Zeszyty Naukowe AON nr 1(102) 2016
ISSN 0867–2245

WSPARCIE KRYPTOLOGICZNE BEZPIECZEŃSTWA NARODOWEGO – ROZWIĄZANIA SYSTEMOWE W WYBRANYCH PAŃSTWACH I UWARUNKOWANIA IMPLEMENTACJI W POLSCE

płk dr Jacek ADAMSKI
Akademia Obrony Narodowej

Streszczenie

W artykule dokonano przeglądu rozwiązań systemowych w zakresie wsparcia kryptologicznego bezpieczeństwa narodowego, funkcjonujących w wybranych krajach. Wyniki skonfrontowano ze stanem obecnym w Polsce. Autor wnioskuje, że w erze postępującej cyfryzacji zdolność państwa do zapewnienia skutecznej ochrony kryptograficznej własnych procesów informacyjnych i decyzyjnych stała się niezbędnym elementem wsparcia bezpieczeństwa narodowego i zapewnienia suwerenności. Wykorzystując analizę SWOT, wskazuje uwarunkowania dla wprowadzenia rozwiązania systemowego w powyższym zakresie w Polsce.

Słowa kluczowe: bezpieczeństwo narodowe, kryptologia, kryptografia, kryptoanaliza

Abstract

The article provides a conspectus of systemic solutions in the field of cryptologic support for national security operative in selected countries. The results were confronted with the current state of affairs in Poland. The author concludes that in the era of ubiquitous digitalisation the ability of a state to provide an effective cryptographic protection of its own information flow and decision processes has become an essential element supporting the national security and sovereignty. Employing SWOT analysis he identifies conditioning for mandating a systemic solution in the abovementioned field in Poland.

Od zarania dziejów dostęp do informacji, zarówno o rzeczywistych i potencjalnych przeciwnikach, jak i sojusznikach, był kluczowy dla zrozumienia zachodzących w tych krajach procesów politycznych, militarnych, gospodarczych i społecznych. Pozwalało to uzyskać na nie wpływ, poprzez przeciwdziałanie im lub ich stymulowanie i ukierunkowywanie dla uzyskania własnych korzyści. Jednocześnie ochrona takich informacji o własnym kraju uniemożliwiała państwom obcym uzyskiwanie wiedzy i przewagi w wymienionych obszarach oraz obniżała skuteczność ich działań. Z tego względu już w czasach antycznych stosowano systemy szyfrowania informacji, których zadaniem była ochrona jej treści, nawet w przypadku przechwycenia przez podmiot nieupoważniony (kryptografia). Jednocześnie państwa rozwijały zdolności do łamania szyfrów stosowanych przez inne kraje (kryptoanaliza).

Szybki postęp w obszarze technologii przetwarzania informacji, wynikający z rewolucji technicznej na polu informatyzacji spowodował, że od przełomu wieków XX i XXI na świecie (szczególnie w państwach wysoko uprzemysłowionych) można zaobserwować gwałtownie rosnącą tendencję do cyfryzacji wszystkich sfer funkcjonowania państwa. Powoduje to, poza skutkami pozytywnymi[1], trwałe i stale postępujące uzależnienie instytucji państwa od sprawnego funkcjonowania systemów przetwarzania informacji[2]. Rodzi również nowe wyzwania dla bezpieczeństwa narodowego, wynikające z możliwości uzyskania nieautoryzo-

[1] M.in. zwiększenie szybkości i wydajności przetwarzania danych i informacji, możliwości ich szybkiej wymiany, współdzielenia oraz katalogowania wg dowolnych kryteriów.

[2] Kluczowymi czynnikami w tym zakresie są technologiczna zdolność systemu informacyjnego do przetwarzania danych i informacji zgodnie z wymaganiami oraz sprawność techniczna systemów teleinformatycznych, stosowanych do utrzymania systemu informacyjnego.

wanego dostępu do przetwarzanych w powyższych systemach danych i informacji – zarówno niejawnych, jak i wrażliwych[3]. Wyzwaniem jest również skryta realizacja w państwie procesów wymiany informacji w ramach procesów analityczno-informacyjnych i decyzyjnych (np. w ramach przygotowywania stanowiska negocjacyjnego lub wypracowywania decyzji), a także niejawna koordynacja procesów wykonawczych (np. podczas prowadzenia negocjacji polityczno-wojskowych lub działań bojowych). Jest to szczególnie istotne w obliczu prowadzenia przez szereg państw (w tym sojuszniczych) szeroko zakrojonych programów inwigilacji elektronicznych systemów łączności[4]. Równie niebezpieczna jest inwigilacja instytucji państwowych prowadzona przez wielkie międzynarodowe korporacje, a także działania wyspecjalizowanych grup przestępczych, pozyskujących informacje w celu udostępnienia ich zainteresowanym w zamian za korzyści finansowe. Należy brać również pod uwagę możliwe negatywne dla bezpieczeństwa narodowego skutki działań organizacji pozarządowych i antysystemowych[5]. Osobne zagrożenie stwarzają grupy terrorystyczne, które koncentrują się nie tylko na walce informacyjnej, ale również aktywnie prowadzą rozpoznanie operacyjne w Internecie[6].

