzenia przynajmniej raz w roku okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji zgodnie z § 19 ust. 2 pkt 14 rozporządzenia KRI;
i) przyznawania i odbierania pracownikom urzędów uprawnień w systemach informatycznych adekwatnie do realizowanych zadań zgodnie z § 19 ust. 2 pkt 4 rozporządzenia KRI;
j) egzekwowania wdrożonych rozwiązań organizacyjnych i technicznych w zakresie bezpieczeństwa informacji;
k) zawierania w umowach o świadczenie usług informatycznych postanowień gwarantujących odpowiedni poziom bezpieczeństwa informacji zgodnie z § 19 ust. 2 pkt 10 obowiązującego rozporządzenia KRI;

l) objęcia nadzorem oprogramowania instalowanego na urządzeniach mobilnych (telefony komórkowe służbowe/tablety).

Wnioski NIK należy ocenić jako niezbędne do zwiększenia poziomu odporności cyfrowej administracji samorządowej. Pozostaje jednak wątpliwość, czy JST dysponują odpowiednimi zasobami, aby je właściwie zaadresować. W tym kontekście należy przywołać wcześniejsze ustalenia NIK. W latach 2014[46], 2016[47] i 2017[48] Izba przeprowadziła łącznie trzy kontrole dotyczące zarządzania bezpieczeństwem informacji w urzędach administracji publicznej[49]. W wyniku kontroli z 2017 r. negatywnie oceniono wykonywanie przez blisko 70% skontrolowanych urzędów jednostek samorządu terytorialnego zadań związanych z zapewnieniem bezpieczeństwa przetwarzania informacji w okresie objętym kontrolą. Kontrolerzy stwierdzili wprost, że brakuje systemowego podejścia do zapewnienia bezpieczeństwa informacji w JST. W wyniku kontroli sformułowano szereg wniosków. Część z nich nie została wdrożona. Trudno zakładać, że w przyszłości stan ten ulegnie znaczącej poprawie.

Ustalenia Najwyższej Izby Kontroli z 2024 r., wynikające z kontroli przeprowadzonej w gminach województwa zachodniopomorskiego[50], ujawniają poważne uchybienia, które jednoznacznie podważają skuteczność i adekwatność mechanizmów zarządzania oraz nadzoru w zakresie cyberbezpieczeństwa[51]. W wystąpieniu pokontrolnym wyraźnie wskazano, że „wieloletnie zaniedbania dotyczące cyberbezpieczeństwa, nieświadomość i brak skutecznych procedur reagowania na zagrożenia, a także wykorzystywanie oprogramowania, które miało krytyczne luki – to główne nieprawidłowości wykryte w urzędach gmin w województwie zachodniopomorskim. W konsekwencji samorządy te nie były w stanie zapewnić skutecznej ochrony przed potencjalnymi atakami cyberprzestępców”[52].

Syntetyzując tę część rozważań warto wskazać, że w wyniku przeprowadzonej kontroli do kierowników jednostek kontrolowanych skierowano 24 wystąpienia pokontrolne. Łącznie NIK zidentyfikowała 222 nieprawidłowości, z których 51 zostało usuniętych już w trakcie kontroli. Izba sformułowała 171 wniosków pokontrolnych.

---

[46] Informacja o wynikach kontroli NIK: *Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu*, nr ewid. 205/2014/P/14/004/KAP, Warszawa 2015.

[47] Informacja o wynikach kontroli NIK: *System rejestrów państwowych – bezpieczeństwo, funkcjonowanie i użyteczność*, nr ewid. 208/2016/P/16/006/KAP, Warszawa 2017.

[48] Informacja o wynikach kontroli NIK: *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego*, nr ewid. 187/2018/P/18/006/KAP, Warszawa 2019.

[49] A. Chodakowska, S. Kańduła, J. Przybylska: *Jak polskie gminy radzą sobie z cyberbezpieczeństwem*, „Kontrola Państwowa” nr 1/2022, s. 135.

[50] Informacja o wynikach kontroli NIK: *Zapewnienie bezpieczeństwa teleinformatycznego przez jednostki samorządu terytorialnego województwa zachodniopomorskiego*, nr ewid. I/23/001/LSZ, Warszawa 2024.

[51] *Zachodniopomorskie gminy nieprzygotowane na cyberzagrożenia,* Najwyższa Izba Kontroli, <https://www.nik.gov.pl/aktualnosci/zachodniopomorskie-gminy-cyberzagrozenia.html> (dostęp: 30.11.2025).

[52] Tamże.

Stan ich realizacji na 16 stycznia 2025 r. prezentował się następująco: 72 wnioski zostały zrealizowane, 99 było w trakcie realizacji.

