Wstęp

Praca w całości składa się z trzech rozdziałów. Pierwszy rozdział omawia środki oraz pojęcie współczesnej ochrony i obrony narodowej, które nie są bezpośrednio związane z ochroną informacji aczkolwiek są bardzo istotne i można od nich zacząć. Drugi rozdział opisuje strukturę organizacyjną Straży Granicznej, zaczynając od historii Wojsk Ochrony Pogranicza aż do formacji SG powstałej w 1991 r. Rozdział ten przybliża również dokładne, współczesne przepisy dotyczące kontroli osób przejeżdżających przez granicę państwową. Trzeci rozdział traktuje bezpośrednie o ochronie informacji, o jej celach, o konieczności jej ochrony oraz o konsekwencjach jej braku. Całość kończy krótkie podsumowanie

Rozdział I

Powszechna ochrona i obrona narodowa

1. Pojęcie i środki powszechnej ochrony i obrony narodowej

Podstawą trwałego bezpieczeństwa narodowego dla obecnego i przyszłych pokoleń Polaków jest zapewnienie przetrwania naszego społeczeństwa i dziedzictwa narodowego, jako warunku koniecznego do pomyślnego rozwoju. Realizacja tej podstawowej misji tworzenia bezpieczeństwa narodowego jest domeną powszechnej ochrony i obrony narodowej.

Państwo, aby mogło się swobodnie i skutecznie rozwijać, zapewnia ochronę i obronę własnych interesów w taki sposób, aby nikt na drodze ich osiągania nie tworzył przeszkód i utrudnień natury politycznej, militarnej, kulturowej, gospodarczej i społecznej. Jedną z zasadniczych funkcji i form organizacyjnych gwarantujących bezpieczeństwo pomyślnego rozwoju narodu jest powszechna ochrona i obrona narodowa.

Współczesne szerokie spektrum bezpieczeństwa narodowego wymaga istotnego poszerzenia tradycyjnego terminu „obrona narodowa" właśnie na „ochronę i obronę narodową". Celowość, a nawet konieczność wprowadzenia tego terminu do systemu pojęć z zakresu bezpieczeństwa narodowego wynika z następujących przesłanek:

1. Po pierwsze, dotychczasowe, wyniesione z XXw. pojęcie obrony narodowej w świadomości społeczeństw było powszechnie utożsamiane z obroną przed agresją, z przeciwstawianiem się zagrożeniom militarnym (wojennym). Jednak współczesne, różnorodne zagrożenia niemilitarne, są równie groźne jak wojna, a ochrona przed nimi jest równie ważna, jak obrona zbrojna przed zagrożeniami militarnymi.
2. Po drugie w systemie pojęć z obszaru bezpieczeństwa narodowego termin „ochrona"[1], np.: ochrona ludności, ochrona granic, ochrona dziedzictwa narodowego itd., powszechnie funkcjonuje podobnie jak w terminologii NATO np. ochrona wojsk, ochrona obiektów infrastruktury krytycznej itd.
3. Po trzecie przygotowanie sił zbrojnych i cywilnej organizacji obrony narodowej zarówno do „obrony narodowej" – w tradycyjnym rozumieniu

[1] Por. Zapis w Konstytucji III RP (1997 r.), art. 26: Siły zbrojne służą ochronie niepodległości państwa i niepodległości jego terytorium oraz zapewnieniu bezpieczeństwa i nienaruszalności jego granic.

– obrony przed agresją, jak i „obrony narodowej" w rozumieniu zapobiegania i przeciwdziałania zagrożeniom niemilitarnym, są nierozłączne.

4. Po czwarte, termin „ochrona i obrona narodowa, ujmuje całokształt działań cywilnych i wojskowych, zapewniających przetrwanie wartości i interesów narodowych w obliczu zagrożeń zarówno militarnych, jak i niemilitarnych.

Przyjmując zatem, że bezpieczeństwo narodowe jest najwyższą potrzebą i wartością narodu oraz głównym celem działań państwa – to ochrona i obrona narodowa jest funkcją, której celem jest chronić i bronić wartości narodowych przed zagrożeniami zewnętrznymi i wewnętrznymi, militarnymi i niemilitarnymi.

Zatem ochrona i obrona narodowa tworzy warunki niezbędne i konieczne dla pozostałych działań zapewniających bezpieczeństwo narodowe, jakim jest rozwój kulturalny i materialny. Równocześnie ochrona i obrona narodowa stanowi podstawę[2] skuteczności i wiarygodności polityki zagranicznej[3] w tworzeniu zewnętrznych warunków bezpieczeństwa narodowego.

Innymi słowy, w całokształcie działań państwa w tworzeniu i utrzymywaniu bezpieczeństwa narodowego ochrona i obrona narodowa zapewnia bezpieczeństwo rozwoju (tworzenia) siły narodowej, a jednocześnie chroni i broni wartości wytworzone.

W opinii czołowego stratega Zachodu A. Beaufre'a funkcja obrony okazuje się na bliższy i dalszy okres niezbędnym uzupełnieniem rozkwitu ekonomicznego i postępu kulturalnego, tak jak było w ciągu całej historii[4].

W dokonanym w 1934 r. przez gen. broni W. Sikorskiego ujęciu „nowoczesnej obrony kraju) całość organizacji ochrony i obrony narodowej została podzielona na dwie równorzędne części: cywilną i wojskową organizację

[2] Por Obrona zewnętrzna powinna być powszechną mocą narodu, Staszic S., Przestrogi dla Polski, PWN, Wrocław 2003, s. 24, Skubiszewski K., Z rewolucją i ewolucją w środowisku międzynarodowym nasza polityka radziła sobie i radzi, lecz skuteczność naszych działań zależy od mocy wewnętrznej państwa, w: Racja stanu z perspektywy polskiej, w: Rocznik polskiej polityki zagranicznej 1992, Warszawa 1994, s. 37.
[3] Slessor J. Polityka zagraniczna bez siły jest bezsilna, Strategia Zachodu, AON Warszawa 1958, s. 29.
[4] Beaufre, A., Wstęp do strategii. Odstraszanie i strategia, Warszawa 1968, s. 240.

obrony narodowej[5]. Upływ czasu, bogaty w wojenne i pokojowe doświadczenia, potwierdził trafność takiego ogólnego ujęcia struktury ochrony i obrony narodowej, które w tworzeniu tożsamości obronnej należy wykorzystać.

Obydwa komponenty, cywilny i wojskowy ochrony i obrony narodowej są ze sobą ściśle powiązane relacjami współpracy i koordynacji na szczeblu centralnym i terytorialnym oraz przygotowane do wzajemnego wsparcia swoich działań w czasie pokoju, a także w okresie kryzysu czy ewentualnej wojny.

Ochronę i obronę narodową można rozpatrywać co najmniej w kilku znaczeniach:

1. Po pierwsze, jako część organizacji państwa, obejmującą przygotowanie społeczeństwa, sił zbrojnych, zasobów i terytorium do zapobiegania, przeciwdziałania, ochrony i obrony całego narodu przed istniejącymi i potencjalnymi zagrożeniami bezpieczeństwa narodowego.
2. Po drugie, jako podstawową (fundamentalną) misję narodową (państwa) obejmującą zabezpieczenie przed istniejącymi i potencjalnymi zagrożeniami bezpieczeństwa narodowego.
3. po trzecie, jako podstawową (fundamentalną) strukturę realizacyjną bezpieczeństwa narodowego, obejmującą przygotowanie społeczeństwa, zasobów i terytorium do zapobiegania, przeciwdziałania, ochrony i obrony narodu (interesów narodowych) przed istniejącymi i potencjalnymi zagrożeniami bezpieczeństwa narodowego.
4. Po czwarte jako realizację konstytucyjnego obowiązku obrony ojczyzny[6] (Konstytucja III RP z 1997 r.) oraz podstawową powinność narodową[7] (Konstytucja z 3 maja 1791 r.).

Warto zwrócić uwagę, że w ujęciu ustawowym, zgodnie z ustawą z 4.09.1997 r. o działaniach administracji rządowej, obrona narodowa obejmuje sprawy: obrony państwa oraz sił zbrojnych.

[5] Sikorski W., Przyszła wojna, MON Warszawa 1984, s. 89.
[6] Konstytucja III RP, art. 85: Obowiązkiem obywatela polskiego jest obrona ojczyzny.
[7] Konstytucja 3 maja 1791 r.: Naród winien jest sobie samemu obronę od napaści i dla przestrzegania całości swojej. Wszyscy przeto obywatele są obrońcami całości i swobód narodowych.

Należy również dodać, że każde państwo – stosownie do specyfiki postrzegania i określania własnych interesów narodowych – odrębnie określa swoje pojęcie ochrony i obrony narodowej. Jednakże cechą wspólną dla państw demokratycznych jest to, że ochrona i obrona narodowa (totalna, powszechna) stanowi sumę wszystkich wojskowych (obrona militarna) i cywilnych (obrona cywilna – niemilitarna) zabezpieczeń służących zapewnieniu bezpieczeństwa państwa i społeczeństwa wobec zagrożeń godzących w bezpieczeństwo narodowe[8].

W życiu narodu i funkcjonowaniu państwa konieczne jest przygotowanie i stosowne użycie wszystkich własnych sił i środków działania[9] oraz pomoc innych państw – o ile takową potrafi się pozyskać. Ponieważ może być zagrożony byt i pomyślność wszystkich Polaków oraz wszystkich instytucji i dziedzin życia narodowego i społecznego, dlatego obrona narodu musi obejmować wszystkie sprawy: musi być nawet bardziej :"totalna" niż „totalny" jest nowoczesny napad[10].

Całość środków ochrony i obrony narodowej można podzielić na strukturalne środki ochrony i obrony narodowej, do których należy zaliczyć organy władzy, służbę zagraniczną, siły zbrojne oraz służby, inspekcje i straże, takie jak np. Policja, Straż Graniczna, Państwowa Straż Pożarna oraz funkcjonalne środki ochrony i obrony narodowej, np. polityczne, gospodarcze, wojskowe, ekologiczne, normatywne i inne.

Ze względu na zastosowanie, całość środków ochrony i obrony narodowej można podzielić na zabezpieczenia wartości i interesów narodowych (są to tzw. środki niemilitarne) oraz środki wojskowe traktowane jako ostateczny, decydujący środek ochrony i obrony narodowej.

2 Polityka i strategia powszechnej ochrony i obrony narodowej

Głównym celem polityki ochrony i obrony narodowej, wynikającym z podstawowej funkcji państwa oraz ustaleń Konstytucji RP, jest zapewnienie

[8] Kitler W., Obrona narodowa w wybranych państwach demokratycznych, AON, Warszawa 2001, s. 156.
[9] Por. Dyrektywy sprawnego działania: jak najpełniejszego wykorzystania posiadanych zasobów: maksymalnego wykorzystania zdolności do działania, J. Zieleniewski, Organizacja i zarządzanie, Warszawa 1969, s. 258-259.
[10] Koziej S., Teoria sztuki wojennej. Wydawnictwo "Bellona", Warszawa 1993, s. 142.

skutecznej ochrony i obrony wartości interesów narodowych przed istniejącymi i potencjalnymi zagrożeniami militarnymi i niemilitarnymi, wewnętrznymi i zewnętrznymi – bezpieczeństwa narodowego.

Nowoczesna strategia ochrony i obrony narodowej stanowi część realizacyjną strategii bezpieczeństwa narodowego, obejmującą wybór, przygotowanie i wykorzystanie oraz zespolenie cywilnych i wojskowych środków i metod w celu skutecznego zapobiegania (odstraszania), ochrony i obrony interesów narodowych przed istniejącymi i potencjalnymi zagrożeniami – militarnymi i niemilitarnymi, wewnętrznymi i zewnętrznymi – bezpieczeństwa narodowego Polski, członka wspólnoty obronnej NATO.

Istota takiej strategii zawiera się w wyborze właściwych i koniecznych, a posiadanych przez Polskę cywilnych i wojskowych środków i metod ochrony i obrony, odpowiednich do współczesnych uwarunkowań i zagrożeń bezpieczeństwa narodowego oraz bezpieczeństwa wspólnoty obronnej NATO.

Dla zrozumienia współczesnego pojęcia „strategii ochrony i obrony narodowej" konieczne jest poznanie rodowodu pierwotnego znaczenia terminu „strategia", który współcześnie, po jego „ucywilnieniu" od połowy XIX w. „wstąpił" do języka potocznego, stając się synonimem każdego planowanego, długofalowego działania. Dlatego właśnie, dla uniknięcia nieporozumień, konieczne jest rozróżnienie pierwotnego znaczenia strategii – od potocznego jej używania (a raczej nadużywania)[11].

Termin „strategia" ma rodowód grecki z okresu „gigantów" myśli i działania, jak cytowany na wstępie Sokrates i tacy słynni „stratedzy" – czyli pełniący tę funkcję w okresie „złotego wieku Aten" – jak Temistokles i Perykles. Najpierw z połączenia dwóch wyrazów: sratos – wojsko i ago – prowadzić, powstał termin strateg, oznaczający (naczelnego) dowódcę.

Z kolei połączenie wyrazu „strateg" z wyrazem gia – wiedza, sztuka, powstał termin „strategia", oznaczający dosłownie sztukę wodza albo dowodzenie (przez wodza). Od czasów starożytnych do przełomu napoleońskiego (XVIII/XIX w.), kiedy wojny sprowadzały się najogólniej do

[11] Por. Menkiszak M., Czy Polska potrzebuje strategii? w: R. Kuźniar (red.), Między polityką a strategią, OSW, Warszawa 1994, s. 31.

tzw. bitew walnych (generalnych)[12] przygotowanych i prowadzonych przez wodzów (strategów), to stare słowo określało przez długi czas tylko wiedzę i umiejętności naczelnego wodza, co oczywiście odnosiło się naprawdę jedynie do bardzo małej liczby osób.

Tak więc do Napoleona włącznie strategia miała swoje pierwotne, tradycyjne znaczenie „czysto" wojskowe dla określenia działalności i wodzów (strategów) w prowadzeniu bitew walnych przy użyciu wojska.