Kwestia kryptograficznego zabezpieczenia zasobu informacyjnego dotyczy szczególnie obszaru obronności, gdzie sukces prowadzonych działań jest w dużym stopniu uzależniony od skutecznego ich utajnienia, w pełnym zakresie ośrodków decyzyjnych i struktur funkcjonalno-organizacyjnych państwa oraz sił zbrojnych. Ponadto, wskutek postępujących utechnicznienia i cyfryzacji wojsk oraz robotyzacji i autonomiczności środków bojowych, niezbędna stała się ochrona kryptograficzna nie tylko środków łączności oraz systemów identyfikacji bojowej (systemów „swój – obcy"), ale także informacji przetwarzanych w poszczególnych typach sprzętu wojskowego[7]. Nieposiadanie przez państwo organicznych możliwości kryptograficznej ochrony systemów kierowania i dowodzenia oraz posiadanego uzbrojenia stwarza niebezpieczeństwo ich obezwładnienia bez konieczności prowadzenia tradycyjnych działań bojowych. Rozwiązaniem nie może być pozyskanie kryptograficznych rozwiązań zagranicznych, ponieważ takie działanie powoduje faktyczne uzależnienie sprawnego funkcjonowania systemu kierowania i dowodzenia siłami zbrojnymi oraz taktycznych systemów dowodzenia od techniki zagranicznej oraz nie gwarantuje pełnej niezależności w korzystaniu z pozyskanego zaawansowanego sprzętu wojskowego obcej produkcji[8].

Przedstawione powyżej wyzwania i zagrożenia powodują, że współcześnie zapewnienie bezpieczeństwa zasobów informacyjnych państwa, z których korzystają i które współdzielą jego podmioty analityczne, decyzyjne i wykonawcze, funkcjonujące we wszystkich sferach jego funkcjonowania, nie może być już postrzegane jedynie przez pryzmat działań *stricte* technicznych. Wymaga natomiast implementacji rozwiązania systemowego na poziomie państwa, umożliwiającego prowadzenie konsekwentnej polityki skonsolidowanie potencjału umożliwiającego uzyskanie i rozbudowę własnych, narodowych zdolności nie tylko w zakresie ochrony systemów teleinformatycznych, ale również – dla zwiększenia poziomu ochrony informacji – kryptologii. Z powyższych powodów obecnie władze większości państw wy-

[3] Problem ten od strony teoretycznej przedstawiono w: L. Ciborowski *Walka informacyjna*, wyd. Europejskie Centrum Edukacyjne, Toruń 1999, s. 112–114.

[4] Programy takie realizują m.in. USA, Wielka Brytania, Niemcy, Francja, Rosja i Chiny, ale również Izrael, Japonia, Turcja, Iran i KRLD. W zależności od posiadanych możliwości technologicznych i technicznych w zakresie informatyki i kryptologii oraz potrzeb państwa, mają one zasięg globalny, regionalny lub są skierowane przeciwko określonemu krajowi. Celem ich realizacji jest zdobywanie pożądanych informacji, mających zapewnić lepszą pozycję negocjacyjną, militarną, ekonomiczną, pozyskanie wiedzy (*know-how*) i in.

[5] Działania takich organizacji jak WikiLeaks, Anonymous czy polskiej Fundacji Panoptykon, publikujących oficjalne dokumenty państwowe, mogą doprowadzić nie tylko do strat wizerunkowych, ale również znacząco zaszkodzić procesom politycznym, militarnym, gospodarczym i społecznym (np. negocjacjom, działaniom sojuszniczym i koalicyjnym, przedsięwzięciom instytucji egzekwowania prawa i in.).

[6] Na ten temat zob. J. Adamski, *Nowe technologie w służbie terrorystów*, Wydawnictwo Trio, Warszawa 2007, s. 91–117, 145.

[7] Np. na pokładzie współczesnego środka walki (np. samolotu bojowego, bojowego wozu piechoty, czołgu lub okrętu) znajduje się co najmniej kilkadziesiąt niezależnych komputerów, nadzorujących działanie poszczególnych podzespołów funkcjonalnych. Dane wymieniane między nimi muszą być chronione kryptograficznie (szyfrowane), ponieważ ich zablokowanie, przechwycenie lub modyfikacja może doprowadzić do zmiany własności funkcjonalnych, unieszkodliwienia lub zniszczenia systemów uzbrojenia, łączności, sterowania i in., a w konsekwencji – wyłączenia sprzętu wojskowego z walki.

[8] Istnieje ryzyko pozostawienia w zagranicznych rozwiązaniach luk umożliwiających ich penetrację, co może ograniczyć suwerenność użycia pozyskanego uzbrojenia zagranicznego.

soko uprzemysłowionych postrzegają kryptologię narodową jako jeden kluczowych i niezbędnych elementów wzmacniających bezpieczeństwo państwa, a także wdrożyły i rozwijają narodową politykę kryptologiczną, przeznaczając na ich realizację znaczące środki finansowe[9].

W Polsce literatura przedmiotu, mimo że dość obszerna, koncentruje się na ochronie systemów teleinformatycznych państwa (szczególnie w kontekście reagowania kryzysowego), pomijając z reguły problematykę znaczenia kryptologii (zarówno kryptografii, jak i kryptoanalizy) jako integralnego elementu osłony strategicznej państwa[10]. Celem niniejszego artykułu jest próba wypełnienia powyższej luki w wiedzy. W niniejszej publikacji dokonano przeglądu rozwiązań systemowych w zakresie wsparcia kryptologicznego bezpieczeństwa narodowego w wybranych krajach oraz skonfrontowano je z sytuacją w Polsce. Autor stawia tezę, że w XXI w., w obliczu powszechnego zagrożenia inwigilacją radio-optoelektroniczną oraz wyzwaniami będącymi pochodną postępującej globalnej cyfryzacji, posiadanie i rozwijanie przez państwo własnych zdolności do kryptograficznej ochrony procesów informacyjnych i decyzyjnych stało się niezbędnym atrybutem suwerenności i wsparcia bezpieczeństwa narodowego. Ponadto, wykorzystując metodę analizy SWOT, wskazuje uwarunkowania dla wdrożenia w Polsce strategicznego rozwiązania systemowego w powyższym zakresie na poziomie strategicznym.