Kluczowe wnioski *de lege lata* i *de lege ferenda*

Należy według mnie zwiększyć odpowiedzialność osób zarządzających jednostkami samorządu terytorialnego za właściwą realizację zadań z zakresu cyberbezpieczeństwa przez wprowadzenie przejrzystego katalogu zadań oraz sankcji i kar za naruszenie obowiązków związanych z zapewnieniem cyberbezpieczeństwa. Wzorem dla ustawodawcy mogą być tu rozwiązania przyjęte w odniesieniu do podmiotów rynku finansowego w ramach implementacji rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA)[53]. W prawie krajowym regulacje te doprecyzowano w ustawie z 25 czerwca 2025 r. o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji[54].

Drugi wniosek ma charakter całościowy i odnosi się do kwestii organizacji systemu cyberbezpieczeństwa w jednostkach samorządu terytorialnego. Niezbędne jest moim zdaniem wprowadzenie rozwiązań centralizujących realizację zadań z zakresu cyberbezpieczeństwa. Powołanie na poziomie województw centrów reagowania na incydenty cyberbezpieczeństwa oraz odpowiedzialnych za realizację zadań związanych z rozwijaniem odporności cyfrowej wydaje się pożądanym kierunkiem. Nie ulega bowiem wątpliwości, że pozyskiwanie odpowiednich zasobów finansowych i kadrowych z perspektywy małych jednostek samorządowych jest utrudnione. Można wręcz zaryzykować stwierdzenie, że działanie takie jest niecelowe i niegospodarne. Odpowiedzialność za budowanie odporności cyfrowej podmiotów publicznych powinna być przypisana do wyspecjalizowanych podmiotów podległych ministrowi właściwemu do spraw informatyzacji. Organ ten z kolei winien dysponować odpowiednimi siłami i środkami niezbędnymi do planowania, organizowania i wdrażania adekwatnych rozwiązań obejmujących wszystkie JST.

Kolejny wniosek odnosi się do sfery standaryzacji. Zasadne wydaje się opracowanie rekomendowanych, standaryzowanych wzorców polityk, procedur i planów ciągłości działania, które mogłyby być dobrowolnie adaptowane przez JST, z zachowaniem ich konstytucyjnej samodzielności. Takie działanie znacząco ułatwi nadzór i kontrolę, a tym samym może przyczynić się do zwiększenia poziomu odporności cyfrowej administracji rządowej. Ważne w tym kontekście jest również rozwijanie i zacieśnianie współpracy z krajowymi zespołami CSIRT, w szczególności w zakresie podnoszenia kwalifikacji oraz wymiany informacji o zagrożeniach i incydentach.

---

[53] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14.12.2022, op.cit.

[54] Ustawa z 25.6.2025 o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji (Dz.U. poz. 1069).

Nowelizacja ustawy o KSC

Jak wspomniano we wstępie do artykułu, w styczniu 2026 r. uchwalono nowelizację ustawy o krajowym systemie cyberbezpieczeństwa implementującą do polskiego porządku prawnego dyrektywę NIS 2[55]. Nowelizacja zakłada szereg istotnych zmian wpływających zarówno na stronę podmiotową, jak i przedmiotową systemu. Szczegółowa analiza przyjętych rozwiązań wykracza poza ustalone założenia badawcze, jednak warto zasygnalizować najważniejsze zmiany.

Ustawa przewiduje nowe kompetencje organów odpowiedzialnych za cyberbezpieczeństwo, co ma przyczynić się do zwiększenia ich skuteczności i efektywności realizacji zadań. Organy właściwe do spraw cyberbezpieczeństwa poszczególnych sektorów (tj. ministrowie, Komisja Nadzoru Finansowego czy Prezes Urzędu Komunikacji Elektronicznej) zyskały możliwość wydawania ostrzeżeń, wyznaczania osoby monitorującej wykonywanie obowiązków przez dany podmiot kluczowy, a także nakazywania przeprowadzenia oceny bezpieczeństwa systemu informacyjnego bądź audytu bezpieczeństwa.

Zgodnie z nowymi przepisami Minister Cyfryzacji będzie mieć prawo do wydawania poleceń zabezpieczających, które mają ograniczać skutki incydentu krytycznego. Kompetencja ta ma zwiększyć sprawność działania i efektywność współpracy w reakcji na pojawiające się zagrożenia. Trzeba również odnotować, że Minister Cyfryzacji będzie odpowiadać za prowadzenie działań informacyjno-edukacyjnych w zakresie cyberbezpieczeństwa.