Radykalna zmiana charakteru strategii z tradycyjnej na nowoczesną dokonała się w okresie przełomu napoleońskiego XVIII/XIX w., ale sam Bóg wojny Napoleon nie był ojcem tych zmian, a tylko symbolem wykorzystania i ofiarą zmian, jakie przyniosła historia. To zmiany społeczne i polityczne (rewolucja amerykańska 1775-1782 r. i rewolucja francuska 1789 r.) spowodowały powstanie całkowicie nowej kategorii państwa – państwa narodowego, w którym naród – jako ogół społeczeństwa, a nie oligarchia stał się suwerenem państwa, utożsamiającym się z państwem, gotowym z przekonania (a nie przymusu) go bronić.

Właśnie Napoleon był tą postacią w historii, której nowoczesne narodowe państwo francuskie „dało" nowoczesną armię narodową[13], armię obywatelską z powszechnego poboru (której żołnierze utożsamiając się z Napoleonem symbolizującym wolną Francję wykazali olbrzymią siłę moralną), odtąd decydujący czynnik nowoczesnej strategii. To właśnie tą armią narodową geniusz Napoleona dokonał w obronie interesów narodowych Francji bezprecedensowych w historii wojen czynów. Stosując tradycyjną strategię bitwy walnej (generalnej), ale nowoczesną armią narodową rozbił w kilkudziesięciu bitwach armie ówczesnych mocarstw – Austrii, Prus i Rosji, stając się w 1807 r. władcą Europy od kanału La Manche do Niemna.

Z kolei Napoleon jako agresor został pokonany przez obrońców Hiszpanii i Rosji, nie w bitwach walnych (generalnych), ale przez nowoczesną strategię powszechnej obrony narodowej. Podobnie w XX w. zostały pokonane wszystkie mocarstwa i wszystkie mocarstwa przez państwa (narody) broniące się lub wyzwalające spod dominacji.

[12] Bitwa walna (generalna) – walka głównych sił obu stron rozstrzygająca o zwycięstwie lub klęsce w wojnie. Według C. v. Clausewitz: Jest to walka sił głównych lecz walka toczona z całym wysiłkiem o istotne zwycięstwo, O Wojnie, Lublin 1995, s. 267.

[13] Napoleon: „tylko armia narodowa może zapewnić republice spokój i poszanowanie z zewnątrz".

Na czym zatem polega nowoczesna strategia ochrony i obrony narodowej – szansa na zapewnienie trwałego i skutecznego bezpieczeństwa Polski, a zarazem bezpieczeństwa wspólnoty obronnej NATO? Odpowiedź na to pytanie znajdują światli politycy i dowódcy od blisko 200 lat w ponadczasowym, uniwersalnym dziele strategii „O wojnie" gen. C. v. Clausevitza. Ten Pruski generał był świadkiem błyskawicznego rozbicia przez narodową armię Napoleona potężnej armii pruskiej opartej na legendarnym drylu Fryderyka II Wielkiego. Upokorzenie, a wręcz ośmieszenie armii pruskiej wyzwoliło m. in u Clausewitza potrzebę jej generalnej reformy z wykorzystaniem doświadczeń napoleońskich. W ostatnim okresie wojen napoleońskich C. v. Clausewitz walczył z Napoleonem, najpierw w szeregach armii rosyjskiej, a potem pruskiej. Pod koniec kariery wojskowej był komendantem Szkoły Wojennej w Berlinie.

Według współczesnego stratega amerykańskiego B. Brodiego: Carl von Clausewitz jest pierwszą wielką twórczą postacią w nowoczesnej strategii, podobnie jak Adam Smith jest pierwszą osobistością w nowoczesnej ekonomii. Jednakże Clausewitz, w przeciwieństwie do Smitha pozostał na wyżynach swojej twórczości prawie samotny.

W czym zatem wyraża się nowoczesna strategia obrony narodowej ujęta przez C. v. Clausewitza w dziele O wojnie? Przede wszystkim w odesłaniu do historii bitwy walnej (generalnej), jako rozstrzygającej o wyniku wojny: Żadne państwo nie powinno sądzić, że los jego, a mianowicie cały jego byt zawisł od jednej bitwy, chociażby najbardziej rozstrzygającej. Następnie o wyrażeniu, że to nie tylko armia bierze udział i decyduje o obronie narodu, ale cały naród.

Clausewitz wykazał, że „obezwładnienie państwa" (narodowego) nie sprowadza się do wygrania rozstrzygającej bitwy walnej (generalnej), ale do obezwładnienia w trzech obszarach: Siły zbrojne należy zniszczyć, kraj należy zdobyć. Jednakże nawet po osiągnięciu obu tych celów, tak długo nie można wojny – czyli nieprzyjaznego napięcia i działania wrogich sił – uważać za ukończoną, dopóki jego rząd i sojusznicy nie będą zmuszeni do podpisania pokoju, a naród do poddania się[14].

Jednym z najdonioślejszych założeń nowoczesnej strategii C. v. Clausewitza jest teza o przewadze obrony nad natarciem. Przewaga obrony

[14] Ibidem, s. 28.

(dobrze pojętej) jest bardzo duża – o wiele większa, niż się to na pierwszy rzut oka wydaje[15]. Zlekceważenie tej tezy w doktrynach[16] obronnych zaatakowanych przez Hitlera państw na czele z Polską, uważane jest za główną przyczynę ich klęsk a zarazem źródło blitzkriegu (błyskawicznej wojny) Wehrmachtu.

3. Warunki i wymogi powszechnej ochrony i obrony narodowej

Przygotowanie strategii ochrony i obrony narodowej Polski powinno uwzględniać następujące warunki.

1. Polska zajmuje kluczowy dla bezpieczeństwa Europy obszar, położony na korytarzu euroazjatyckim, który był, jest i będzie przedmiotem ekspansji dla mocarstw dążących do dominacji kontynentalnej bądź globalnej,
2. Polska położona jest w sąsiedztwie dwóch wielkich mocarstw dysponujących państwową, o historycznie potwierdzonej dążności do ekspansji,
3. słabą, w stosunku do wielkich sąsiadów, państwowość polską cechuje ugruntowana historycznie skłonność do anarchii[17] - odwrócenie obywateli od działania na rzecz wspólnego dobra, brak państwowotwórczych elit politycznych, wojskowych i administracyjnych, brak przezorności, naiwna wiara w trwałość i skuteczność sojuszów, brak troski o własną siłę obronną,
4. członkostwo w NATO wzmacnia nasze narodowe wysiłki obronne i włącza Polskę do działań na rzecz obrony wspólnej NATO. Zgodnie z Traktatem Północnoatlantyckim (art. 3) i „Koncepcją strategiczną Sojuszu" członkostwo w NATO nie tylko nie pozbawia Polski „suwerenności w dziedzinie obrony", ale zobowiązuje do utrzymywania i rozwijania swojej indywidualnej i zbiorowej zdolności do odparcia zbrojnej napaści. Warunkiem otrzymania wzmocnienia od innych państw NATO oraz wiarygodności Polski jest osiągnięcie interoperacyjności

[15] Ibidem, s. 18.
[16] Doktryna: 1. „Podstawowe zasady (dogmaty), którymi siły zbrojne kierują się w działaniach, Dictionary of Military and Associated Terms, Washington 1987, s. 118, 2. Oficjalnie przyjęta, mająca odbicie w dyrektywach i instrukcjach (określona) strategia.
[17] Por. Jeziorański J., „Żadne jednak wojskowe sojusze nie zabezpieczą nas przed zagrożeniem płynącym od wewnątrz", Polska wczoraj, dziś i jutro, Warszawa 1999, s. 128-129.

przez część wojsk operacyjnych oraz zdolność wypełnienia funkcji państwa-gospodarcza (HNS – Host Nation Support),

5. nowoczesna generacja broni rakietowej kierowanej i samonaprowadzanej, stworzyła niespotykaną w historii wojen szansę techniczną i ekonomiczną skutecznego przeciwstawienia się nawet wielokrotnej przewadze potencjalnych przeciwników w broni ofensywnej (broń pancerna, lotnictwo, wielkie okręty)[18],
6. zacieranie się wyraźnych różnic między zagrożeniami militarnymi oraz niemilitarnymi bezpieczeństwa narodowego (np. broń masowego rażenia, terroryzm) oraz wciąż wzrastająca skala zagrożeń niemilitarnych, stwarzająca konieczność zwiększenia zdolności i sprawności cywilnych środków i metod obrony narodowej, a także coraz szerszego przygotowania sił zbrojnych do wsparcia władz i społeczeństwa w sytuacjach zagrożeń niemilitarnych,
7. warunkiem koniecznym skuteczności współczesnej ochrony i obrony narodowej oraz obrony wspólnej NATO jest zespolenie przygotowania i wykorzystania cywilnych i wojskowych środków ochrony i obrony na wszystkich szczeblach kierowania państwa oraz struktury polityczno-wojskowej NATO,
8. największym, niezastąpionym i najbardziej twórczym „środkiem", a zarazem największą szansą dla zapewnienia skutecznej obrony narodowej na progu XXI w. jest potencjał ludzki Polski[19] - liczba ludności o jednym z największych odsetków młodzieży, niemalże jednorodne narodowo społeczeństwo, dynamiczne, świadome daru wolności i demokracji, żądne doścignięcia cywilizacyjnego Zachodu, a zarazem zachowujące dumną cechę starożytnych Słowian.

[18] Najważniejsze w XX w. rodzaje sprzętu: czołg, samolot będą miały – jako nosiciele systemów uzbrojenia – znaczenie jedynie symboliczne. Zostaną zastąpione przez rakiety kierowane i niekierowane, Johanes Gerber, International Military and Defense Encyclopedia, London-New York 1991.

[19] „Koncentracja uwagi na czynniku ludzkim – klucz do sukcesu organizacji spoczywa co najmniej w takim samym stopniu na czynniku ludzkim jak na czynnikach technologicznych lub finansowych" jedna – z trzech złotych reguł kultury strategicznej, [w]: A. Klasik (red.), Planowanie strategiczne, Warszawa 1993, s. 79.

Dlatego największym wyzwaniem dla strategii ochrony i obrony narodowej jest powszechne włączenie potencjału ludzkiego Polski w cywilne i wojskowe przygotowania oraz działania ochrony i obrony wartości i interesów narodowych.

Podstawowe wymogi strategii ochrony i obrony narodowej można sformułować następująco:

1. strategia ma tworzyć (kreować) przyszłe bezpieczeństwo narodowe, a więc uprzedzać, zapobiegać (odstraszać) zagrożeniom i likwidować ich źródła. Nie może być konstruowana w oparciu o przewidywania przyszłości, gdyż „przyszłość" jest zmienna, nieprzewidywalna, a regułą jest zaskoczenie,
2. strategia musi być przygotowana na sprostanie najgorszemu zagrożeniu, jakie się może zdarzyć w oparciu o doświadczenia z historii. Błędem jest zakładanie, że będzie dobrze ponieważ – jak t ujął P. Jasienica – „tylko głupiec rachuje wyłącznie na okoliczności najlepsze".
3. zadaniem strategii jest osiągnięcie celów ustalonych przez politykę przy jak najlepszym wykorzystaniu posiadanych środków,
4. w wyborze środków i metod działania nie należy obierać za punkt wyjścia tego, co jest możliwe, ale szukać tego, co jest konieczne i starać się to osiągnąć[20],
5. w strategii zmierzać do określonego celu w danych warunkach przy użyciu właściwych środków,
6. w strategii należy zapewnić zgodność i równowagę celów, metod i środków[21],
7. zapewnienie strategii zdolności przystosowania się do najróżniejszych i być może najmniej przewidzianych sytuacji.

[20] Ibidem, s. 161.
[21] Nevell, C., R. Balancing The Ends, Ways and Means Army 1986, nr. 8, s. 24-32.

4. Ochrona i obrona w dziedzinie informacyjnej

Niezwykle intensywny rozwój cywilizacyjny w ostatnim wieku, określanym jako „stulecie globalne”[22], ściśle wiąże się z postępem w zakresie zdolności pozyskiwania, przetwarzania i przekazywania informacji. Dlatego też druga połowa XX w., zwana „erą informacyjną”, to czas w którym jednym z czynników stanowiących kluczowy element sprawności działania wielu złożonych organizacji, a zwłaszcza państw i ich zasadniczych elementów składowych oraz organizacji o charakterze międzynarodowym jest informacja[23].

Poziom rozwoju technicznych nośników i przetworników informacji oddziałuje bezpośrednio na poziom rozwoju państwa (na naukę, gospodarkę, kulturę, środowisko, świadomość społeczną) i jego bezpieczeństwo, a także na jakość kierowania nim w całości oraz funkcjonującymi na jego obszarze organizacjami z osobna[24]. Im wyższe uzależnienie od technicznej sfery informacji, tym większa wrażliwość na wszelkie potencjalne zakłócenia i zagrożenia, które mogą mieć różnorakie przyczyny i różną postać[25]. Mogą to być wszelkiego rodzaju zdarzenia naturalne i wywołane przez człowieka, prowadzące do fizycznego zniszczenia systemów informacyjnych (np. pożary, powodzie, katastrofy techniczne) lub naruszenia technicznych parametrów pracy tychże systemów (np. wyładowania atmosferyczne, oddziaływanie magnetyczne ziemi i kosmosu, zakłócenia elektromagnetyczne i czujnikowe, a także zmiana daty nieprzewidziana w oprogramowaniu komputerowym) lub zmiany danych stanowiących rzetelności przesyłanych informacji (np. zakłócenia informatyczne: „wirusy” „konie trojańskie” „bomby logiczne”, „bakterie i króliki”, wprowadzenie fałszywych informacji w trybie pozainformatycznym,

[22] Jemioło T., Globalizacja, Szanse i zagrożenia, AON, Warszawa 2000, s. 13
[23] Ciborowski L., Walka informacyjna, Europejskie Centrum Edukacyjne, Toruń 1999, s. 7
[24] T. Jemioło stwierza, że wzrost dostępności informacji spowoduje decentralizację procesu decyzyjnego i odrodzenie się struktur poziomych, T. Jemioło, op. cit., s. 22
[25] Doskonałym tego przykładem był „Problem roku 2000” związany z „krytycznymi datami”: 9 i 19 września 1999 roku., 1 stycznia 2000 roku., 29 lutego 2000 roku oraz 1 marca 2000 roku. Gdyby nie było tak znaczącego uzależnienia życia międzynarodowego i państwowego od systemów informatycznych, nie byłoby żadnego problemu. Jednak „krytyczna data” sprawiła, że należało się liczyć z ewentualnością wystąpienia zakłóceń w gospodarce, bankowości, systemach bezpieczeństwa (np.: urządzenia sterujące rakiet, stacji rozpoznawczych, samoczynnych czujników), mediach, infrastrukturze i wielu innych dziedzinach.

jak choćby w prasie, radiu i telewizji, ingerowanie w tryb przesyłania informacji, blokowanie, mylenie[26].