Przegląd rozwiązań systemowych w wybranych państwach

Do lat 70. XX w. na świecie dominowało tradycyjne podejście do problematyki kryptologii narodowej, jako obszaru zarezerwowanego dla elitarnego, funkcjonującego na rzecz państwa zespołu matematyków i informatyków, opracowujących oraz implementujących nowe szyfry, a także zajmujących się łamaniem szyfrów obcych. Wskutek radykalnego wzrostu możliwości ośrodków komputerowych obliczeń masowych oraz upowszechnienia rozwiązań technicznych pozwalających na zwiększenie mocy obliczeniowej pojedynczych komputerów, przedstawione powyżej postrzeganie kryptologii stało się nieadekwatne do rzeczywistości, ponieważ uniemożliwia utrzymanie akceptowalnego poziomu bezpieczeństwa narodowej kryptografii[11] oraz uzyskanie sukcesów na polu kryptoanalizy. Stąd władze wielu krajów dostrzegły konieczność systemowego uregulowania problematyki kryptologii na poziomie strategicznym, w celu kumulowania zasobów państwa w tym obszarze (w sferach militarnej i niemilitarnej, a także prywatnej). Takie podejście umożliwia uzyskanie efektu synergii przedsięwzięć dostarczających środki do realizacji mechanizmów zabezpieczania informacji narodowych.

Wspólnymi elementami tych działań są:

– prowadzenie usankcjonowanej prawnie, narodowej polityki w zakresie kryptologii;

– wykorzystywanie na potrzeby państwa narodowych rozwiązań kryptograficznych lub rozwiązań zagranicznych samodzielnie dostosowanych do własnych wymagań i potrzeb;

– utrzymywanie potencjału do samodzielnego zapewnienia kryptologicznej interoperacyjności w sojuszach polityczno-wojskowych oraz na potrzeby działań koalicyjnych;

– dysponowanie państwowym ośrodkiem kompetencji kryptologicznych, posiadającym własne zdolności kryptoanalityczne.

Narodowa polityka kryptologiczna. Większość państw posiadających własny potencjał w obszarze kryptologii prowadzi jednolitą politykę w tym za-

[9] Przykładowo Francja, inwestując w rozwój narodowej kryptologii, przeznaczyła w latach 2001–2013 na ten cel ok. 400 mln EUR. Efektem konsekwentnie prowadzonych działań było uruchomienie w 2013 r. w Paryżu centralnego, narodowego ośrodka kryptologicznego, w którym zatrudniono ok. 150 specjalistów. Budżet instytucji wynosi ok. 3,5 mln EUR rocznie. Więcej o strategicznym znaczeniu centrum dla bezpieczeństwa narodowego Francji w: P. Merchet, *Ce que l'on sait du Pôle national de cryptanalyse et de décryptement*; http://www.lopinion.fr/blog/secret-defense/que-l-on-sait-pole-national-cryptanalyse-decryptement-actualise-2-23488 (dostęp 10.02.2016)

[10] „Osłona strategiczna odnosi się do przedsięwzięć militarnych oraz niemilitarnych i obejmuje działania realizowane stale w czasie pokoju i kryzysu dla ochrony przed zaskoczeniem i innymi formami przemocy". R. Jakubczak, J. Marczak, K. Gąsiorek, *Założenia polityki i strategii bezpieczeństwa narodowego* [w:] *Podstawy bezpieczeństwa narodowego Polski w erze globalizacji*, wyd. Akademia Obrony Narodowej, Warszawa 2008, s. 130

[11] Decydują o tym zdolności do zapewnienia: poufności (siła zastosowanego algorytmu kryptograficznego), anonimowości (ukrycie nadawcy i adresata w przesyłanej wiadomości), integralności (niezmienność podczas procesu przekazywania do odbiorcy), uwierzytelniania (potwierdzenia przez nadawcę) oraz niezaprzeczalności (jednoznacznego wskazania nadawcy).

kresie. Pryncypia polityki kryptologicznej powyższych państw są zwykle ujęte w formie oddzielnych rozdziałów w aktach prawnych dotyczących zasad zapewniania bezpieczeństwa informacji (*information security*) lub określających zadania służb specjalnych.

Ich wspólnymi cechami są:

– wskazanie podmiotów decyzyjnych (odpowiedzialnych) oraz wykonawczych w zakresie narodowej polityki kryptologicznej (w tym organów nadzorujących, certyfikujących i autoryzujących);

– jednoznaczne określenie wymagań dla produktów kryptograficznych na potrzeby instytucji państwa, jak również innych obszarów jego funkcjonowania, a także zasad ich pozyskiwania, certyfikacji i autoryzacji;

– nadanie priorytetu stosowaniu narodowych rozwiązań kryptograficznych, a także określenie reguł użycia produktów zagranicznych, przy zachowaniu praw skarbu państwa do własności intelektualnej[12];

– ukierunkowywanie prac naukowych i badawczo-rozwojowych państwowych i prywatnych (ale narodowych) ośrodków akademickich;

– wspieranie narodowego przemysłu kryptograficznego poprzez określanie długoterminowych potrzeb państwa w tym zakresie, finansowanie opracowania nowych rozwiązań technicznych oraz promowanie opracowanych rozwiązań narodowych na rynkach zagranicznych;

– zapewnienie interoperacyjności narodowej kryptografii w wymiarze sojuszniczym i koalicyjnym.