Zmiany obejmują również kompetencje Pełnomocnika Rządu do spraw Cyberbezpieczeństwa. Katalog uprawnień tego podmiotu został poszerzony. Pełnomocnik zyska prawo do:

- wydawania rekomendacji mających na celu wzmocnienie poziomu cyberbezpieczeństwa;
- kierowania żądań przekazania informacji od organów administracji rządowej oraz zlecania badań niezbędnych do wykonywania jego zadań;
- zakupu oprogramowania dla uczestników posiedzeń Połączonego Centrum Operacyjnego Cyberbezpieczeństwa.

Ustawa zakłada również poszerzenie katalogu kompetencji zespołów CSIRT poziomu krajowego.

Istotna z perspektywy podmiotowej krajowego systemu cyberbezpieczeństwa jest zmiana katalogu podmiotów zobowiązanych do stosowania przepisów ustawy. Uchwalony podział podmiotowy – zgodnie z dyrektywą NIS 2 – zakłada funkcjonowanie podmiotów kluczowych i ważnych oraz Połączonego Centrum Operacyjnego Cyberbezpieczeństwa. Podmioty kluczowe oraz podmioty ważne będą zobligowane do implementacji adekwatnych środków technicznych i organizacyjnych w zakresie cyberbezpieczeństwa, ukierunkowanych

[55] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14.12.2022 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 (dyrektywa NIS 2), Dz. U. UE. L. z 2022 r. nr 333, s. 80, z późn. zm.

na zapewnienie ochrony przetwarzanych danych oraz utrzymywanej infrastruktury przed zidentyfikowanymi zagrożeniami teleinformatycznymi. Dobór tych środków powinien pozostawać w proporcji do skali działalności danego podmiotu oraz specyfiki świadczonych przez niego usług. W ramach procesu dostosowawczego podmioty te będą musiały przeprowadzić kompleksową analizę posiadanych zasobów, dokonać identyfikacji potencjalnych zagrożeń cybernetycznych, zweryfikować obowiązujące procedury wewnętrzne oraz zapewnić odpowiednie szkolenia dla personelu. Nowelizacja poszerza katalog podmiotów objętych regulacją, jednak z perspektywy jednostek samorządu terytorialnego nie wprowadza istotnych zmian. Nadal będą one objęte regulacjami w zakresie cyberbezpieczeństwa.

Uchwalona ustawa wprowadza również procedurę uznania za dostawcę wysokiego ryzyka. Postępowanie w tej sprawie umożliwi eliminację niebezpiecznego sprzętu i usług z kluczowych systemów państwa. Decyzje w tym zakresie będzie podejmował Minister Cyfryzacji, przy udziale Kolegium do spraw Cyberbezpieczeństwa, w ramach transparentnego i wieloetapowego postępowania administracyjnego. Podmioty istotne dla funkcjonowania państwa nie będą mogły wprowadzać do swoich systemów produktów pochodzących od dostawcy wysokiego ryzyka. Jeżeli już z nich korzystają, zostaną zobowiązane do ich wycofania w terminie 7 lat. Dostawca, który nie zgadza się z decyzją, będzie miał możliwość wniesienia skargi do sądu administracyjnego.

W mojej ocenie nowelizacja może przynieść wymierne korzyści dla bezpieczeństwa państwa, w tym jednostek samorządu terytorialnego. Po pierwsze, zwiększa odporność infrastruktury krytycznej dzięki objęciu regulacją nowych sektorów, co ogranicza ryzyko efektu domina w łańcuchach dostaw. Po drugie, wzmacnia zdolności instytucjonalne państwa, umożliwiając szybsze wykrywanie i neutralizowanie zagrożeń dzięki rozszerzonym kompetencjom organów właściwych i sektorowych zespołów CSIRT. Po trzecie, podnosi poziom bezpieczeństwa usług cyfrowych świadczonych obywatelom i przedsiębiorstwom, wprowadzając jednolite standardy zarządzania ryzykiem oraz odpowiedzialność kierownictwa za cyberbezpieczeństwo. Procedura identyfikacji dostawców wysokiego ryzyka zwiększa wreszcie strategiczną autonomię państwa i redukuje podatność na zagrożenia wynikające z niepewnych technologii. Nowelizacja może więc wzmocnić stabilność systemów ICT, poprawić jakość usług publicznych i komercyjnych, a w konsekwencji zwiększyć zaufanie społeczne do infrastruktury cyfrowej.