Powszechna dostępność do informacji, poza jej pozytywnymi rezultatami, powoduje także wystąpienie wielu nowych uwarunkowań obcych erze industrialnej. Liczyć się będą tylko ci, których stać na nieograniczone dysponowanie informacją, którzy będą mieli możliwość sterowania opinią społeczną, a co za tym idzie sterowania zachowaniami społecznymi nie zawsze zgodnymi z powszechnie przyjętymi normami społecznymi[27].

Zatem ochrona i obrona w sferze informacyjnej to wszelka działalność związana z realizacją celów ochrony i obrony narodowej, przez informacyjne oddziaływanie na zachowania i postawy podmiotów międzynarodowych i krajowych, ochronę interesów narodowych przed negatywnymi skutkami oddziaływań tych podmiotów[28], a także ochronę technicznych urządzeń informacyjnych przed oddziaływaniami sił przyrody i człowieka, w razie potrzeby oddziaływanie na techniczne urządzenia informacyjne innego podmiotu (grupy społecznej państwa).

Informacyjne oddziaływanie na zachowania i postawy podmiotów międzynarodowych i krajowych, ochrona interesów narodowych przed negatywnymi skutkami oddziaływań tych podmiotów powinna być koordynowana w ramach polityki rządu, zaś w sferze wykonawczej miałaby charakter wybitnie zdecentralizowany. Związana byłaby bowiem z działalnością w zakresie obrony dyplomatycznej, ochrony porządku konstytucyjnego (głównie w zakresie: ochrony państwa, ochrony informacji niejawnych, ochrony danych osobowych), obrony militarnej, gospodarczej, porządku publicznego, ochrona granicy państwowej, ochrony ludności.

[26] Nowacki G., Współczesne poglądy na prowadzenie walki informacyjnej, AON, Warszawa 2001, s. 55-66

[27] Korzystają z tego mass media, które z powodzeniem sterują ludzkimi zachowaniami, wpływają na psychikę ludzką, a w konsekwencji zmieniają przyzwyczajenia i zachowania ludzi, a wszystko w imię wolnego przepływu informacji. Doceniają to także silne państwa używając mediów do celów publicznej dyplomacji, czyli oddziaływania informacyjnego na inne państwa i społeczność międzynarodową.

[28] Chodzi tu m. in. o takie interesy jak: bezpieczeństwo państwa, porządek publiczny, bezpieczeństwo powszechne, prawa i wolności człowieka i obywatela, suwerenność państwa.

Rozdział II

Ochrona polskiej granicy państwowej

1. Rys historyczny Wojsk Ochrony Pogranicza

Wojska Ochrony Pogranicza – utworzone na podstawie rozkazu Naczelnego Dowódcy Wojska Polskiego nr 0245 z dnia 13 września 1945 roku w celu ochrony granicy państwowej. Do głównych zadań Wojsk Ochrony Pogranicza należało zapobieganie, przeciwdziałanie i zwalczanie przestępczości granicznej, zapewnienie bezpieczeństwa i porządku publicznego w pasie granicznym, nadzór nad przestrzeganiem przepisów dotyczących obrony granicy państwowej, obowiązujących w strefie nadgranicznej, pasie granicznym na morskich wodach wewnętrznych i morzu terytorialnym oraz wykonywanie niektórych czynności będących w kompetencji administracji celnej[29].

Zorganizowane były według struktur wojskowych, instancję naczelną stanowił Departament Wojsk Ochrony Pogranicza, podległy wiceministrowi Obrony Narodowej. Przy dowództwach okręgów wojskowych utworzono Wydziały Wojsk Ochrony Pogranicza, którym podporządkowano Oddziały Wojsk Ochrony Pogranicza, a tym Komendy Odcinków i Strażnice Wojsk Ochrony Pogranicza, (które stanowiły najmniejsze jednostki formacji). W październiku 1945 roku zorganizowano dodatkowo na granicy Przejściowe Punkty Kontrolne. Na wybrzeżu Bałtyckim zaczęto tworzyć Flotylle, złożone ze ścigaczy i motorówek.

Na mocy rozkazu Ministerstwa Obrony Narodowej nr 055 z dnia 20 marca 1948 roku przemianowano Departament Wojsk Ochrony Pogranicza na Główny Inspektorat Ochrony Pogranicza, Oddziały Wojsk Ochrony Pogranicza na Brygady Ochrony Pogranicza, Komendy Odcinków na Samodzielne Bataliony Ochrony Pogranicza, a dotychczasowe Przejściowe Punkty Kontrolne na Graniczne Placówki Kontrolne. W grudniu tego roku Wojska Ochrony Pogranicza przechodziły z Ministerstwa Obrony Narodowej pod kompetencje Ministerstwa Publicznego, co formalnie nastąpiło z dniem 1 stycznia 1949 roku. Dla nadania większej wagi ochronie granic i podkreślenie wojskowego charakteru przeformowano z dniem 1 stycznia 1950 roku Główny Inspektorat Ochrony Pogranicza w Dowództwo Wojsk Ochrony Pogranicza. Zmiany polityczne, jakie dokonały się po śmierci Stalina, wpłynęły w dużym stopniu na

[29] Dominiczak H., Granice państwa i ich ochrona na przestrzeni dziejów 966–1996; Warszawa 1997, s. 43

organizację Wojsk Ochrony Pogranicza. W 1954 roku wyszły one spod kompetencji Ministerstwa Bezpieczeństwa Publicznego i zostały podporządkowane Ministerstwu Spraw Wewnętrznych. W czerwcu 1956 roku rozformowano na granicy wschodniej 4 brygady Wojsk Ochrony Pogranicza, a w ich miejsce utworzono Grupy Manewrowe Wojsk Ochrony Pogranicza. Podlegały one Dowództwu Wojsk Ochrony Pogranicza, a w sprawach operacyjnych – czterem sformowanym Samodzielnym Oddziałom Zwiadowczym, odpowiedzialnym odtąd za ochronę granicy wschodniej. W 1957 roku połączono Grupy Manewrowe z Samodzielnymi Oddziałami Zwiadowczymi i utworzono cztery Oddziały Wojsk Ochrony Pogranicza. W roku następnym każda z brygad i oddziały otrzymały nazwy regionalne (np.: 12 Pomorska Brygada Wojsk Ochrony Pogranicza, 26 Przemyski Oddział Wojsk Ochrony Pogranicza). Z dniem 1 lipca 1965 roku Wojska Ochrony Pogranicza wyszły spod kompetencji Ministerstwa Spraw Wewnętrznych i zostały ponownie podporządkowane Ministerstwu Obrony Narodowej. W resorcie Ministerstwa Spraw Wewnętrznych pozostały natomiast graniczne placówki kontrolne, które ochraniały przejścia graniczne. Naruszeniu uległ, jednolity dotąd, system ochrony granic państwa: granicę „zieloną" ochraniali żołnierze Wojsk Ochrony Pogranicza (podlegli Ministerstwu Obrony Narodowej), a ruch graniczny: obiekty z nim związane – funkcjonariusze Milicji Obywatelskiej (podlegli Ministerstwu Spraw Wewnętrznych). Wraz z przeprowadzonymi zmianami rozformowano Dowództwo Wojsk Ochrony Pogranicza, a w jego miejsce powołano w październiku 1965 roku Szefostwo Wojsk Ochrony Pogranicza. W podległych Szefostwu brygadach i oddziałach Wojsk Ochrony Pogranicza przeprowadzono następnie szereg zmian organizacyjnych i etatowych, których wynikiem było między innymi utworzenie strażnic technicznych, lądowych i morskich[30].

Decyzją Prezydium Rządu z 30 lipca 1971 roku Wojska Ochrony Pogranicza z dniem 1 października 1971 roku pod względem dowodzenia, a z dniem 1 stycznia 1972 roku pod względem gospodarczym przechodziły ponownie pod kompetencje Ministerstwa Spraw Wewnętrznych. Z dniem 1 stycznia tego roku do Wojsk Ochrony Pogranicza powróciły także wszystkie przejścia graniczne (wraz z obsadą). Szefostwo Wojsk Ochrony Pogranicza zostało zlikwidowane, a w jego miejsce powołano Dowództwo Wojsk Ochrony Pogranicza. W 1976 roku, w związku z nowym podziałem

[30] Jackiewicz Z., Wojska Ochrony Pogranicza 1945 – 1991. Krótki Informator Historyczny, Kętrzyn 1998, s. 96

administracyjnym kraju (likwidacje powiatów), dołączono odcinki jednostek i pododdziałów do granic województw i gmin granicznych.

W brygadach rozformowano bataliony graniczne, a utworzono placówki zwiadu i kompanie odwodowe do wzmocnienia strażnic. Oddziały Wojsk Ochrony Pogranicza ochraniające granicę wschodnią przeformowano w brygady, a placówki na całej granicy w strażnice. Zrezygnowano z numeracji brygad i nadano nowe nazwy regionalne brygadom (np.: Pomorska Brygada Wojsk Ochrony Pogranicza, Bieszczadzka Brygada Wojsk Ochrony Pogranicza). Proces odtwarzania niektórych batalionów granicznych zapoczątkowano po zniesieniu stanu wojennego (lipiec 1983 rok). W tak ukształtowanej strukturze organizacyjnej Wojska Ochrony Pogranicza w zasadzie przetrwały do końca ich istnienia (jedynie 1989 roku rozformowano Lubuską Brygadę Wojsk Ochrony Pogranicza, a w 1990 roku przeformowano Bałtycką Brygadę Wojsk Ochrony Pogranicza w Bałtycki Oddział Wojsk Ochrony Pogranicza).

W dniu 15 maja 1991 roku Wojska Ochrony Pogranicza zostały zlikwidowane, a ochronę granic przejęła nowa formacja graniczna – Straż Graniczna Rzeczpospolitej Polskiej.

2. Straż graniczna a ochrona granicy państwowej

Zmiany polityczne zachodzące w Europie Środkowej i Wschodniej pod koniec lat osiemdziesiątych i na początku lat dziewięćdziesiątych spowodowały konieczność zmiany charakteru granicy państwa. Przestała być barierą polityczną, stała się natomiast granicą wyznaczającą terytorium suwerennego, demokratycznego państwa oraz jego obszar ekonomiczny. Do nowej sytuacji politycznej i ekonomicznej należało dostosować sposób ochrony granicy państwowej. Dlatego też ustawą z 12 października 1990 r. powołana została Straż Graniczna[31], która z dniem 16 maja 1991 r. przejęła od Wojsk Ochrony Pogranicza ochronę granicy państwowej i kontrolę ruchu granicznego[32], stając jednocześnie przed nowymi, nie do końca znanymi w tym czasie zadaniami i wyzwaniami. Straż Graniczna to formacja typu policyjnego, przystosowana zarówno swoim charakterem, strukturami, jak i metodami pełnienia służby do ogólnych

[31] Ustawa z 12 października 1990 r. o Straży Granicznej (tekst jedn. Dz. U z 2005 r. nr. 234, poz. 1997. ze zm.).

[32] Wojska Ochrony Pogranicza (WOP) zostały utworzone 13 września 1945 r. były odpowiedzialne za ochronę polskiej granicy państwowej aż do 15 maja 1991 r. W tym okresie system ochrony granicy był zorganizowany inaczej niż w II RP: główny nacisk położono na ochronę odcinka zachodniego i morskiego, koncentrując tam większe siły i środki niż na wschodzie. Strukturę WOP tworzyły: Dowództwo WOP, brygady, bataliony i strażnice.

przepisów prawnych obowiązujących w państwach UE, a także do współpracy ze służbami granicznymi tych państw.

W chwili powoływania do życia Straży Granicznej pojawiły się hipotezy, że przestępczość graniczna powinna stopniowo zanikać. Po 15 latach funkcjonowania nowej formacji należy stwierdzić, że na pewno ona nie zanika, może się zmieniać i zmniejszać, z pewnością ulega różnym przeobrażeniom. Ma na to wpływ wiele różnych uwarunkowań (zewnętrznych i wewnętrznych), które będą występować jeszcze przez wiele lat. Najważniejszym i najistotniejszym zagrożeniem jest nielegalna migracja tranzytowa przez teren Polski do państw członkowskich „starej piętnastki" oraz przemyt, w tym przemyt używek (narkotyków, papierosów, alkoholu) i materiałów zagrażających środowisku naturalnemu. W obu przypadkach pojawiają się grupowe formy działania. Zauważa się, że przestępczość coraz częściej przybiera formy zorganizowane. Kanały przerzutu osób zaczynają się w dalekich krajach Azji lub Afryce, wiodą przez Rosję, Ukrainę, Litwę do Polski. Zdarza się, że polskie paszporty fałszuje się gdzieś w Azji, a mieszkańcy Dalekiego lub Bliskiego Wschodu (np. Wietnamczycy, Czeczeńcy) wiedzą z kim nawiązać kontakt tuż po przekroczeniu polskiej granicy. Coraz częściej zajmują się tym wyspecjalizowane grupy przestępcze, które z tego procederu uczyniły swoje stałe źródło dochodów. Ich ujawnienie jest utrudnione, gdyż kierują swoją działalnością z obszaru Polski. Ponadto doskonalą one swoje metody działania, angażują wiele środków, korzystają z szerokiego kręgu pomocników, rekrutujących się zarówno z obywateli polskich, jak i obywateli obcych państw przebywających na terenie Polski[33]. Należy dodać, że harmonizowanie polskich przepisów prawnych z przepisami unijnymi, podpisywane tzw. umowy readmisyjne, stanowią ważny element przeciwdziałania nielegalnej migracji. Odnosi się to głównie do kształtowania polityki azylowej oraz polityki wizowej Wspólnoty Europejskiej. Istotny wpływ na ograniczenie nielegalnej migracji ma na ogół dobrze rozwijająca się współpraca służb granicznych państw ościennych, zwłaszcza Niemiec.