Instytucje odpowiedzialne. Większość państw posiadających potencjał w obszarze kryptologii prowadzi jednolitą politykę w tym zakresie, zwykle formułowaną i nadzorowaną przez tę samą instytucję – centralny urząd państwowy (patrz tabela 1), podległy prezydentowi, premierowi lub ministrowi właściwemu do spraw obrony albo spraw zagranicznych. Istotnym jest, by zauważyć, że w przypadku przekazania tego obszaru do służb specjalnych, za politykę kryptologiczną odpowiada albo służba wyspecjalizowana, albo jej autonomiczna jednostka organizacyjna, składająca raporty najwyższym władzom państwowym. Poddanie problematyki wsparcia kryptologicznego nadzorowi najważniejszych czynników decyzyjnych w państwie wskazuje na świadomość władz wielu krajów jej wagi dla bezpieczeństwa państwa.

Tabela 1

Instytucje wybranych państw odpowiedzialne za formułowanie i nadzorowanie realizacji narodowej polityki kryptologicznej[13]

Państwo	Instytucja	Typ
Brazylia	Narodowa Rada ds. Bezpieczeństwa Informatycznego i Kryptograficznego (RENASIC[1])	Urząd państwowy
Chiny	Centralna Grupa Sterująca ds. Bezpieczeństwa Internetu i Informatyzacji[2]	Kolegialne, polityczno-techniczne ciało decyzyjne
Czechy	Narodowa Władza Bezpieczeństwa (NBU)	Urząd państwowy
Dania	Centrum Bezpieczeństwa w Cyberprzestrzeni (CFCS)[3]	Jednostka organizacyjna służby specjalnej
Francja	Narodowa Agencja Bezpieczeństwa Systemów Informacyjnych (ANSSI)	Urząd państwowy
Holandia	Narodowa Agencja Bezpieczeństwa Łączności (NBV)[4]	Jednostka organizacyjna służby specjalnej
Niemcy	Federalny Urząd Bezpieczeństwa Informacji (BSI)	Służba specjalna
Norwegia	Narodowa Agencja Bezpieczeństwa (NSM)	Służba specjalna
Rosja	Państwowy Komitet Federacji Rosyjskiej ds. Standaryzacji, Metrologii i Certyfikacji (GOSSTANDART)/ Federalna Służba Bezpieczeństwa (FSB)	Urząd państwowy/służba specjalna
Rumunia	Narodowy Urząd ds. Informacji Niejawnych (ORNISS)	Urząd państwowy
Szwecja	Narodowa Organizacja Obrony Radiowej (FRA)	Służba specjalna
Turcja	Turecka Rada ds. Badań Naukowych i Technologicznych (TUBITAK)	Urząd państwowy
USA	Agencja Bezpieczeństwa Narodowego (NSA)	Służba specjalna
Wielka Brytania	Rada Bezpieczeństwa Narodowego (NSC)[5]/Grupa Bezpieczeństwa Łączności i Elektroniki (CESG)[6]	Kolegialne, polityczne ciało decyzyjne/jednostka organizacyjna służby specjalnej
Polska	nie ma	----------

[1] RENASIC (*Rede Nacional de Segurança da Informação e Criptografia*) podlega Gabinetowi Bezpieczeństwa

[12] W szczególności chodzi o posiadanie pełnej dokumentacji technicznej wraz z prawami do serwisowania, modyfikowania i rekonfigurowania produktów, a także możliwość użycia ich w innych rozwiązaniach.

[13] Opracowanie własne na podstawie informacji dostępnych w Internecie.

Instytucjonalnego (GSI) w Biurze Prezydenta Federacyjne Republiki Brazylii.

[2] Znana jako *Central Leading Group for Internet Security and Informatization* lub *Cyberspace Affairs Leading Group.* Na jej czele stoi przewodniczący Chińskiej Republiki Ludowej.

[3] Autonomiczna struktura organizacyjna, podległa Duńskiej Służbie Wywiadu Obronnego (DDIS), podporządkowanej ministrowi obrony.

[4] Autonomiczna struktura organizacyjna, podległa Naczelnej Służbie Wywiadu i Bezpieczeństwa (AIVD), podporządkowanej ministrowi spraw wewnętrznych.

[5] Jej przewodniczącym jest premier Wielkiej Brytanii.

[6] Autonomiczna struktura organizacyjna, formalnie podległa Centrali Łączności Rządowej (GCHQ).

Zasady pozyskiwania rozwiązań zagranicznych. Większość analizowanych państw umożliwia stosowanie zagranicznych rozwiązań kryptograficznych, jednak wykorzystanie ich w instytucjach państwowych oraz obiektach informatycznej infrastruktury krytycznej państwa (*critical information infrastructure*)[14] obwarowuje szeregiem zastrzeżeń. W przypadku rozwiązań kryptograficznych na potrzeby obronności i sił zbrojnych, zwykle wymagane jest przekazanie przez producenta praw do serwisu i modyfikacji pozyskiwanej techniki.

Współpraca z ośrodkami naukowymi i przemysłem kryptograficznym. Konsekwentna realizacja narodowej polityki kryptologicznej w analizowanych państwach wymaga stworzenia mechanizmów współpracy z narodowymi ośrodkami naukowo-badawczymi oraz przedsiębiorstwami. Polegają one na przedstawieniu sferom nauki i przemysłu długookresowych wizji rozwoju narodowej kryptografii oraz potrzeb państwa w tym zakresie. Umożliwia to ośrodkom badawczym oraz przedsiębiorstwom kryptograficznym perspektywiczne planowanie i ukierunkowywanie własnej działalności, co znacząco wpływa na stabilność ich funkcjonowania. Procesy te są przez państwo (instytucję odpowiedzialną) dodatkowo stymulowane poprzez rozpisywanie konkursów państwowych oraz przyznawanie grantów na przeprowadzenie badań teoretycznych w obszarze kryptografii lub kryptoanalizy, a także opracowanie propozycji nowych produktów kryptograficznych, spełniających określone przez państwo wymagania[15].