Zakończenie

Przeprowadzona analiza jednoznacznie potwierdza, że JST w Polsce – mimo rosnącej roli w systemie bezpieczeństwa państwa – pozostają obecnie jego „miękkim podbrzuszem" w wymiarze cyberbezpieczeństwa. Wyniki kontroli NIK oraz przykłady udanych cyberataków wskazują na utrzymujące się systemowe braki w zarządzaniu bezpieczeństwem informacji, ciągłością działania oraz świadomością zagrożeń cyfrowych. Pomimo obowiązywania regulacji prawnych i wielu inicjatyw centralnych, praktyka funkcjonowania jednostek samorządu terytorialnego

ujawnia liczne nieprawidłowości, wynikające zarówno z niedostatku zasobów, jak i braku odpowiednich mechanizmów nadzoru oraz sankcji. Przywołane w artykule ich przykłady, związane z realizacją obowiązków w zakresie cyberbezpieczeństwa na poziomie jednostek samorządu terytorialnego, pozwalają na stwierdzenie, że mamy do czynienia z istotnym problemem w ujęciu systemowym. Ustawa o krajowym systemie cyberbezpieczeństwa obowiązuje od kilku lat, a problemy, które zdefiniowali kontrolerzy NIK mają wymiar fundamentalny.

Współczesne wyzwania, takie jak cyfryzacja usług publicznych, wzrost liczby incydentów oraz coraz bardziej zaawansowane zagrożenia, wymagają od samorządów nie tylko formalnego wdrażania przepisów, lecz przede wszystkim konsekwentnego budowania realnej odporności cyfrowej. Oznacza to konieczność inwestowania w rozwój kompetencji pracowników, wdrażania nowoczesnych narzędzi zarządzania bezpieczeństwem informacji oraz systematycznego testowania i doskonalenia procedur reagowania na incydenty. Kluczowe znaczenie ma również budowanie kultury bezpieczeństwa – zarówno wśród decydentów, jak i wszystkich pracowników administracji samorządowej.

W perspektywie strategicznej niezbędne jest podjęcie działań o charakterze systemowym – zarówno na poziomie legislacyjnym (wprowadzenie jasnych standardów, katalogu obowiązków i sankcji), jak i organizacyjnym (centralizacja wybranych funkcji, wsparcie kompetencyjne, wdrożenie dobrych praktyk oraz efektywna współpraca z administracją rządową i sektorem prywatnym). Warto również czerpać z doświadczeń innych krajów oraz sektorów, w których wdrożono skuteczne mechanizmy nadzoru i odpowiedzialności.

Poziom cyberbezpieczeństwa w jednostkach samorządu terytorialnego bezpośrednio wpływa na bezpieczeństwo obywateli, zaufanie do instytucji publicznych oraz efektywność funkcjonowania całego systemu władzy publicznej. Przekształcenie administracji samorządowej z „miękkiego podbrzusza" w rzeczywisty filar odporności cyfrowej państwa wymaga konsekwentnego wdrażania rekomendacji pokontrolnych, rozwoju kompetencji cyfrowych oraz adaptacji rozwiązań sprawdzonych w innych sektorach i krajach. Tylko wówczas samorząd terytorialny będzie mógł pełnić rolę wzorcowego modelu działania w zakresie cyberbezpieczeństwa, odpowiadając na wyzwania współczesności i przyszłości.

W tym kontekście należy odnotować kolejne inicjatywy podejmowane przez decydentów na poziomie centralnym, ukierunkowane na wzmacnianie cyberbezpieczeństwa w samorządach. W ostatnich miesiącach podjęto ważną decyzję o uruchomieniu samorządowej platformy współpracy w obszarze cyberbezpieczeństwa ISAC-JST[56]. Jest to forum wymiany wiedzy i doświadczeń na temat incydentów cyberbezpieczeństwa oraz dobrych praktyk pomiędzy należącymi do platformy samorządami, a także dzielenia się informacjami

[56] ISAC to skrót od angielskiej nazwy *Information Sharing and Analysis Centre* – centrum wymiany danych i analiz.

o cyberincydentach i sposobach ograniczania ryzyka[57]. W mojej ocenie powołanie tego forum to krok w dobrym kierunku, bowiem szybka i efektywna wymiana informacji w krajowym systemie cyberbezpieczeństwa jest fundamentalnie ważna. Kluczowe znaczenie ma w tym wymiarze przełożenie ustaleń Najwyższej Izby Kontroli na konkretne działania, prowadzące do eliminacji lub ograniczania zidentyfikowanych problemów, luk i wyzwań.