Walka z przemytem nie jest głównym zadaniem Straży Granicznej, jednakże w ramach współdziałania oraz zintegrowanego zarządzania granicą jej funkcjonariusze na równi ze służbą celną angażują się m. in w działania przeciwko przemytnikom. Każdy z odcinków polskiej granicy ma swój charakterystyczny „asortyment" towaru, np. przez

[33] Gawryś R., Olejnik G., Doświadczenia Straży Granicznej w przeciwdziałaniu międzynarodowej przestępczości zorganizowanej związanej m. in. z nielegalną migracją, Centrum Szkolenia Straży Granicznej, „Problemy Ochrony Granic", Kętrzyn 2004, nr. 29, s. 42-44

wschodnią granicę od wielu lat przemycane są używki (alkohol, papierosy). Specyficznym przemycanym towarem są kradzione samochody. Generalnie zajmują się tym służba celna (podobnie jak całym granicznym obrotem towarowym), ale ujawnianie takich aut stało się już niejako „specjalnością" Straży Granicznej. To, że Polska znalazła się w kręgu zainteresowania międzynarodowych grup przestępczych, zajmujących się przemytem narkotyków, nie budzi dziś wątpliwości. Przeciwdziałanie nielegalnemu importowi i wszelkiego rodzaju materiałów zagrażających środowisku naturalnemu, środków i materiałów o podwyższonej radiacji oraz chemicznych należy także do obszarów działalności Straży Granicznej.

Działania Straży Granicznej to nie tylko przeciwdziałanie i zwalczanie przestępczości granicznej, to również kontrola ruchu granicznego, zabezpieczenie przekraczania granicy przez osoby, które z zachowaniem stosownych przepisów oraz na podstawie ujawniających się do tego dokumentów podróżują po Europie i po innych kontynentach. Dynamiczny rozwój ruchu granicznego wpłynął na zmianę zasad dokonywania jego kontroli, zwłaszcza gdy coraz ważniejszą rolę spełniają w nich systemy informatyczne[34].

Ze względu na różne formy przestępczości granicznej oraz przesłanki jej wystąpienia ustawodawca określił w ustawie o Straży Granicznej liczne zadania Straży Granicznej RP (art. 1 ust 2). Są to:

1. ochrona granicy państwowej,
2. organizowanie i dokonywanie kontroli ruchu granicznego,
3. wydawanie zezwoleń na przekraczanie granicy państwowej, w tym wiz,
4. rozpoznawanie, zapobieganie i wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców, w zakresie właściwości Straży Granicznej, a w szczególności:
    a. przestępstw i wykroczeń dotyczących zgodności przekraczania granicy państwowej z przepisami, związanych z jej oznakowaniem oraz dotyczących wiarygodności dokumentów uprawniających do przekraczania granicy państwowej,
    b. przestępstw skarbowych i wykroczeń skarbowych wymienionych w art. 134 & 1 pkt. 1 Kodeksu karnego skarbowego,

[34] Ibidem

c. przestępstw i wykroczeń pozostających w związku z przekraczaniem granicy państwowej lub przemieszczaniem przez granicę państwową towarów oraz wyrobów akcyzowych podlegających obowiązkowi oznaczania znakami akcyzy, jak również przedmiotów określonych w przepisach o broni i amunicji, o materiałach wybuchowych, o ochronie dóbr kultury, o narodowym zasobie archiwalnym, o przeciwdziałaniu narkomanii oraz o ewidencji ludności i dowodach osobistych,
d. przestępstw i wykroczeń określonych w ustawie z 13 czerwca 2003 r. o cudzoziemcach oraz ustawie z 13 czerwca 2003 r. o udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej Polskiej[35],
e. przestępstw przeciwko bezpieczeństwu powszechnemu oraz przestępstw przeciwko bezpieczeństwu w komunikacji, pozostających w związku z wykonywaniem komunikacji lotniczej.

5. zapewnienie bezpieczeństwa w komunikacji międzynarodowej i porządku publicznego w zasięgu terytorialnym przejścia granicznego, a w zakresie właściwości Straży Granicznej – także w strefie nadgranicznej,
6. przeprowadzanie kontroli bezpieczeństwa w zasięgu terytorialnym przejścia granicznego oraz w środkach transportu w komunikacji międzynarodowej,
7. zapewnienie bezpieczeństwa na pokładzie statków powietrznych wykonujących przewóz lotniczy pasażerów,
8. osadzanie i utrzymywanie znaków granicznych na lądzie oraz sporządzanie, aktualizacja i przechowywanie granicznej dokumentacji geodezyjnej i kartograficznej,
9. ochrona nienaruszalności znaków i urządzeń służących do ochrony granicy państwowej,
10. gromadzenie i przetwarzanie informacji z zakresu ochrony granicy państwowej i kontroli ruchu granicznego oraz udostępnianie ich właściwym organom państwowym,

[35] Dz. U. Nr. 128, poz. 1176 ze zm.

11. nadzór nad eksploatacją polskich obszarów morskich oraz przestrzeganiem przez statki przepisów obowiązujących na tych obszarach,
12. ochrona granicy państwowej w przestrzeni powietrznej RP przez prowadzenie obserwacji statków powietrznych i obiektów latających, przelatujących przez granicę państwową na małych wysokościach, oraz informowanie o tych przelotach właściwych jednostek sił powietrznych RP,
13. zapobieganie transportowaniu, bez zezwolenia wymaganego w myśl odrębnych przepisów, przez granicę państwową odpadów, szkodliwych substancji chemicznych oraz materiałów jądrowych i promieniotwórczych, a także zanieczyszczaniu wód granicznych,
14. zapobieganie przemieszczaniu bez zezwolenia wymagane w myśl odrębnych przepisów, przez granicę państwową środków odurzających i substancji psychotropowych oraz broni, amunicji i materiałów wybuchowych,
15. wykonywanie zadań określonych w innych ustawach[36].

Oprócz przedstawionych powyżej zadań organy Straży Granicznej zobowiązane są (na zasadzie wzajemności) do współpracy z organami administracji rządowej, jednostkami samorządu terytorialnego oraz państwowymi i innymi jednostkami organizacyjnymi. Celem takiego współdziałania powinno być zapewnienie niezbędnych warunków do wykonywania zadań w zakresie ochrony granicy państwowej i kontroli ruchu granicznego. Nie mniej ważnym obszarem działalności Straży Granicznej jest ciągła współpraca z organami ochrony granic innych państw, w tym z sąsiadami zza wschodniej granicy.

Centralnym organem administracji rządowej właściwym w sprawach ochrony granicy państwowej i kontroli ruchu granicznego jest Komendant Główny Straży Granicznej, podległy ministrowi właściwemu do spraw

[36] Przykładem takim jest chociażby możliwość prowadzenia przez Straż Graniczną postępowań w sprawach rozpoznawania, zapobiegania i wykrywania przestępstw, określonych w art. 228, 229, 231 Kodeksu karnego, popełnianych przez funkcjonariuszy i pracowników SG w związku z wykonywaniem obowiązków służbowych.

wewnętrznych. Powołuje i odwołuje go Prezes Rady Ministrów na wniosek ministra właściwego do spraw wewnętrznych.

Do zakresu działania Komendanta Głównego Straży Granicznej należy w szczególności:

- kierowanie prowadzonymi działaniami w zakresie ochrony granicy państwowej oraz kontroli ruchu granicznego,
- analizowanie zagrożeń bezpieczeństwa granicy państwowej,
- nadawanie regulaminów organizacyjnych komendom oddziałów oraz jednostkom organizacyjnym Komendy Głównej, a także nadawanie statutów ośrodkom szkolenia Straży Granicznej,
- organizowanie i określanie zasad szkolenia zawodowego funkcjonariuszy oraz pracowników SG
- sprawowanie nadzoru nad podległymi mu terenowymi organami oraz nad ośrodkami szkolenia,
- udział w przygotowaniu projektu budżetu państwa w zakresie dotyczącym Straży Granicznej, zgodnie z odrębnymi przepisami,
- współdziałanie w zakresie realizowanych zadań z właściwymi organami państwowymi, jednostkami samorządu terytorialnego i organizacjami społecznymi,
- prowadzenie współpracy międzynarodowej z organami i instytucjami właściwymi w sprawach ochrony granic państwowych.

Z kolei terenowymi organami Straży Granicznej są:

- komendanci oddziałów – powołuje i odwołuje minister spraw wewnętrznych,
- komendanci placówek – powołuje i odwołuje ich Komendant Główny Straży Granicznej.

Zarówno Komendant Główny Straży Granicznej, jak i organy terenowe są przełożonymi wszystkich podległych im funkcjonariuszy. Komendant Główny wykonuje swoje zadania przy pomocy podległego mu urzędu – Komendy Głównej Straży Granicznej.

Tabela 1 Struktura organizacyjna Komendy Głównej Straży Granicznej

Komendant Główny Straży Granicznej		
Zastępca Komendanta Głównego Straży Granicznej	Gabinet Komendanta Głównego Straży Granicznej	Zastępca Komendanta Głównego Straży Granicznej
Zarząd Operacyjno-Śledczy	Rzecznik Prasowy Komendanta Głównego Straży Granicznej	Biuro Łączności i Informatyki
Zarząd Graniczny	Zarząd Spraw Wewnętrznych Straży Granicznej	Biuro Techniki i Zaopatrzenia
Zarząd ds. cudzoziemców KG SD	Biuro Prawne	Biuro Finansów
Laboratorium Kryminalistyczne Straży Granicznej	Zespół Audytu Wewnętrznego KG SG	Samodzielny zespół Ds. Zamówień Publicznych
Biuro Analiz Strategicznych KG SG	Biuro Kadr i Szkolenia	Samodzielny Zespół Ds. Lecznictwa I Orzecznictwa
Archiwum	Biuro Współpracy Międzynarodowej	
	Inspektorat Nadzoru i Kontroli Komendanta Głównego Straży Granicznej	
	Biuro Ochrony Informacji Niejawnych Centrum Koordynacji Działań Straży Granicznej	

Źródło: opracowanie własne

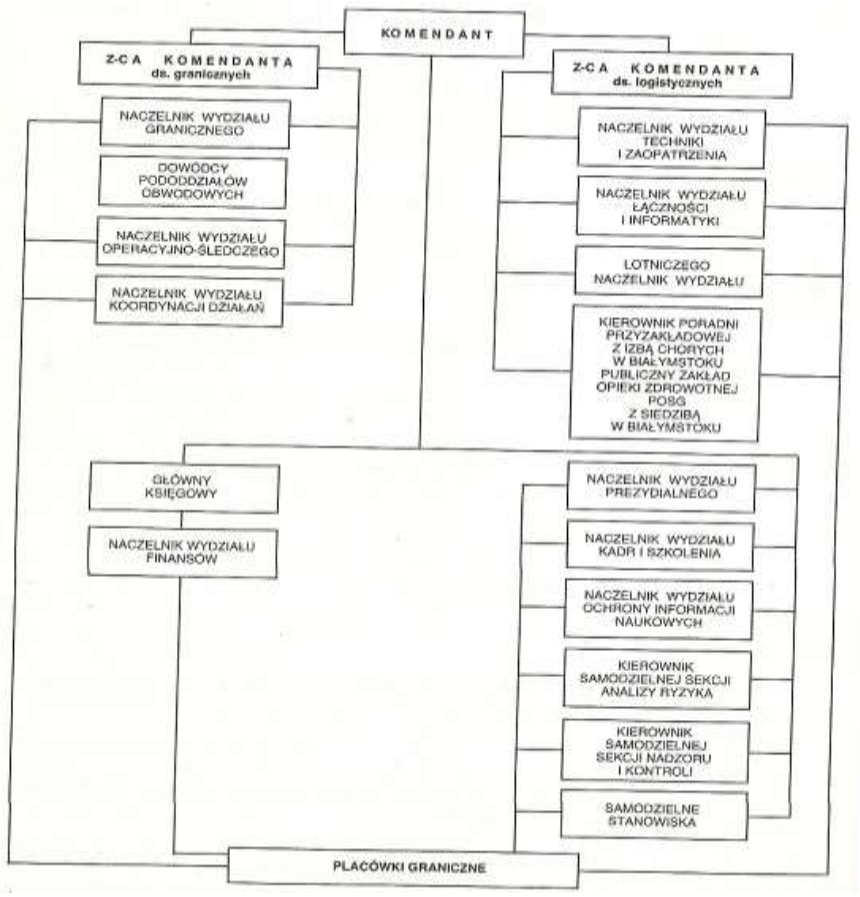
Komendanci oddziałów i placówek wykonują swoje zadania przy pomocy podległych im urzędów, tj. komend oddziałów, placówek, dywizjonów.

W gestii ministra właściwego do spraw wewnętrznych leży tworzenie i znoszenie oddziałów Straży Granicznej wraz z nadaniem im nazwy, określeniem siedziby oraz terytorialnego zasięgu działania. Natomiast Komendant Główny Straży Granicznej ma kompetencje w zakresie:

- tworzenia i znoszenia placówek oraz dywizjonów (na granicy morskiej), a także określania ich terytorialnego zasięgu działania,

- określania liczby i rodzajów etatów w jednostkach organizacyjnych Straży Granicznej,
- Stanowienia szczegółowych zakresów zadań terenowych organów Straży Granicznej oraz organizację Komendy Głównej, komend oddziałów, placówek i dywizjonów.

Rysunek 1. Struktura organizacyjna Komendy Oddziału Straży Granicznej (na przykładzie Podlaskiego Oddziału Straży Granicznej)



Źródło: http://www.podlaski.strazgraniczna.pl/struktura.htm (Polski Oddział Straży Granicznej, 25 listopada 2006 r.)

Rysunek 2. Lokalizacja jednostek organizacyjnych Straży Granicznej (oddziałów i ośrodków szkoleniowych)

Źródło: Komenda Główna Straży Granicznej

Rysunek 3. Lokalizacja oraz struktura organizacyjna granicznych jednostek organizacyjnych (na przykładzie Podlaskiego Oddziału Straży Granicznej na granicy państwowej z Litwą i Białorusią)

Źródło: http://www.posg.pl/struktura.asp (Podlaski Oddział Straży Granicznej, 25 stycznia 2006 r.)