Interoperacyjność kryptologiczna. Dzięki posiadaniu własnych zdolności w zakresie narodowej kryptologii szereg państw jest zdolna do samodzielnego wytwarzania rozwiązań kryptograficznych, umożliwiających sprawne funkcjonowanie jego podmiotów i środków w środowisku międzynarodowym, podczas różnorodnych działań (przede wszystkim militarnych), podejmowanych w ramach inicjatyw sojuszniczych lub koalicyjnych. Ponadto, szereg państw oferuje własne produkty, przystosowane do wypełniania powyższych zadań (patrz tabela 2). Podnosi to prestiż tych państw na arenie międzynarodowej oraz wzmacnia ich pozycję negocjacyjną w organizacjach sojuszniczych. Praktyka pokazuje, że tylko państwa posiadające własne zdolności w zakresie kryptografii oraz obecne na rynku kryptograficznym NATO i UE formułują kierunki rozwoju i mają decydujący wpływ na decyzje tych organizacji, podejmowane w powyższym zakresie.

Tabela 2

Liczba produktów narodowych certyfikowanych do stosowania w NATO i UE (wg stanu w maju 2016 r.)[16]

NATO		UE	
Państwo	**Liczba produktów**	**Państwo**	**Liczba produktów**
USA	81	Niemcy	18
Niemcy	40	Francja	11
Wlk. Brytania	34	Szwecja	9
Francja	23	Wlk. Brytania	8
Włochy	13	Holandia	4
Holandia	9	Włochy	2
Hiszpania	4	Polska	0
Turcja	4		
Polska	0		

Narodowy ośrodek kompetencji kryptologicznych. Każde z analizowanych państw dąży do posiadania państwowego ośrodka kryptologicznego,

[14] Termin niestosowany w Polsce, używany dla wskazania systemów teleinformatycznych kluczowych dla funkcjonowania państwa; *Założenia Strategii Cyberbezpieczeństwa dla Rzeczypospolitej Polskiej*; Zespół zadaniowy ministerstwa cyfryzacji, luty 2016, s.32; mc.gov.pl/files/zalozenia_strategii_ cyberbezpieczenstwa_v_final_z_dnia_22-02-2016.pdf (dostęp: 15 maja 2016 r.).

[15] Zwykle wymaga się zakończenia prac na wysokim poziomie gotowości technologii, tj. co najmniej na etapie demonstratora.

[16] Opracowanie własne na podstawie *NATO Information Assurance Product Catalogue (NIAPC)*; www.ia.nato.int/niapc (dostęp: 30 maja 2016 r.) oraz danych Sekretariatu Generalnego UE (*General Secretariat UE*); www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/information-assurance/ (dostęp: 30 maja 2016 r.).

w którym zatrudnieni są najwyższej klasy specjaliści. Zwykle jest on częścią lub podlega instytucji odpowiedzialnej za formułowanie i nadzorowanie realizacji narodowej polityki kryptologicznej. Jego zadaniem jest opracowywanie kluczowych z punktu widzenia państwa, modelowych rozwiązań kryptograficznych, często we współpracy z narodowymi ośrodkami akademickimi i przemysłem. Ponadto wypracowuje on standardy techniczne kryptografii obowiązujące w państwie oraz aktualizuje je na podstawie analizy rozwiązań w tym zakresie, funkcjonujących w państwach obcych. Narodowy ośrodek kryptologii zwykle posiada centrum kryptoanalizy. Funkcjonuje ono zarówno w wymiarze narodowym, działając na rzecz uzyskania przez państwo przewagi informacyjnej, jak i międzynarodowym – poprzez współpracę i wymianę osiągnięć z wybranymi sojusznikami. Należy zaznaczyć, że taka forma współpracy jest świadectwem najwyższego zaufania między państwami i jest realizowana zwykle w ramach wspólnych programów inwigilacji elektronicznej[17].

Stan obecny w Polsce

Narodowa polityka kryptologiczna. W okresie od zakończenia II wojny światowej do 1989 r. polska kryptologia, podobnie jak wiele innych dziedzin, była całkowicie podporządkowana dyktatowi b. ZSRR. W kraju stosowano głównie radzieckie rozwiązania kryptograficzne[18]. Po 1989 r. sytuacja związana z wykorzystaniem zagranicznych produktów kryptograficznych dla potrzeb państwa (zarówno w sferze cywilnej, jak i wojskowej) nie uległa znaczącej poprawie. Państwo nadal nie artykułowało swoich potrzeb kryptologicznych. Problematyka kryptografii i kryptoanalizy (bez bezpośredniego użycia słowa kryptologia) została rozproszona w szeregu aktów prawnych i dokumentów oficjalnych[19], nadając plenipotencje w tym zakresie służbom specjalnym, przede wszystkim Agencji Bezpieczeństwa Wewnętrznego (ABW) i Służbie Kontrwywiadu Wojskowego (SKW). W wielu przypadkach uprawnienia te zostały określone wyjątkowo nieprecyzyjnie, co stwarza możliwość dowolnej interpretacji[20]. Ponadto, w przywołanych przepisach skupiono się na kwestiach technicznych, zaniedbując rozwiązanie systemowe w skali państwa. W rezultacie ABW i SKW ograniczyły swoją aktywność do działań organizacyjno-formalnych, tj. przeprowadzania postepowań certyfikacyjnych i akredytacyjnych. Nie sformułowały natomiast, bo nie zostały do tego prawnie zobowiązane, propozycji strategicznej koncepcji wsparcia kryptologicznego dla bezpieczeństwa państwa. Skutkiem tego jest szerokie stosowanie zagranicznych produktów kryptograficznych, zarówno w sektorach cywilnych, jak i w Siłach Zbrojnych RP.