Tylko kompleksowe podejście, łączące działania prawne, organizacyjne i edukacyjne, pozwoli przekształcić JST z „miękkiego podbrzusza" w rzeczywisty filar odporności cyfrowej państwa. Wdrażanie rekomendacji pokontrolnych, adaptacja sprawdzonych rozwiązań z innych sektorów i krajów oraz budowanie kultury bezpieczeństwa to warunki konieczne do zapewnienia bezpieczeństwa obywateli i sprawności administracji publicznej w dobie transformacji cyfrowej. Pozostaje mieć nadzieję, że działania podejmowane w następstwie kontroli oraz wyzwań dla krajowego systemu cyberbezpieczeństwa będą przedmiotem zainteresowania kluczowych interesariuszy.

dr hab. **KAMIL SYLWESTER MROCZKA**
adiunkt w Katedrze Nauk o Państwie i Administracji Publicznej Wydziału Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego,
Chief Compliance Officer w Santander Bank Polska SA,
ORCID: 0000-0003-3809-3479

[57] *Samorządowa platforma cyberbezpieczeństwa zwiększy cyfrową odporność JST,* Serwis Samorządowy PAP, <https://samorzad.pap.pl/kategoria/e-urzad/samorzadowa-platforma-cyberbezpieczenstwa-zwiekszy-cyfrowa-odpornosc-jst> (dostęp 30.11.2025).

Słowa kluczowe: cyberbezpieczeństwo, cyberbezpieczeństwo w JST, krajowy system cyberbezpieczeństwa, bezpieczeństwo informacji, system zarządzania bezpieczeństwem informacji, samorządy

Bibliografia:

1. Banasiński C.: *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2023.
2. *Baza JST. Samorząd terytorialny w Polsce*, Ministerstwo Spraw Wewnętrznych i Administracji.
3. Chałubińska-Jentkiewicz K., Brzostek A.: (red.) *Modele rozwiązań prawnych w systemie cyberbezpieczeństwa RP. Rekomendacje*, Warszawa 2021.
4. Chodakowska A., Kańduła S., Przybylska J.: *Jak polskie gminy radzą sobie z cyberbezpieczeństwem*, „Kontrola Państwowa" nr 1/2022.
5. *Cyberbezpieczny samorząd. Poradnik*, Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK), Warszawa 2023.

6. Dziomdziora W.: *Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik*, Warszawa 2021.
7. *Gawkowski: miękkie podbrzusze systemu cyberbezpieczeństwa to samorząd*, Serwis Samorządowy PAP.
8. Izdebski H.: *Domniemanie zadań samorządu terytorialnego i domniemanie zadań gminy w obrębie samorządu terytorialnego – klauzule generalne dotyczące zadań samorządu*, „Samorząd Terytorialny" 2015/1–2.
9. Kitler W., Taczkowska-Olszewska J., Radoniewicz F.: (red.) *Ustawa o krajowym systemie cyberbezpieczeństwa*. Komentarz, Warszawa 2019.
10. *Samorządowa platforma cyberbezpieczeństwa zwiększy cyfrową odporność JST*, Serwis Samorządowy PAP.
11. Siudak R.: C*yberbezpieczeństwo w Polsce. Od dyskursów do polityk publicznych*, Kraków 2022.
12. Szczegielniak M.: *Dostęp do informacji w administracji publicznej a rozwój partycypacji obywatelskiej w Polsce*, Warszawa 2025.
13. Szpor G., Gryszczyńska A.: (red.) *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019.

ABSTRACT

Cybersecurity in Local Government Units – Significance of NIK's Audit Findings

The article addresses the level of cybersecurity in local government units in Poland (Polish: *jednostki samorządu terytorialnego*, JST, also: self-governments) by analysing the results of the most recent audits conducted by the Supreme Audit Office (NIK) and the applicable legal regulations. The author presents the thesis that local self-governments currently constitute the "soft underbelly" of the state security system, due to the lack of resources, insufficient awareness among decision-makers, and inadequate oversight and sanctioning mechanisms. The article outlines the legal framework of the national cybersecurity system, the key obligations of local self-government administration, and the most frequent irregularities and gaps identified by NIK. On the basis of an empirical analysis and a literature review, the author formulates *de lege lata* and *de lege ferenda* recommendations, pointing to the need for centralisation of selected functions, strengthening of individual accountability, and development of digital competences. The importance of cooperation with the Computer Security Incident Response Teams (CSIRTs) and the ISAC-JST platform is also emphasised.

Kamil Sylwester Mroczka, PhD, assistant professor, Department of State and Public Administration Sciences, Faculty of Political Sciences and International Studies, University of Warsaw, Chief Compliance Officer at Santander Bank Polska SA, ORCID: 0000-0003-3809-3479

Key words: cybersecurity, cybersecurity at local self-government units, national cybersecurity system, security of information, information security management system, local self-government units