W celu rozpoznawania, zapobiegania i wykrywania przestępstw i wykroczeń w zakresie określonym funkcjonariusze pełnią różne formy czynności służbowych, a mianowicie[37]:

- służbę graniczną,
- prowadzą działania graniczne, wykonują czynności operacyjno-rozpoznawcze,
- wykonują działania administracyjno-porządkowe,
- prowadzą postępowania przygotowawcze według przepisów Kodeksu postępowania karnego,
- wykonują czynności na polecenie sądu i prokuratury oraz innych właściwych organów państwowych w zakresie, w jakim obowiązek ten został określony w odrębnych przepisach,

Straż Graniczna w celu realizacji ustawowych zadań może korzystać z informacji o osobie, w tym danych osobowych uzyskanych przez uprawnione organy, służby i instytucje państwowe w wyniku wykonywania czynności operacyjno-rozpoznawczych lub prowadzenia kontroli operacyjnej, oraz przetwarzać je w rozumieniu ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych[38], bez wiedzy i zgody osoby, której dane dotyczą. Administrator danych jest obowiązany udostępnić dane, na podstawie imiennego upoważnienia Komendanta Głównego Straży Granicznej, komendanta oddziału lub upoważnionego funkcjonariusza.

Czynności operacyjno-rozpoznawcze podejmowane przez Straż Graniczną mają na celu, zapobieżenie, wykrycie, ustalenie sprawców oraz uzyskanie i utrwalenie dowodów, ściganych z oskarżenia publicznego, umyślnych przestępstw[39]:

- określonych w art. 264 Kodeksu karnego,
- określonych w art. 270-275 Kodeksu karnego w zakresie dokumentów uprawniających do przekraczania granicy państwowej,
- skarbowych, o których mowa w art. 134 & 1 pkt 1 Kodeksu karnego skarbowego, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznej przekraczają 50-krotną wysokość najniższego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów,

[37] Art. 9 ustawy o Straży Granicznej
[38] Tekst jedn. Dz. U. z 2002 r. Nr. 101, poz. 926 ze zm.
[39] Art. 9e ustawy o Straży Granicznej.

- pozostających w związku z przekraczaniem granicy państwowej lub przemieszczaniem przez granicę państwową towarów oraz wyrobów akcyzowych podlegających obowiązkowi oznaczania znakami akcyzy, jak również przedmiotów określonych w przepisach o broni, amunicji oraz o materiałach wybuchowych, a także o przeciwdziałaniu narkomanii,
- określonego w art. 147 ustawy z 13 czerwca 2003 r. o cudzoziemcach,
- określonych w art. 228, 229, 231 Kodeksu karnego, popełnionych przez funkcjonariuszy lub pracowników Straży Granicznej w związku z wykonywaniem obowiązków służbowych,
- ściganych na mocy umów międzynarodowych, gdy inne środki okazały się bezskuteczne albo zachodzi wysokie prawdopodobieństwo, że będą nieskuteczne lub nieprzydatne.

Czynności operacyjno-rozpoznawcze mogą także polegać na złożeniu propozycji nabycia, zbycia lub przejęcia przedmiotów pochodzących z przestępstwa, ulegających przepadkowi, albo których wytwarzanie, posiadanie, przewożenie lub którymi obrót są zabronione, a także przyjęcia lub wręczenia korzyści majątkowej.

Sąd okręgowy, na pisemny wniosek Komendanta Głównego Straży Granicznej, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, lub na pisemny wniosek komendanta oddziału Straży Granicznej, złożony po uzyskaniu zgody Komendanta Głównego Straży Granicznej i pisemnej zgody właściwego miejscowo prokuratora okręgowego, może, w drodze postanowienia, zarządzić kontrolę operacyjną. Pisemną zgodę komendantowi oddziału Straży Granicznej wydaje prokurator okręgowy właściwy ze względu na siedzibę tego komendanta.

Kontrola operacyjna jest prowadzona niejawnie i polega na:

- kontrolowaniu treści korespondencji
- kontrolowaniu zawartości przesyłek,
- stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w

szczególności obrazu treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych.

Kontrolę operacyjną zarządza się na okres nie dłuższy niż 3 miesiące. Sąd okręgowy może, na pisemny wniosek Komendanta Głównego Straży Granicznej lub komendanta oddziału Straży Granicznej, złożony po uzyskaniu pisemnej zgody Komendanta Głównego Straży Granicznej i właściwego prokuratora, na okres nie dłuższy niż kolejne 3 miesiące wydać postanowienie o jednorazowym przedłużeniu kontroli operacyjnej, jeżeli nie ustały przyczyny zarządzenia.

Funkcjonariusze wykonując zadania w ochronie granicy państwowej RP, mają prawo m. in[40]:

- dokonywania kontroli granicznej,
- dokonywania kontroli osobistej, a także przeglądania zawartości bagaży, sprawdzania ładunków w portach i na dworcach oraz w środkach komunikacji lotniczej, drogowej, kolejowej i wodnej w celu wykluczenia możliwości popełnienia przestępstw lub wykroczeń, zwłaszcza skierowanych przeciwko nienaruszalności granicy państwowej lub bezpieczeństwu w międzynarodowej komunikacji,
- dokonywania kontroli bezpieczeństwa na przejściach granicznych oraz w środkach komunikacji lotniczej, drogowej, kolejowej i wodnej w celu wykluczenia możliwości popełnienia przestępstw lub wykroczeń, zwłaszcza skierowanych przeciwko nienaruszalności granicy państwowej lub bezpieczeństwu w międzynarodowej komunikacji,
- pełnienia wart ochronnych na pokładzie statku powietrznego oraz stosowania niezbędnych środków, łącznie z użyciem środków przymusu bezpośredniego i broni służbowej, w celu unieszkodliwienia osoby, która stanowi bezpośrednie zagrożenie bezpieczeństwa lotu, zdrowia lub życia pasażerów lub członków załogi,

[40] Art. 11 ustawy o Straży Granicznej

- wydawania wiz i innych zezwoleń na przekroczenie granicy państwowej na podstawie odrębnych przepisów,
- legitymowania lub ustalania w inny sposób tożsamości osoby,
- zatrzymywania osób w trybie i przypadkach określonych w przepisach Kodeksu postępowania karnego i innych ustaw oraz doprowadzania ich do właściwego organu Straży Granicznej, sądu lub prokuratury,
- przeszukiwania osób, rzeczy, pomieszczeń i środków transportu w trybie i przypadkach określonych w przepisach Kodeksu postępowania karnego i innych ustaw,
- nakładania grzywien w drodze mandatu karnego za wykroczenia,
- obserwowania i rejestrowania, przy użyciu środków technicznych służących do rejestracji obrazu i dźwięku, zdarzeń na drogach oraz w innych miejscach publicznych,
- zatrzymywania pojazdów i wykonywania innych czynności z zakresu kontroli ruchu drogowego w trybie i przypadkach określonych w ustawie z 20 czerwca 1997 r. – Prawo o ruchu drogowym[41],
- zatrzymywania i cofania z granicy państwowej do nadawcy szkodliwych materiałów jądrowych i promieniotwórczych, środków chemicznych i biologicznych jak również odpadów,
- przebywania i poruszania się na gruntach bez uzyskiwania zgody ich właścicieli lub użytkowników oraz przechodzenia przez pola uprawne w czasie bezpośredniego pościgu, również z użyciem psa służbowego, jeżeli nie ma możliwości korzystania z dróg,
- żądania niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz jednostek gospodarczych prowadzących działalność w zakresie użyteczności publicznej, wymienione instytucje, organy i jednostki obowiązane są, w zakresie swojego działania, do udzielenia tej pomocy na podstawie obowiązujących przepisów prawa,

[41] Tekst jedn. Dz. U. z 2005, Nr. 108, poz 908 ze zm.

- zwracania się o niezbędną pomoc do innych jednostek gospodarczych i organizacji społecznych, jak również zwracania się w nagłych wypadkach do każdej osoby o udzielenie doraźnej pomocy, w ramach obowiązujących przepisów prawa[42].

Od kilku lat realizowany jest proces dostosowania systemu ochrony granicy do standardów wspólnotowych (ewaluacja). Podstawowym wymogiem członkostwa w Unii Europejskiej było przyjęcie przez Polskę dorobku prawnego UE wraz z dorobkiem Schengen, czyli Układu z Schengen z 14 czerwca 1985 r. i Konwencji Wykonawczej do Układu Schengen z 19 czerwca 1990 roku.

3. Kontrola graniczna osób

Według Kodeksu granicznego Schengen[43] kontrola graniczna oznacza wszystkie działania podejmowane na granicy, zgodnie z rozporządzeniem i do celów w nim określonych, wyłącznie w odpowiedzi na zamiar przekroczenia tej granicy lub na akt jej przekroczenia, bez względu na wszelkie inne okoliczności, składające się z odprawy granicznej oraz ochrony granicy. Z kolei odprawa graniczna została zdefiniowana jako czynności kontrolne przeprowadzane na przejściach granicznych w celu zapewnienia, że można zezwolić na wjazd osób, w tym ich środków transportu oraz przedmiotów będących w ich posiadaniu, na terytorium państw członkowskich lub można zezwolić na opuszczenie przez niego tego terytorium.

Należy podkreślić, iż kontrola graniczna leży w interesie nie tylko państwa, na którego granicach zewnętrznych jest ona dokonywana, ale w interesie wszystkich państw członkowskich, które zniosły kontrolę graniczną na granicach wewnętrznych. Zasadniczym celem kontroli granicznej powinna być pomoc w zwalczaniu nielegalnej imigracji i handlu ludźmi oraz zapobiegania wszelkim zagrożeniom dla bezpieczeństwa wewnętrznego, porządku publicznego, zdrowia publicznego i stosunków międzynarodowych UE. Natomiast sama już odprawa graniczna powinna być dokonywana w sposób zapewniający pełne poszanowanie godności osoby ludzkiej.

[42] W czasie wykonywania czynności służbowych z ochroną granicy państwowej funkcjonariusze mogą, na obszarze strefy nadgranicznej, korzystać nieodpłatnie ze środków komunikacji publicznej.
[43] Rozporządzenie (WE) nr. 562/2006 Parlamentu Europejskiego i Rady z 15 marca 2006 r. ustanawiające wspólnotowy kodeks zasad regulujących przepływ osób przez granice (Kodeks graniczny Schengen), Dz. Urz. WE L 105 z 13 kwietnia 2006 r., s. 1

Kontrola graniczna powinna być przeprowadzana profesjonalnie i z zachowaniem szacunku oraz powinna być proporcjonalna do założonych celów.

Cytowany wyżej Kodeks określa również kontrolę drugiej linii. Oznacza ona szczegółową odprawę, która może zostać przeprowadzona w odpowiednim miejscu, innym niż miejsce, w którym dokonywana jest odprawa wszystkich osób (pierwsza linia, czyli na przejściach granicznych).

Na granicy państwowej RP (zewnętrznej granicy UE), zgodnie z treścią art. 2 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 25 czerwca 2002 r. w sprawie kontroli granicznej dokonywanej przez funkcjonariuszy Straży Granicznej[44], kontrola graniczna osoby obejmuje przede wszystkim:

- sprawdzenie autentyczności i ważności dokumentu uprawniającego do przekroczenia granicy państwowej,
- stwierdzenie tożsamości na podstawie przedstawionego dokumentu uprawniającego do przekroczenia granicy państwowej,.
- ustalenie, czy osoba nie jest poszukiwana lub uprawnione organy nie zleciły wobec niej albo środka transportu, którym podróżuje, wykonania czynności określonych przepisami odrębnymi, a także wykonanie tych czynności,
- ustalenie, czy osoba, środek transportu, którym podróżuje, oraz przedmioty przez nią przewożone nie zagrażają bezpieczeństwu państwa, porządkowi publicznemu lub zdrowiu publicznemu,
- wykonanie czynności związanych z gromadzeniem danych z przeprowadzonej kontroli,

W ramach czynności kontroli granicznej sprawdzana jest ponadto autentyczność i ważność wiz lub innych zezwoleń, jeżeli są wymagane, następuje kontrola spełnienia warunków wjazdu na terytorium RP oraz sprawdza się, czy opuszczenie terytorium kraju następuje przed upływem okresu ważności wizy lub terminu pobytu określonego na podstawie przepisów odrębnych. Należy dodać, iż kontroli granicznej towarzyszy kontrola osobista, a także przeglądanie zawartości bagaży, środka transportu oraz

[44] Dz. U. Nr. 96, poz. 862 ze zm.

przewożonego ładunku, w razie istnienia uzasadnionego podejrzenia popełnienia przez osobę przekraczającą granicę czynu zabronionego pod groźbą kary[45].

Uwiarygodnienie przeprowadzenia kontroli granicznej może być potwierdzone przez odciśnięcie stempla kontrolerskiego na dokumencie uprawniającym do przekroczenia granicy państwowej. Stempel kontrolerski zawiera litery PL, nazwę przejścia granicznego, datę, numer oraz graficzne oznaczenie rodzaju ruchu granicznego i jego kierunku. Zamieszcza się go na dokumentach podróży cudzoziemców, na dokumentach obywateli Polski uprawniających do przekroczenia granicy państwowej na ich wniosek.

Nie ma obowiązku zamieszczania odcisku stempla kontrolerskiego na dokumentach uprawniających do przekroczenia granicy państwowej przedstawicieli państw i organizacji międzynarodowych, których przyjazd był zgłoszony drogą dyplomanta, oraz na dokumentach uprawniających załogi statków morskich do przekroczenia granicy państwowej, jeżeli podczas pobytu statku w porcie na terytorium Polski schodzą na ląd, bez opuszczenia miasta portowego.

Kontrola graniczna osoby może być ograniczona do czynności, o których mowa w & 2 ust 1 pkt 1 i 2 oraz ust 2 pkt 1 i 4 cytowanego wyżej rozporządzenia. Ograniczenia zakresu kontroli granicznej nie stosuje się, jeżeli istnieje uzasadnione podejrzenie, że osoba podlegająca kontroli granicznej stanowi zagrożenie dla bezpieczeństwa państwa, porządku publicznego lub zdrowia publicznego.