Dopiero w połowie drugiej dekady XXI w. władze polskie zwróciły uwagę na znaczenie wsparcia kryptologicznego dla bezpieczeństwa narodowego. Świadectwem tego są zapisy *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* z 2014 r., w której po raz pierwszy zwrócono uwagę na rolę kryptologii w bezpieczeństwie narodowym:

– „istotne jest też rozwijanie narodowych zdolności w zakresie kryptologii i nabycie pełnych zdolności w dziedzinie wytwarzania narodowych rozwiązań kryptograficznych”[21];

[17] Więcej na ten temat w: L. Harding, *Polowanie na Snowdena*, wyd. Wielka Litera, Warszawa 2014, s. 165–180 i 282 oraz G. Greenwald, *Snowden. Nigdzie się nie ukryjesz*, wyd. Agora, Warszawa 2014, s.149–153 i 156–157.

[18] Chlubnym wyjątkiem jest tu rodzina polskich szyfratorów dalekopisowych *DUDEK*, zob.: *DUDEK – polskie urządzenie szyfrujące z lat 60-tych* [w:] http://www.zawszeczujni.pl/2015/12/dudek-polskie-urzadzenie-szyfrujace-z.html (dostęp 27.05.2016 r.)

[19] Są to: Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. 2010.29.154 z późn. zm.), Ustawa z dnia 9 marca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U. Nr 104, poz. 709 z późn. zm.), Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. Nr 182, poz. 1228), Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U.2013.262), Ustawa z dnia 25 maja 2012 r. o zmianie ustawy o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa oraz niektórych innych ustaw (Dz.U. 2012.70), Rozporządzenie Ministra Gospodarki z dnia 30 kwietnia 2013 r. w sprawie wykazu uzbrojenia, na obrót którym jest wymagane zezwolenie (Dz.U.2013.541), Rozporządzenie Prezesa Rady Ministrów z dnia 16 września 2010 r. w sprawie szczegółowych zasad wykonywania działalności telekomunikacyjnej w Sieci Łączności Rządowej (Dz.U. 2010.177.1192), Zarządzenie Nr 10/MON Ministra Obrony Narodowej z dnia 29 kwietnia 2013 r. w sprawie utworzenia i nadania statutu państwowej jednostce budżetowej – Narodowe Centrum Kryptologii (Dz. U. MON z dnia 29 kwietnia 2013 r.).

[20] Przykładem może być zapis art. 5. pkt 5 Ustawy z dnia 9 marca 2006 r.: *Do zadań SKW należy m.in. prowadzenie* […] *przedsięwzięć z zakresu ochrony kryptograficznej i kryptoanalizy*.

[21] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, pkt 117.

– „podstawowe znaczenie dla ochrony systemów teleinformatycznych ma rozwój i implementacja narodowych rozwiązań z zakresu kryptografii”[22].

Powyższe stanowisko zostało rozwinięte w opublikowanej rok później Doktrynie Cyberbezpieczeństwa RP, w której stwierdzono m.in. że:

– „do głównych zadań sektora publicznego […] należą […] działania w dziedzinie kryptografii i kryptoanalizy”[23];

– konieczne jest „przyjęcie nowych rozwiązań prawnych […] dla zapewnienia strukturalnego wsparcia i finansowania prac badawczo-rozwojowych w zakresie tworzenia nowych, narodowych rozwiązań w dziedzinie teleinformatyki i kryptologii”[24].

Jednak zapisy powyższych dokumentów strategicznych nie zostały przełożone na akty wykonawcze. Natomiast, w wyniku nowelizacji Ustawy o działach administracji rządowej w 2016 r., organem odpowiedzialnym za cyberbezpieczeństwo RP stał się minister właściwy do spraw cyfryzacji. Ministerstwo Cyfryzacji w przyjętej koncepcji działania skupiło się na budowie krajowego systemu reagowania na incydenty komputerowe, czyli ochronie systemów teleinformatycznych, całkowicie pomijając kwestie kryptologii[25].

Instytucje odpowiedzialne. W Polsce nie ma instytucji formułującej i koordynującej narodową politykę kryptologiczną. W ograniczonym zakresie rolę tę spełniają ABW i SKW, które jednak skupiają się na aspektach technicznych (certyfikacja urządzeń kryptograficznych i akredytacja systemów teleinformatycznych je wykorzystujących) i nie prezentują woli oraz zrozumienia dla potrzeby wprowadzenia systemowego rozwiązania na poziomie strategicznym[26]. Instytucją odpowiedzialną za ten obszar w państwie mogło stać się funkcjonujące w resorcie obrony narodowej Narodowe Centrum Kryptologii (NCK), które w latach 2013–2014 podjęło szereg działań o charakterze systemowym, w zakresie posiadanych kompetencji statutowych. Jednak obecnie nie posiada ono potencjału do wypełniania tego zadania, z powodów opisanych poniżej.

Zasady pozyskiwania rozwiązań zagranicznych. Zgodnie z zapisami Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, ABW i SKW są instytucjami właściwymi dla certyfikacji urządzeń i narzędzi kryptograficznych oraz określają zasady jej przeprowadzenia, jednak ta sama ustawa umożliwia szefom tych służb dopuszczenie zagranicznych rozwiązań kryptograficznych w systemach teleinformatycznych do klauzuli ZASTRZEŻONE, bez przeprowadzania powyższych procedur w kraju, a jedynie na podstawie certyfikatu uzyskanego w jednym z państw NATO i UE. Rozwiązanie takie jest potencjalnie szkodliwe dla bezpieczeństwa informacji, systemów teleinformatycznych, a w konsekwencji – dla bezpieczeństwa narodowego[27]. W przypadku pozyskiwania rozwiązań kryptograficznych na potrzeby obronności i Sił Zbrojnych RP, Polska zwykle nie zabiega o uzyskanie praw do serwisu i modyfikacji pozyskiwanych produktów. Tym samym Siły Zbrojne RP posiadają przeważnie prawo wyłącznie do eksploatacji zakupionej techniki, a w nielicznych przypadkach – do jej wstępnego diagnozowania.

Współpraca z ośrodkami naukowymi i przemysłem kryptograficznym. Państwo polskie nie stymuluje aktywności krajowych ośrodków akademickich[28] i firm kryptograficznych[29]. Nie wskazuje pożądanych kierunków rozwoju nauki i badań oraz wdrożeń w tym obszarze. Nie wspiera również narodowego przemysłu zamówieniami państwowymi. Skutkuje to rozproszeniem wysiłków naukowo-badawczych i niechęcią przedsiębiorstw do opracowywania innowacyjnych rozwiązań, na które potem może nie być zapotrzebowania. W rezultacie powiększa się w Polsce luka w obszarze

[22] Tamże, pkt. 131.

[23] *Doktrynie Cyberbezpieczeństwa Rzeczypospolitej Polskiej*, pkt 29.

[24] Tamże, pkt 35.

[25] Resort ten postrzega Narodowe Centrum Kryptologii jedynie jako element systemu reagowania na incydenty komputerowe resortu obrony narodowej; *Założenia Strategii Cyberbezpieczeństwa…*, s. 5, 23.

[26] Systemowe uregulowanie tej problematyki mogłoby znacząco ograniczyć istniejącą obecnie swobodę działania służb specjalnych w tym zakresie.

[27] Niezależnie od wprowadzenia losowego i personalnego pierwiastka uznaniowości, faworyzuje zagranicznych producentów, którzy nie muszą ponosić kosztów długotrwałych badań certyfikacyjnych w Polsce, do czego zobowiązani są producenci krajowi. Ponadto, produkt zagraniczny mógł być certyfikowany dawno temu, wskutek czego jest obecnie przestarzały.

[28] Wiodącymi narodowymi ośrodkami naukowo-badawczymi w zakresie kryptologii w Polsce są: Wojskowa Akademia Techniczna, Politechnika Warszawska, Politechnika Wrocławska, Politechnika Gdańska, Uniwersytet Warszawski, Instytut Matematyki PAN oraz Instytut Podstaw Informatyki PAN.

[29] Głównymi narodowymi producentami kryptografii w Polsce są: Enigma SOI, Krypton Polska, PIT-RADWAR, Transbit i Wojskowy Instytut Łączności.

kryptologii między wiedzą teoretyczną, która pozostaje na poziomie światowym, a dokonaniami konstrukcyjnymi. Podsumowując, Polska nie wykorzystuje posiadanego potencjału kryptologicznego na rzecz bezpieczeństwa narodowego.

Interoperacyjność kryptologiczna. Pomimo udziału polskich firm w programach NATO[30], ukierunkowanych na opracowanie rozwiązań kryptograficznych dla nowych standardów łączności sojuszu (*SCIP* i *NINE*)[31], w resorcie obrony narodowej dominuje praktyka pozyskiwania zagranicznych urządzeń kryptograficznych, zapewniających interoperacyjność w operacjach sojuszniczych. Państwo nie dąży do uzyskania samodzielnych zdolności w powyższym zakresie (patrz tabela 2), a tym samym – do dołączenia do elitarnego grona zaawansowanych technologicznie członków NATO oraz UE. W konsekwencji Polska zaprzepaszcza szansę na wzmocnienie roli odgrywanej w tych organizacjach, która w coraz większym stopniu zależy od realnych możliwości technologicznych i technicznych państwa, możliwych do wykorzystania przez ich członków dla zwiększenia sojuszniczych zdolności obronnych[32].

Narodowy ośrodek kompetencji kryptologicznych. W 2013 r. w resorcie obrony narodowej utworzono nową jednostkę wojskową – Narodowe Centrum Kryptologii (NCK), podległą bezpośrednio szefowi resortu. Jej misją miało być konsolidowanie państwowych kompetencji w zakresie kryptografii i kryptoanalizy oraz opracowywanie narodowych rozwiązań kryptograficznych (w szczególności narodowego algorytmu szyfrującego i szyfratora narodowego), we współpracy z polskimi ośrodkami naukowymi oraz polskim przemysłem kryptograficznym. Wskutek sporów kompetencyjnych z innymi podmiotami podległymi lub nadzorowanymi przez ministra obrony narodowej oraz braku konsekwencji w procesie formowania jednostki, od 2015 r. NCK skupiło się na zadaniu wsparcia resortowego systemu reagowania na incydenty komputerowe oraz przygotowaniu środowiska do prowadzenia działań w cyberprzestrzeni. Tym samym jednostka nie wypełnia swoich zadań statutowych, dotyczących wsparcia kryptologicznego bezpieczeństwa narodowego. Podsumowując, należy stwierdzić, że Polska nie posiada narodowego centrum kompetencji kryptologicznych.