Można ją też uprościć lub dokonywać jej wyrywkowo. Ma to zazwyczaj miejsce w przypadku, gdy w następstwie wzrostu ruchu granicznego, mimo wykorzystania wszystkich możliwości organizacyjnych, czas na przekroczenie granicy państwowej nadmiernie wzrasta. Wyrywkowego dokonywania kontroli nie stosuje się, jeżeli wobec osoby wielokrotnie przekraczającej granicę państwową uprawnione organy zleciły czynności określonych odrębnymi przepisami, a także wówczas, gdy osoba ta jest poszukiwana listem gończym.

Kontrola graniczna osób posiadających paszporty dyplomatyczne lub paszporty zaopatrzone w wizy dyplomatyczne prowadzona jest z uwzględnieniem prawa międzynarodowego, zawartych umów i zwyczajów międzynarodowych. Ta forma kontroli dotyczy także członków międzynarodowych zespołów inspekcyjnych

[45] Kontrolę graniczną może uprościć lub dokonywać jej wyrywkowo u osób, które w tym samym dniu wielokrotnie przekraczają granicę państwową.

przekraczających granicę państwową w związku z realizacją zobowiązań międzynarodowych wynikających z:

1. Traktatu o konwencjonalnych siłach zbrojnych w Europie, podpisanego w Paryżu 19 listopada 1990 r. (dz. U z 1995 r. Nr. 15, poz 73),
2. Traktatu o otwartych przestworzach , sporządzonego w Helsinkach 24 marca 1992 r. (Dz. U. z 2001 r. Nr 103, poz. 1127),
3. Konwencji o zakazie prowadzenia badań, produkcji, składowania i użycia broni chemicznej oraz o zniszczeniu jej zapasów, sporządzonej w Paryżu 13 stycznia 1993 r. (Dz. U. z 1999 r. Nr 63, poz 703) – niezależnie od dokumentów uprawniających te osoby do przekroczenia granicy państwowej.

Stosownie do zasad wynikających z umów międzynarodowych wiążących RP oraz przyjętych zwyczajów kontroli granicznej dokonuje się poza kolejnością, w szczególności wobec:

1. będących w akcji pojazdów straży pożarnej, sanitarnych oraz osób uczestniczących w akcjach ratowniczych,
2. osób posiadających paszporty dyplomatyczne lub paszporty zaopatrzone w polskie wizy dyplomatyczne,
3. osób niepełnosprawnych z widocznym kalectwem, w podeszłym wieku oraz osób z małym dzieckiem na ręku,
4. osób podróżujących regularną międzynarodową komunikacją autobusową,
5. pojazdów przewożących żywe zwierzęta, towary łatwo psujące się lub niebezpieczne.

Kontroli osobistej osób nie dokonuje się obligatoryjnie. Czyni się to tylko w przypadku:

1. zatrzymania osoby, co do której zachodzi uzasadnione podejrzenie, że popełniła przestępstwo lub wykroczenie,
2. doprowadzenia do pomieszczeń służbowych osoby ujętej w związku z uzasadnionym podejrzeniem popełnienia przestępstwa lub wykroczenia,
3. ujawnienia rzeczy przy osobie,, które mogą stanowić zagrożenie bezpieczeństwa w komunikacji międzynarodowej.

Przeprowadza się ją w wydzielonym do tego celu pomieszczeniu, niedostępnym dla osób trzecich, oraz przez osoby tej samej płci. Przed przystąpieniem do kontroli osobistej uprzedza się osobę, która ma być poddana tej kontroli. Jednocześnie powiadamia się ją jednocześnie o możliwości przeprowadzenia kontroli w obecności osoby trzeciej. Na żądanie osoby poddawanej kontroli osobistej kontroli tej dokonuje się w obecności osoby trzeciej.

Sprawdzenia ładunku przemieszczanego lub przeznaczonego do przemieszczenia przez granicę państwową można dokonać w miejscu jego składowania, a także podczas jego załadowania, rozładowania lub przeładowania oraz w środku transportowym. Czynności te dokonuje się w obecności właściciela, przewoźnika lub spedytora. Sprawdzenia ładunku znajdującego się pod zamknięciem celnym dokonuje się w obecności funkcjonariusza urzędu celnego. Sprawdzenia ładunku przy użyciu środków technicznych oraz psów służbowych dokonuje się w sposób niepowodujący jego uszkodzenia[46].

Kontrola graniczna na przejściach drogowych przeprowadzana jest bezpośrednio na pasach ruchu:

1. w autobusie – osób podróżujących autobusami,
2. przy pojeździe – osób podróżujących pojazdami innymi niż autobus, bez konieczności opuszczania go przez osoby podróżujące,
3. przy stanowiskach kontroli na wyznaczonych pasach ruchu – osób przekraczających granicę pieszo.

Kontrola graniczna na przejściach kolejowych jest wykonywana w czasie postoju pociągu na stacji kolejowej lub w czasie jazdy pociągu na wyznaczonych odcinkach linii kolejowych. Dokonywanie kontroli w czasie jazdy pociągu może być uzależnione od rozdzielenia osób podróżujących w komunikacji międzynarodowej od osób podróżujących w komunikacji krajowej.

Kontrolę graniczną osób odbywających loty międzynarodowe przeprowadza się:

1. na przejściach lotniczych portu lotniczego na wyznaczonych i odpowiednio oznaczonych pasach ruchu. W uzasadnionych przypadkach może ona być dokonana na pokładzie statku powietrznego albo przy zejściu lub wejściu na jego pokład,

[46] Ibidem

2. podróżujących statkiem powietrznym odbywających lot:
    a) z zagranicy, z międzylądowaniem na terytorium RP, jeżeli nie następuje zmiana statku i nie dosiadają się inni pasażerowie, dokonuje się jej na terytorium RP, na lotnisku dla nich docelowym,
    b) za granicę, z międzylądowaniem na terytorium RP, jeżeli nie następuje zmiana statku i na terytorium Polski nie dosiadają się inni pasażerowie, dokonuje się jej na lotnisku ich wyjazdu,
    c) z zagranicy, które kontynuują podróż na liniach krajowych, dokonuje się jej na lotnisku lądowania statku powietrznego z zagranicy,
    d) przesiadających się z lotu na linii krajowej na lot za granicę, dokonuje się jej na lotnisku, z którego statek odlatuje za granicę,
3. podróżujących tranzytem lotniczym przez terytorium RP, zmieniających statek powietrzny, dokonuje się jej tylko w przypadku opuszczenia strefy tranzytowej portu lotniczego[47].

Kontroli granicznej osób podróżujących statkami morskimi oraz członków załóg tych statków dokonuje się w wyznaczonych pomieszczeniach morskiego przejścia granicznego. Można jej dokonać także na pokładzie statku podczas zawijania do portu lub w czasie rejsu. Obejmuje ona w szczególności.

1. odebranie listy załogi i listy pasażerów, przy wjeździe na terytorium RP,
2. porównanie listy załogi i listy pasażerów ze stanem faktycznym załogi i pasażerów, przy wyjeździe z terytorium RP,
3. odebranie od kapitana statku polskiego zgłoszenia wyjścia, przy wyjeździe z terytorium RP i zgłoszenie wejścia, przy wjeździe na terytorium RP.

Kontroli granicznej załóg jednostek rybackich dokonuje się według zasad jak wyżej. Od polskich jednostek rybackich nie wymaga się zgłoszenia wyjścia przy wyjeździe z terytorium RP i zgłoszenia wejścia przy wjeździe na terytorium RP. W przypadku gdy jednostki te nie zawijają do obcych portów lub nie wypływają poza

[47] Zbigniew B. Kumoś: *Granice Rzeczpospolitej Polskiej : (na przestrzeni dziejów)*. Warszawa: Wydawnictwo Comandor, 2005, s. 74

polską wyłączną strefę ekonomiczną, kontrola graniczna może być dokonywana wyrywkowo.

Kontroli granicznej osób przekraczających granicę państwową jednostkami żeglugi śródlądowej oraz członków ich załóg dokonuje się w rzecznych przejściach granicznych na pokładzie tych jednostek. Od kapitana statku żeglugi śródlądowej nie wymaga się listy załogi i listy pasażerów. Może być dokonywana:

1. na postoju, w wyznaczonym miejscu przystani rzecznej lub portu rzecznego, w odpowiednio przystosowanych pomieszczeniach,
2. na postoju w nurcie rzeki lub kanału, na pokładzie jednostki,
3. w czasie rejsu na określonym odcinku śródlądowej drogi wodnej[48].

Kontroli granicznej żołnierzy jednostek wojskowych Sił Zbrojnych RP przekraczających granicę państwową, dokonuje się w sposób uproszczony. Może być ograniczona do odebrania listy żołnierzy zawierającej dane personalne oraz numery dokumentów uprawniających do przekroczenia granicy państwowej, poświadczonej przez uprawniony organ wojskowy.

Są też okoliczności, kiedy dopuszcza się możliwość odstąpienia od kontroli granicznej lub też dokonuje się jej w sposób ograniczony. Ma to miejsce w przypadku przyjęcia zgłoszenia zamiaru przekroczenia granicy państwowej przez:

1. załogi statków Morskiej Służby Poszukiwania i Ratownictwa Okręgowego i Państwowej Straży Pożarnej, wychodzące w morze w związku z akcją ratowniczą,
2. załogi statków ratownictwa morskiego innych państw znajdujące się w polskich portach, wychodzące w morze w związku z akcją ratowniczą,
3. załogi pojazdów i statków powietrznych służb policyjnych państw sąsiednich uczestniczących w akcjach, których celem jest ochrona życia lub zdrowia,
4. członków załóg i osoby podróżujące polskimi statkami handlowymi, pasażerskimi i specjalnymi między portami polskimi oraz po Morzu Bałtyckim bez zawijania do obcych portów,

[48] Ibidem

5. członków załóg statków budowanych lub remontowanych w stoczniach znajdujących się na terytorium RP odbywających próbne rejsy bez zawijania do obcych portów,
6. członków załóg i pasażerów statków obcych podróżujących między portami polskimi, w przypadku gdy wobec osób tych została dokonana kontrola graniczna przy wjeździe na terytorium Rzeczypospolitej Polskiej,
7. załogi okrętów wojennych i statków powietrznych Sił Zbrojnych RP,
8. załogi okrętów wojennych i statków powietrznych państw obcych wykonujących zadania w ramach wiążących RP umów międzynarodowych i porozumień.

Od 1 maja 2004 r. na granicach wewnętrznych (ze Słowacją, Czechami, Litwą i Niemcami) wobec obywateli państw UE i EOG, w ruchu osobowym, kontrola graniczna z reguły ogranicza się do kontroli wzrokowej wolno przejeżdżających samochodów, bez ich zatrzymywania. Służby graniczne mogą przeprowadzić, wyrywkowe, dokładniejsze kontrole podróżnych, poza pasami ruchu. Zmieniły się również zasady kontroli obowiązkowego ubezpieczenia komunikacyjnego OC. Od obywateli Unii i EOG, Szwajcarii oraz Chorwacji w czasie przekraczania granicy państwowej nie jest wymagane okazywanie obowiązkowego ubezpieczenia. Obywatele pozostałych państw przy wjeździe na terytorium Polski powinni posiadać i okazywać na żądanie uprawnionych organów dokument stwierdzający zawarcie umowy obowiązkowego ubezpieczenia odpowiedzialności cywilnej posiadacza pojazdu lub stwierdzające opłacenie składki tego ubezpieczenia (tzw. Zieloną Kartę).

Rozdział III

Ochrona informacji niejawnych

1. Istota ochrony informacji

Wszyscy spotkali się kiedyś z ogólnym lub dokładniejszym wyjaśnieniem pojęcia informacja. Nie warto w tym miejscu przytaczać określonej definicji podawanych przez uczonych zajmujących się teorią informacji lub cybernetyką, aczkolwiek warto podkreślić rolę informacji, ich wszechobecność w życiu społecznym, gospodarczym i w wojsku.

Tak więc informacja to znaczenie przypisywane danym, z uwzględnieniem konwencji stosowanych do ich wyrażenia. Istnieje też lapidarne określenie: informacja to wiadomość mająca postać danych. Natomiast dane to reprezentacja faktów lub pojęć przekazanych w sposób sformalizowany.

W informatyce postać danych (np. zapisanych na kartkach dziurkowanych) powinna umożliwiać automatyczne przekazywanie (wczytanie) ich do maszyn cyfrowych[49].

Informacje o różnorodnych zjawiskach przyrody, celowym działaniu ludzi, w tym również o charakterze gospodarczym lub wojskowym, tworzą czy też wypełniają krąg informacji społecznych. Bez ciągłego obiegu i przetwarzania informacji nie mogłoby istnieć zorganizowane życie człowieka, całego społeczeństwa. A więc informacja społeczna jest niezbędna w każdym działaniu, dodając w działaniu racjonalnym, a zatem i w zarządzaniu gospodarką narodową, czy też w dowodzeniu wojskami[50].

Działalność ludzi determinowana jest informacją społeczną i ogólnie pojętą percepcją. Informację taką określamy jako wszelkie wiadomości występujące w sferze doświadczenia, wiedzy i świadomości, a więc uzyskane i przetworzone w toku szeroko pojętej praktyki ludzkiej. Wszystkie rodzaje informacji takie jak : ekonomiczne (gospodarcze), techniczne, naukowe, polityczne, wojskowe itd. stanowią części informacji społecznej, a podział powstał jedynie ze względu na treść grupowanych wiadomości czy też w oparciu o pewne ich cechy.

Mówiąc wprost – informacje krążą w społeczeństwie, a docierając do ludzi stają się ważnym elementem procesów społecznych.

---

[49] Szaniawski K., hasło Informacja w: Filozofia a nauka, 1987, s. 244.
[50] Lissowski G., hasło Informacja, w: Wielka Encyklopedia Powszechna, 2002, s. 126.

Traktując je w ten sposób można zauważyć, że stanowią one istotny czynnik organizowania i kierowania tymi procesami. O roli informacji jako znaczącego elementu w społeczeństwie świadczy wzrost znaczenia i możliwości różnych form celowego oddziaływania na procesy informacyjne przenikające gospodarkę, wspomagających poznawanie przez ludzi naukowego światopoglądu, orientowania się w zjawiskach i życiu społecznym[51].