Podsumowanie

Wspólną cechą polityk kryptologicznych państw obcych jest dążenie do uzyskania efektu synergii, wynikającego z prawnie uregulowanych działań na rzecz ukierunkowania i stymulowania przez państwowy ośrodek kompetencji kryptologicznych prac prowadzonych w tym zakresie przez krajowe ośrodki akademickie i badawczo-rozwojowe, a także narodowe przedsiębiorstwa funkcjonujące w obszarze kryptologii. Uzyskane rozwiązania techniczne są implementowane w celu ochrony informacji niejawnych oraz wrażliwych, wykorzystywanych w procesach informacyjnych, analitycznych, decyzyjnych i wykonawczych we wszystkich sferach funkcjonowania państwa, przyczyniając się tym samym do zwiększenia poziomu bezpieczeństwa narodowego. Kryptologia narodowa jest traktowana jako integralny element strategicznej osłony państwa.

Polska, pomimo demonstrowanych ambicji uzyskania statusu państwa liczącego się we wspólnocie międzynarodowej (w tym w NATO i UE) oraz ważnego „gracza" regionalnego, nie wykazuje determinacji w działaniach na rzecz budowy narodowego rozwiązania, które systemowo zapewniłoby wsparcie polskiej kryptologii dla bezpieczeństwa narodowego. Władze koncentrują się na ochronie systemów teleinformatycznych, pomijając kwestie kryptograficznego zabezpieczenia informacji.

Zdaniem autora, w obliczu narastających zagrożeń cybernetycznych oraz pojawiających się w szybkim tempie nowych wyzwań cyfryzacyjnych (wynikających m.in. z szybkiego upowszechnienia internetu rzeczy, organizacji wirtualnych i kryptowalut), które wkrótce wymuszą powszechne stosowanie kryptografii, nieuregulowanie systemowe narodowej polityki kryptologicznej w Polsce należy postrzegać jako poważny błąd strategiczny. Jego skutki staną się odczuwalne w perspektywie średniookresowej, prawdopodobnie już w przyszłej dekadzie. Niepodejmowanie działań w zakresie kryptologii narodowej, może doprowadzić

[30] Są to: Enigma SOI, Krypton Polska i Transbit.

[31] *SCIP* (*Secure Communications Interoperability Protocol*) – nowy standard cyfrowej łączności głosowej NATO; *NINE* (*Networking and Information Infrastructure (NII) Internet Protocol Network Encryption*) – nowy standard łączności sieciowej NATO.

[32] Są to przedsięwzięcia realizowane w ramach wielonarodowych inicjatyw rozwoju zdolności obronnych NATO *Smart Defence* oraz UE *Pooling and Sharing.*

do utraty przez Polskę zdolności i suwerenności w tym obszarze i całkowitego uzależnienia od zagranicznych produktów kryptograficznych, co w coraz większym stopniu będzie negatywnie oddziaływać na bezpieczeństwo państwa, zarówno w sferze niemilitarnej, jak i militarnej.

W tabeli 3 przedstawiono analizę SWOT dotyczącą możliwości wprowadzenia rozwiązania systemowego w zakresie kryptologii narodowej w Polsce.

Podsumowując treści przedstawione w artykule, autor uważa, że kwestie rozwoju narodowej kryptologii i jej znaczenia dla bezpieczeństwa narodowego powinny stać się przedmiotem pogłębionych badań i rozważań polskich ośrodków naukowych. Ich rezultaty służyłyby wypracowaniu propozycji rozwiązań umożliwiających uregulowanie oraz sformalizowanie powyższej problematyki na poziomie strategicznym w państwie.

Tabela 3

Analiza SWOT uwarunkowań wprowadzenia w Polsce rozwiązań strategicznych w zakresie wsparcia kryptologicznego bezpieczeństwa narodowego[33]

	Pozytywne	**Negatywne**
WEWNĘTRZNE	***Mocne strony*** • jednoznaczne zapisy dokumentów strategicznych • finansowanie (w ramach środków przeznaczanych na cyberbezpieczeństwo)	***Słabe strony*** • brak świadomości władz państwowych co do wagi problemu • brak koncepcji realizacji • brak instytucji odpowiedzialnej za kryptologię narodową na poziomie strategicznym państwa • brak bazy technologicznej i zaplecza technicznego • ograniczony zasób specjalistów z dziedziny kryptologii • wieloletnia praktyka dokonywania zakupów kryptografii za granicą
ZEWNĘTRZNE	***Szanse*** • duży potencjał narodowych ośrodków naukowych • utrzymane bazowe zdolności produkcyjne narodowego przemysłu kryptograficznego • doświadczenie polskich przedsiębiorstw w związku z udziałem w projektach NATO dot. kryptograficznej ochrony informacji • kształcenie specjalistów z dziedziny kryptologii na uczelniach cywilnych i cywilno-wojskowych (WAT)	***Zagrożenia*** • włączenie kwestii narodowej kryptologii do bieżącej walki politycznej – niezdolność organów państwa do sformalizowania narodowej polityki kryptologicznej • brak koordynacji działań podmiotów wykonawczych państwa • rywalizacja i spory kompetencyjne między podmiotami państwa – sferą militarną (MON i Siły Zbrojne RP) i cywilną (Ministerstwo Cyfryzacji) oraz służbami specjalnymi (ABW, SKW) • brak koncepcji dot. współpracy podmiotów państwa z akademią i przemysłem

[33] Opracowanie własne.