Nie warto tu rozgraniczać informacji na gospodarcze i wojskowe. Trzeba przede wszystkim podkreślić znaczenie informacji, a następnie podać podstawowe czynniki, które warunkują konieczność jej ochrony w systemach komputerowych.

Mówiąc inaczej, chodzi o zarysowanie tych funkcji informacji, a właściwie pewnego jej zakresu, który ze względów gospodarczych lub państwowych musi być chroniony. Trzeba również sobie uświadomić, że współcześnie przeciętnie 15-20% wszystkich informacji w różnym stopniu podlega ochronie, to łatwo zrozumieć, jak ważny jest, przy znacznym już obecnie zastosowaniu maszyn cyfrowych, to problem[52].

Zrozumiałe, że informacje mają podobne, a w wielu przypadkach niewspółmierne większe znaczenie w wojsku, zwłaszcza w dowodzeniu. Dowodzenie wojskami czy siłami granicznymi jest procesem, w którym nieustannie przetwarza się informacje, w wyniku czego określa się wojska własne, ich działanie oraz wojska przeciwnika. W takich sytuacjach należy operować pojęciem: systemy informacyjne. System taki można zdefiniować jako układ umożliwiający rejestrowanie, przetwarzanie i udostępnianie lub przekazywanie informacji.

W systemach informacyjnych lub określonych podsystemach (np. w podsystemie ewidencyjno-sprawozdawczym) – w Straży Granicznej od dawna zaczęto stosować elektroniczne maszyny cyfrowe (EMC).

Zastosowanie maszyn cyfrowych, głównie w gospodarce, a w wojsku w znacznej części, odbywa się właśnie w sferze obiegu informacji, a więc w ramach istniejących już systemów informacyjnych, modyfikując często strukturę tych systemów. Takie zastosowanie może mieć miejsce np. w systemie informacyjnym przedsiębiorstwa, instytucji lub oddziału gospodarczego. Powstają wówczas zautomatyzowane systemy zarządzania (dowodzenia), a mówiąc dokładniej, systemy informatyczne zarządzania[53].

[51] Kowalczyk E., O istocie informacji, 1981, s. 18.
[52] Mynarski S, Elementy teorii systemów i cybernetyki, 1979, s. 141
[53] Boruń K., hasło Informacja, w: Mały słownik cybernetyczny, pod red. M. Kempisty, 1973, s. 155.

Współczesne potrzeby informacyjne w dowodzeniu wojskami, ograniczony czas podejmowania decyzji oraz konieczność szybkiego przetwarzania dużych ilości informacji stwarzają potrzebę stosowania maszyn cyfrowych na wszystkich szczeblach dowodzenia. W znacznym stopniu inny więc zakres informacji jest przetwarzany w zautomatyzowanych systemach dowodzenia. Systemy te umożliwiają doskonalenie zbierania, przetwarzania i przekazywania niezbędnych informacji w dowodzeniu wojskami, przyczyniają się też do usprawnienia funkcjonowania samych organów dowodzenia[54].

2. Uwarunkowania społeczne i prawne ochrony informacji

Uwarunkowania społeczne i prawne ochrony informacji określone są istniejącymi normami prawnymi i przepisami wewnętrznymi, które dotyczą informacji niejawnych, jak też innych, zaliczonych do dóbr osobistych. A zatem również informacje przetwarzane za pomocą komputera, w stosunku do których obowiązują te uwarunkowania, powinny być chronione.

Śledząc rozwój elektronicznej techniki obliczeniowej można zauważyć, że jeszcze przed pierwszymi przypadkami infiltracji stosowano pewne sposoby ochrony informacji. Zapobiegały one przypadkowym zniszczeniom lub błędom (przekłamaniom). Temu właśnie służyło wprowadzenie np. bitów parzystości (kontrola poprawności zapisu lub odczytu informacji) lub etykiety zbiorów (kontrola użycia właściwego zbioru), a w tym takich informacji, jak data zapisu lub numer generacji (ochrona przed przedwczesnym skasowaniem zbioru, kontrola aktualności zbioru).

Wymienione i inne sposoby programowe, organizacyjne, w znacznej mierze chronią zbiory informacji przed przypadkowym zniszczeniem lub przekłamaniem. Z chwilą jednak ujawnienia pierwszych przypadków infiltracji okazały się one niewystarczające, ponieważ nie były przewidziane do ochrony przed działaniem osób nie upoważnionych. Dotychczasowe zatem sposoby ochrony mogą być w stosunkowo prostych działaniach omijanie przez osoby nieupoważnione. W niektórych

[54] Głuszkow W., Wstęp do cybernetyki, 1967, za: J. L. Kulikowski, Informacja i świat w którym żyjemy, 1978, s. 43.

przypadkach, np. podczas niedozwolonej modyfikacji programów działania tych osób nie napotykają prawie żadnych przeszkód[55].

Możliwość działania osób nie upoważnionych (infiltracji), a przede wszystkim potrzeba przetwarzania zbiorów informacji zastrzeżonych dla określonego użytkownika lub grupy użytkowników, w tym zbiorów tajnych, to podstawowa przyczyna konieczności ochrony tych zbiorów.

Obok oczywiście szkodliwej infiltracji pojawiają się inne, również niebezpieczne zjawiska jak możliwość utraty zaufania do niektórych systemów informatycznych lub obawa przed manipulowaniem informacjami o obywatelach przez osoby nieupoważnione.

W niekorzystnej sytuacji na wymienione zjawiska mogą się nałożyć różne konflikty powstające w czasie wdrażania systemu informatycznego lub podczas eksploatacji systemu[56].

Wymienione, w różnym stopniu negatywne zjawiska, wchodzące w sferę informacji i komunikowania się w społeczeństwie, tworzą różne, w znacznej mierze nowe uwarunkowania społeczne i prawne ochrony informacji w systemach.

Informacja jako niezbędny czynnik całej sfery życia społecznego ma charakter społeczny. Mówiąc wprost informacje krążąc w społeczeństwie, docierając do ludzi, stają się elementem procesów społecznych. Stanowią więc istotny czynnik organizowania procesów społecznych i sterowania nimi. Rola informacji jako elementu procesów społecznych wyraża się w tym, „że coraz większego znaczenia nabierają dociekania na temat możliwości oraz form celowego i zorganizowanego oddziaływania na procesy informacyjne”[57].

Jeśli informacje są ważnym elementem inspirowania procesów społecznych, organizowania i sterowania nimi, to istnieją pewne uwarunkowania czy też ograniczenia w dostępności do niektórych. Dostępność ta wynika głównie ze zróżnicowania lub selekcjonowania informacji.

Fakt istnienia zróżnicowania informacji, i to nie tylko w odniesieniu do jej treści, ale przede wszystkim do różnych kręgów odbiorców, warunkuje konieczność

[55] Zaistniałe przypadki infiltracji wskazują, że znaczna ich część dotyczyła właśnie tego typu działań, tzn. niedozwolonych modyfikacji. Co istotniejsze zazwyczaj działania takie przez dłuższy czas nie były wykrywane.

[56] Konflikty te rozumie się jako sprzeczności między ludźmi wchodzącymi w skład organizacji albo między ludźmi a systemem formalnym. Prezentację konfliktów powstających podczas zastosowania maszyn cyfrowych podanow pracy W. Askanas, Konflikty organizacyjne przy wdrażaniu ETO, Warszawa 1978

[57] Szulczewski M., Polityka informacji, Warszawa 1977, s. 14

ochrony niektórych informacji. Ograniczając zagadnienie jedynie do indywidualnych informacji o obywatelach, gromadzonych w ramach obiektowych systemów informatycznych lub w systemach rządowych, np. Magister[58], nietrudno zauważyć społeczną oraz prawną konieczność określonej, selektywnej ochrony tych informacji.

Oczywiste są też uwarunkowania ochrony (w różnym zakresie) informacji statystycznych, finansowych, gospodarczych, technicznych i wojskowych.

Ochrona określonych informacji statystycznych wynika z ustawowej odpowiedzialności za zachowanie ich poufności. Konieczna jest tu ochrona zarówno informacji o obywatelach (ochrona prywatności zapisów statystycznych), jak też dotycząca gospodarki, techniki i innych dziedzin życia.

Zróżnicowana ochrona znacznej części informacji finansowych jest konieczna nie tylko ze względu na możliwości zapoznania się z nimi, ale przede wszystkim z uwagi na to, że może nastąpić niedozwolona ich modyfikacja. Informacje finansowe, w tym z zakresu rachunkowości, są wyjątkowo podatne na tego rodzaju działania. Brak ochrony lub niedostateczny jej poziom z jednoczesną możliwością niedozwolonych modyfikacji w skrajnym przypadku prowadzi, oprócz ujawnienia do defraudacji, którą niejednokrotnie trudno wykryć.

Zachowanie tajemnicy państwowej i służbowej obliguje do stosowania ochrony określonych informacji gospodarczych i informacji w systemach rządowych. Natomiast w wojskowych systemach informatycznych, ze względu na znaczenie dla ochronności kraju, na ogół wszystkie one wymagają ochrony.

Stosunkowo dobrze wyodrębnioną dziedzinę ochrony stanowią informacje osobowe (dane osobowe), czyli dotyczące prywatnej sfery życia obywateli tzw. Dobra osobiste. Przepisy prawa chronią naruszenie dóbr osobistych takich jak życie, nietykalność cielesną, wolność, tajemnicę korespondencji itd.

Współcześnie w systemach informatycznych pod ochroną prawa znalazły się informacje dotyczące np. sfery życia prywatnego i inne. Dobra osobiste chroni polskie prawo cywilne (art. 23, 24 i inne k.c.), niezależnie od innych przepisów, np. prawa karnego i administracyjnego. „Chodzi tu o problematykę związaną z ochroną praw podmiotowych w sferze życia osobistego oraz z ochroną interesu ogólnego przed

[58] Magister – rządowy system informatyczny dotyczący ewidencjonowania pracowników gospodarki narodowej z wyższym wykształceniem w calu usprawnienia wykorzystania kadr.

różnymi zagrożeniami. Mogą one polegać na niedozwolonej zmianie, zaginięciu, zniekształceniu, zniszczeniu i wreszcie na kradzieży danych osobowych”[59].

Pełny wykaz dóbr osobistych, przy nie dość wyrazistej ich granicy, trudno sprecyzować. Można więc przyjąć, że niektóre dane personalne przetwarzane w systemach informatycznych powinny być chronione na mocy prawa obejmującego dobra osobiste. Obecnie brak regulacji prawnej dotyczącej powstawania, kontroli czy też nadzoru ze strony państwa nad tego typu systemami. Można przypuszczać, że dla obywatela skutki wynikające z tego co o nim wiedzą w przedsiębiorstwie na podstawie systemu informatycznego, mogą być znacznie dotkliwsze niż w przypadku systemów rządowych.

Skutki wynikające dla obywateli z braku ochrony mogą być wielorakie, doraźne i dalekosiężne. Sfałszowanie, np. niektórych treści danych personalnych, może przynieść szkodę, a w innych przypadkach nieuzasadnione korzyści osobie, które taki zapis dotyczył. Powstają jednocześnie skutki o szerszym społecznym zasięgu, podważanie zaufania obywateli zarówno do systemu informatycznego, jak i przedsiębiorstwa[60].

W zakresie uwarunkowań prawnych ochrony informacji przetwarzanych w systemach można wyodrębnić następujące zagadnienie: przed jakimi działaniami lub, mówiąc wprost, przed jakimi przestępstwami należy stosować ochronę i jak je określić. W literaturze przedmiotu podaje się różne określenia, np. przestępstwa komputerowe, nadużycia lub defraudacje komputerowe.

Wydaje się, że oprócz określenia „infiltracja” można też stosować „przestępstwo informatyczne”, co oznacza grupę przestępstw, w którym przedmiotem zamachu są określone elementy (wartości) systemów informatycznych. Przestępstwa te można podzielić na dwie grupy:

1. dokonane przy wykorzystaniu informacji przetwarzanych w systemie czyli przez niewłaściwe ich użycie, celowe przekłamanie lub zniszczenie,
2. przeciwko sprzętowi, czyli majątkowe lub sabotażowe.

W niektórych krajach, w tym i w Polsce, od dawna prowadzi się dyskusje nad uregulowaniem prawnym w zakresie przestępstw informatycznych, jak też innych

[59] Sobczak K., Prawo a informatyka, Warszawa 1978, s. 103

[60] Zob. Kulikowski J., L., Organizacyjne i techniczne aspekty ochrony danych w systemach informatycznych [w:] Prawne problemy systemów informatycznych. Materiały Konferencji Informatyki Prawniczej, t. 1 z. 2, Wrocław 1976, s. 11

zagadnień związanych z zastosowaniem maszyn cyfrowych. Zespół norm prawnych odnoszących się przede wszystkim do przestępstw informatycznych, a następnie do podstawowych uregulowań merytoryczno-formalnych funkcjonowania systemów informatycznych, zwłaszcza przetwarzających dane o obywatelach, określa się jako informatyczne.

Całość tych zagadnień, dotyczących w konsekwencji różnorakich sfer życia społecznego i gospodarczego, jest trudna do uregulowania[61]. Obecnie tylko kilka państw na świecie wprowadziło prawo informatyczne o szerszym lub węższym oddziaływaniu[62].

Akty prawne są znaczącą barierą w dokonywaniu przestępstw informatycznych. Brak jednak pełnego uregulowania prawnego nie zwalnia informatyków, jak i użytkowników, od stosowania środków ochrony informacji.

Komputeryzacja w określonym zakresie jest procesem społecznym, który niesie pozytywne, ale też i negatywne skutki, w tym konflikty w samych jednostkach organizacyjnych oraz ich otoczeniu. „Jeśli zapewni się skuteczną kontrolę, komputer nie będzie ani groźbą, ani zbawieniem, lecz po prostu niesłychanie cenną maszyną, która powinna pomóc w dążeniu do lepszego życia"[63].

3. Konieczność ochrony informacji

Od wieków szczególne zainteresowanie informacjami gospodarczymi, wojskowymi itp. przejawiają niektóre osoby nie upoważnione do korzystania z nich. Nieustannie poszukuje się więc sposobów ochrony informacji, np. znano od dawna utajnianie za pomocą szyfrowania.

Zastosowanie maszyn cyfrowych do przetwarzania informacji zrodziło nowy problem, konieczność ochrony informacji w systemach informatycznych. Obecnie wzrosła znacznie różnorodność zagrożeń informacji. Jest to zrozumiałe przede wszystkim dlatego, że w systemach tych gromadzi się informacje w sposób odmienny niż przy stosowaniu innych technik przetwarzania. Zbieranie, przechowywanie, przetwarzane i przesyłane informacje w systemach informatycznych dotyczą często

[61] W obowiązującym od 1 stycznia 1970 r. kodeksie karnym brak jednoznacznego przepisu który odnosiłby się do przestępstw informatycznych.
[62] Spośród państw europejskich prawo informatyczne wprowadzono w Szwecji, RFN, a prace przygotowawcze prowadzi się w Austrii. Wielkiej Brytanii i Francji.
[63] Wessel M, R., Komputer i społeczeństwo, Warszawa 1976, s. 31

różnych dziedzin życia gospodarczego czy też istotnych spraw wojska. Ponadto są one sukcesywnie, a niekiedy nawet na bieżąco, aktualizowane podczas przetwarzania w ośrodku obliczeniowym.

Łatwo zatem zrozumieć, na jak znaczne niebezpieczeństwo, ze względu na możliwość działania osób nie upoważnionych, narażony jest proces automatycznego przetwarzania informacji, szczególnie gospodarczych i wojskowych. Dlatego wszelkie zakłócenia informacji, jak kradzież, zniszczenie czy przekłamanie umyślne lub przypadkowe mogą prowadzić do nieobliczalnych skutków.

Pierwszy przypadek nadużycia za pomocą systemu informatycznego wydarzył się w 1966 r. w Stanach Zjednoczonych[64], Programista zmodyfikował odpowiednio program, dzięki czemu możliwe było realizowanie jego czeków bez pokrycia. Wykryto to dopiero po trzech miesiącach, gdy komputer się zepsuł. Fakt ten dowodzi, że wykrycie działania osób nie upoważnionych w systemach informatycznych jest wyjątkowo trudne. Wpływa na to przede wszystkim odmienny, w porównaniu do systemów tradycyjnych sposób rejestracji i przetwarzania informacji. Komputer, jako bardzo szybkie urządzenie liczące w zasadzie nie rejestruje w czasie liczenia wszystkich operacji pośrednich, występujących, np. w tradycyjnej księgowości, lecz podaje od razu ostateczny wynik. Znikają więc etapy pośrednie, których kolejne kontrolowanie umożliwia wykrycie nadużycia. Dlatego też większość przypadków szpiegostwa komputerowego lub oszustw (przekłamania informacji) wykrywa się obecnie przypadkowo (podczas różnych działań sprawdzających funkcjonowanie systemu) lub na skutek błędu popełnionego przez oszusta. Potwierdzają to choćby badania przeprowadzone w RFN. Wykazały one, że około 90% wypadków oszustw w dziedzinie informatyki ujawnia się w czasie przypadkowej weryfikacji zbiorów, albo wskutek fałszywego kroku oszusta.

Do klasycznych należą oszustwa dokonywane na listach płac, np. znane są przypadki pozostawienia zapisu zwolnionych pracowników i przelewanie ich poborów (po małej „korekcie" programu, zmianie numeru konta) na kontro nieuczciwego informatyka. Inny przykład to zwiększeni4, po wcześniejszej modyfikacji programu, obliczonej wielkości podatku o kilka centów u każdego pracownika, co zazwyczaj uchodzi uwadze zainteresowanych. Natomiast nieuczciwy informatyk, po przelaniu tych kwot na swoje konto, uzyskuje dodatkowy, znacznej wysokości dochód. Następny

[64] Zob. D. B. Parker, S. Nycum, The New Criminal, „Datamation 1974 nr. 1, s. 56

przykład infiltracji polegał na odpowiedniej „korekcie" programu przez wstawienie do zbioru informacji systemu płac kont fikcyjnych pracowników (swoistych „martwych dusz"). Nadużycia finansowe na szkodę użytkownika systemu wynosiły 280 000 DM.

Znacznie wyższe straty poniósł użytkownik systemu informatycznego na skutek kradzieży zbioru informacji i ujawnienia kontrahentów firmy wydawniczej (Encyklopedia Britanika). Oszacowano je na ok. 3 mln dolarów.

Tego rodzaju działalność nazywa się, o czym już wspomniano defraudacją lub kradzieżą informacji z systemów informatycznych, umyślnym zniszczeniem lub przekłamaniem informacji, sabotażem komputerowym czy też przestępstwem „w białych rękawiczkach"[65].

Dla określenia całokształtu przestępczej działalności w systemach informatycznych zaproponowano termin infiltracja, czyli działanie osób nie upoważnionych, mające na celu przenikanie do zastrzeżonych informacji w systemach informatycznych przy użyciu różnych sposobów i środków.

Działanie takie może się przejawiać w postaci niedozwolonego odczytu, aktualizacji czy też modyfikacji informacji, dopisywania lub niszczenia jej, co jest równoznaczne ze zdezorganizowaniem pracy systemu lub nawet unieruchomieniem go na pewien czas.

Do zagrożeń informacji w systemach informatycznych można zaliczyć też znacznie częstsze zdarzenia przypadkowych zniszczeń lub przekłamań, czyli takich zdarzeń, które powstały w sposób nie zamierzony lub losowy, na skutek błędnego działania sprzętu, personelu lub innych czynników.

Podane określenie infiltracji w sposób ogólny charakteryzuje działalność osób nie upoważnionych. Należy więc wyraźnie rozgraniczyć działalność infiltracyjną osób nie upoważnionych od zdarzających się podczas przetwarzania przypadkowych, nie zamierzonych zdarzeń, które powodują zniszczenie lub przekłamanie informacji. Zdarzenia takie, choć są bardzo niepożądane, w praktyce występują stosunkowo często.

Działania zapobiegawcze (ochronne) w tym przypadku mają na celu przede wszystkim obniżenie liczby takich zdarzeń. Jednak ze względu na skomplikowany charakter samego procesu, a przede wszystkim z uwagi na zawodność działania ludzi i urządzeń, trudno je całkowicie wyeliminować.

[65] Risk Managers Urged For Curbing Graud „Datamation" 1976 nr. 6, s. 155

Można zauważyć w tym miejscu, że do szerzej ujmowanego kręgu zagrożeń informacji można włączyć też manipulowanie nimi, głównie przez ukrywanie, przekłamanie lub nawet niszczenie przez właściciela (użytkownika) niektórych z nich. Ponieważ mowa tu o ochronie informacji podczas automatycznego przetwarzania, dlatego zasygnalizowanego zagadnienia nie warto dalej omawiać.

W niektórych przypadkach zachodzi podobieństwo przejawów infiltracji i zdarzeń niezamierzonych, np. celowe zniszczenie informacji przez osobę nie upoważnioną i podobne zniszczenie przypadków. W obu sytuacjach użytkownik został pozbawiony informacji. Istnieje tu jednak zasadnicza różnica. Przy infiltracji mógł zaistnieć przypadek, że osoba nie upoważniona przed zniszczeniem zastrzeżonych informacji odczytała je (zapoznała się z ich treścią), a następnie zniszczyła, aby pozbawić ich właściwego użytkownika, a ponadto aby stworzyć określone trudności podczas przetwarzania, bądź nawet w procesie decyzyjnym.

Zrozumiała więc jest potrzeba stosowania większej ilości środków ochrony przed różnymi działaniami infiltracyjnymi oraz przypadkowymi zniszczeniami i przekłamaniami. Natomiast ochrona informacji przede wszystkim przed działaniem osób nie upoważnionych, w niektórych systemach informatycznych dotyczących gospodarki narodowej i we wszystkich systemach wojskowych, staje się koniecznością[66].

Konieczność ta wynika z tego, że niektóre systemy przetwarzają informacje niejawne, zastrzeżone dla pewnego, ściśle określonego grona użytkowników. Należy tu zwrócić uwagę na nowy aspekt, a mianowicie na to, że systemy informatyczne charakteryzują się nie spotykanym do tej pory stopniem „zagregowania" informacji oraz, że są eksploatowane w jednym miejscu. Można zatem się spodziewać, że osoby nie upoważnione będą dążyć do zdobycia informacji zastrzeżonych, a mogą to osiągnąć, stosując specjalne sposoby i środki, lub korzystając z zaniedbań w zakresie ochrony.

Żaden użytkownik systemu informatycznego, kwalifikując swoje informacje do grupy niejawnych, nie może być narażony na ich ujawnienie, zamianę czy zniszczenie w trakcie przetwarzania. Spełnienie tego warunku w systemach informatycznych jest jednak szczególnie trudne, zarówno z uwagi na organizację przetwarzania informacji, jak też ze względów technicznych i braku jednoznacznych ustaleń normatywno-prawnych.

[66] Ibidem

Nie trzeba też udowadniać, że zarówno odczyt informacji, jak też jego przekłamania lub utrata nie tylko dezorganizują działania systemu informatycznego, ale przede wszystkim mogą spowodować podejmowanie na różnych szczeblach błędnych decyzji.

W związku z powyższym, projektanci i przyszli użytkownicy muszą doskonale znać te elementy systemu, które są szczególnie narażone na infiltrację. Pozwala to bowiem, z jednej strony, na orientowanie się, w których miejscach systemu informacje są narażone na różnego rodzaju działanie osób nie powołanych, z drugiej zaś na odpowiedni dobór lub projektowanie środków ochrony i właściwe ich zastosowanie.

Zakończenie

Stosunkowo nowa problematyka ochrony informacji, którą zaczęto rozwiązywać w paru krajach w latach siedemdziesiątych, w Polsce, jak można sądzić znajduje się dopiero w początkowej fazie rozwiązań. Należy jednak zaznaczyć, że zarówno zagrożenia informacji, jak i środki ochrony tworzą wzajemnie uwarunkowaną, dynamiczną zależność, dotyczącą automatycznego przetwarzania informacji. Dynamizm ten wynika nie tylko z rozwoju sposobów i środków zagrożenia, co wywołuje konieczność poszukiwania nowych środków ochrony, ale też z doskonalszych metod przetwarzania informacji, które czynią tym trudniejszą ochronę.

Bibliografia

1. A. Beaufre, Wstęp do strategii. Odstraszanie i strategia, Warszawa 1968
2. K. Boruń, hasło Informacja, w: Mały słownik cybernetyczny, pod red. M. Kempisty, 1973
3. L. Ciborowski, Walka informacyjna, Europejskie Centrum Edukacyjne, Toruń 1999
4. H. Dominiczak.; Granice państwa i ich ochrona na przestrzeni dziejów 966–1996; Warszawa 1997
5. R. Gawryś, A. Olejnik, Doświadczenia Straży Granicznej w przeciwdziałaniu międzynarodowej przestępczości zorganizowanej związanej m. in. z nielegalną migracją, Centrum Szkolenia Straży Granicznej, „Problemy Ochrony Granic", Kętrzyn 2004
6. W. Głuszkow, Wstęp do cybernetyki, 1967, za: J. L. Kulikowski, Informacja i świat w którym żyjemy, 1978
7. Z. Jackiewicz.; Wojska Ochrony Pogranicza 1945 – 1991. Krótki Informator Historyczny, Kętrzyn 1998
8. T. Jemioło, Globalizacja, Szanse i zagrożenia, AON, Warszawa 2000
9. J. Jeziorański: „Żadne jednak wojskowe sojusze nie zabezpieczą nas przed zagrożeniem płynącym od wewnątrz", Polska wczoraj, dziś i jutro, Warszawa 1999
10. W. Kitler, Obrona narodowa w wybranych państwach demokratycznych, AON, Warszawa 2001
11. E. Kowalczyk, O istocie informacji, 1981
12. S. Koziej: Teoria sztuki wojennej. Warszawa: "Bellona", 1993
13. J. L Kulikowski, Organizacyjne i techniczne aspekty ochrony danych w systemach informatycznych, Prawne problemy systemów informatycznych. Materiały Konferencji Informatyki Prawniczej, t. 1 z. 2, Wrocław 1976
14. Zbigniew B. Kumoś: Granice Rzeczpospolitej Polskiej : (na przestrzeni dziejów). Warszawa: Wydawnictwo Comandor, 2005
15. G. Lissowski, hasło Informacja, w: Wielka Encyklopedia Powszechna, 2002

16. M. Menkiszak, Czy Polska potrzebuje strategii? w: R. Kuźniar (red.), Między polityką a strategią, Warszawa 1994
17. S. Mynarski, Elementy teorii systemów i cybernetyki, 1979
18. A. R. Nevell, Balancing The Ends, Ways and Means Army 1986
19. G. Nowacki, Współczesne poglądy na prowadzenie walki informacyjnej, AON, Warszawa 2001
20. B. Parker, S. Nycum, The New Criminal, „Datamation 1974
21. W. Sikorski, Przyszła wojna, Warszawa 1984
22. K. Sobczak, Prawo a informatyka, Warszawa 1978
23. K, Szaniawski hasło Informacja w: Filozofia a nauka, 1987
24. M. Szulczewski, Polityka informacji, Warszawa 1977
25. M. R. Wessel, Komputer i społeczeństwo, Warszawa 1976
26. Dz. U. Nr. 128, poz. 1176 ze zm.
27. Ustawa z 12 października 1990 r. o Straży Granicznej (tekst jedn. Dz. U z 2005 r. nr. 234, poz. 1997. ze zm.).
28. Konstytucja III RP, art. 85
29. Dz. U. z 2002 r. Nr. 101, poz. 926 ze zm
30. Dz. U. z 2005, Nr. 108, poz 908 ze zm.
31. Dz. U. Nr. 96, poz. 862 ze zm
32. Art. 9 ustawy o Straży Granicznej
33. Art. 9e ustawy o Straży Granicznej
34. Art. 11 ustawy o Straży Granicznej
35. Rozporządzenie (WE) nr. 562/2006 Parlamentu Europejskiego i Rady z 15 marca 2006 r. ustanawiające wspólnotowy kodeks zasad regulujących przepływ osób przez granice (Kodeks graniczny Schengen), Dz. Urz. WE L 105 z 13 kwietnia 2006