Jerzy Depo

Teoretyczne i prawne aspekty przeciwdziałania i zwalczania destrukcyjnej działalności obcych służb specjalnych

Kultura Bezpieczeństwa. Nauka-Praktyka-Refleksje nr 14, 76-96

2013

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej bazhum.muzhp.pl, gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

MUZEUM HISTORII POLSKI

Jerzy Depo

TEORETYCZNE I PRAWNE ASPEKTY PRZECIWDZIAŁANIA I ZWALCZANIA DESTRUKCYJNEJ DZIAŁALNOŚCI OBCYCH SŁUŻB SPECJALNYCH

Abstrakt

Artykuł podejmuje zagadnienie służb specjalnych, którymi zainteresowanie wzrosło szczególnie po II wojnie światowej. Podjęta została próba scharakteryzowania metod działania służb specjalnych i sformułowania ogólnych definicji związanych z nimi terminów takich, jak: wywiad, szpieg, dywersja czy sabotaż.

Zwrócono także uwagę na nieoczywisty związek służb specjalnych z działalnością terrorystyczną, w szczególności z tzw. cyberterroryzmem, który w niniejszym artykule został scharakteryzowany dzięki wskazaniu najczęstszych metod takiego działania.

Istotnym wątkiem jest także zagadnienie bezpieczeństwa i ochrony informacji, w szczególności prawne sposoby zwalczania terroryzmu i działalności obcych służb specjalnych.

Słowa kluczowe

ochrona informacji niejawnych, służby specjalne, terroryzm, cyberterroryzm

Abstract

In this article considered was issue of special services, which became particularly interesting after the Second World War. Made was an attempt of characterizing methods used by special services, and of formulating general definitions of terms associated to them, such as: intelligence services, spy, diversion and sabotage.

Considered was also an unevident relation of special services to terrorist activity, especially the so called cyberterrorism, which

in the article was characterized through indication of most common methods of such actions.

Relevant for the article is also issue of security and information protection, particularly legal ways of fighting terrorism and activities of foreign special services.
Key words
classified information protection, special services, terrorism, cyberterrorism

Art. 45 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[1], nakłada na jednostki organizacyjne, w których są przetwarzane informacje niejawne obowiązek stosowania środków bezpieczeństwa fizycznego odpowiednio do poziomu zagrożeń w celu uniemożliwienia osobom nieuprawnionym dostępu do takich informacji, w szczególności przed:

- działaniem obcych służb specjalnych;
- zamachem terrorystycznym lub sabotażem;
- kradzieżą lub zniszczeniem;
- próbą wejścia osób nieuprawnionych do pomieszczeń, w których są przetwarzane informacje niejawne;
- nieuprawnionym dostępem do informacji o wyższej klauzuli, tajności, czyli niewynikającym z posiadanych uprawnień.

1. Istota i charakterystyka zadań służb specjalnych

O służbach specjalnych mówi i pisze się dużo, szczególnie od czasów pierwszej i drugiej wojny światowej. Najczęściej jednak opisywano instytucje i operacje wywiadowcze, marginalizując przy tym opis innych form działania służb specjalnych, takich jak sabotaż, dywersja czy terroryzm. A przecież służby specjalne to ogólna nazwa przyjęta dla instytucji państwowych, których domeną jest tajne pozyskiwanie (wywiad), ochrona informacji

[1] Dziennik Ustaw (dalej cyt. Dz.U.) z 2010 r., nr 182, poz. 1228.

kluczowych dla zapewnienia wewnętrznego i zewnętrznego bezpieczeństwa państwa (kontrwywiad) oraz wykonywanie zadań dezinformacyjnych lub dezintegracyjnych.

W Polsce termin „służby specjalne" nie ma ustalonego i powszechnie przyjętego znaczenia. Po raz pierwszy został on użyty w uchwale Sejmu Rzeczypospolitej Polskiej z dnia 27 kwietnia 1995 r. w sprawie zmiany Regulaminu Sejmu z 30 lipca 1992 r. i powołania sejmowej Komisji do spraw Kontroli Służb Specjalnych, która miała nadzorować Urząd Ochrony Państwa i Wojskowe Służby Informacyjne[2]. Natomiast pozostałe służby, mimo iż w swej działalności posługują się metodami operacyjnymi *„podejmowanymi w celu ochrony bezpieczeństwa państwa"*, takiego przymiotu nie posiadają[3].

Ze względu na charakter i przeznaczenie służby specjalne dzielą się na trzy zasadnicze grupy:

1. służby informacyjno-wywiadowcze, których głównym zadaniem jest rozpoznawanie i pozyskiwanie cennych informacji o innych krajach, ich gospodarce, potencjale wojskowym, i innych o strategicznym znaczeniu dla własnego państwa, werbowanie agentów do pracy za granicą, planowanie i organizowanie dywersji, dezinformowanie zagranicznych służb wywiadowczych i kontrwywiadowczych oraz ochrona państwa przed ich działalnością;
2. służby kontrwywiadowcze, których zadania, można najogólniej zdefiniować jako neutralizację zagrożeń wynikających z ofensywnej działalności struktur rozpoznawczych przeciwnika, i -

[2] Monitor Polski Nr 23, poz. 271. W art. 1 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym służbą specjalną nazwano także CBA.

[3] Według leksykonu Jana Lareckiego – *„służby specjalne to usytuowane w strukturze aparatu władzy państwowej organizacyjnie samodzielne lub wchodzące w skład innej jednostki państwowej (np. ministerialnej) instytucje, uprawnione do prowadzenia różnych działań o charakterze tajnym*", idem, *Wielki leksykon służb specjalnych świata. Organizacje wywiadu, kontrwywiadu i policji politycznych świata, terminologia profesjonalna i żargon operacyjny*, Warszawa 2007, s. 621.

3. służby policyjno-prewencyjne, realizujące zadania na rzecz ładu i porządku publicznego oraz bezpieczeństwa osobistego i mienia obywateli.

2. Charakterystyka zagrożeń ze strony obcych służb specjalnych

Z działaniami wywiadu jako wyspecjalizowanej instytucji obcego państwa wiąże się przede wszystkim działalność szpiegowska, realizowana w sposób skryty i świadomy przez osoby lub grupy osób, tworzących tzw. siatkę szpiegowską. Szpiegiem określa się zaś osobę zdobywającą informacje mogące zaszkodzić komuś lub czemuś, bądź w celu przekazania ich innemu podmiotowi - drugiej stronie. Szpiegostwo, to z kolei, działanie przestępcze dokonywane na szkodę określonego państwa, polegające na podjęciu działalności na rzecz obcego wywiadu [4].

Ze szpiegostwem oraz działaniem na rzecz obcego wywiadu mamy do czynienia od ponad 5000 lat. Pojawiło się ono wraz z powstaniem struktur państwowych i występuje w czasach współczesnych, choć nie zawsze jest dostrzegane[5]. Działalność tę prowadzi się w sposób skryty, utajniony, ponieważ jej celem jest zdobycie (uzyskanie) informacji, które z założenia stanowią istotną tajemnicę państwa ze względu na ważny interes danego kraju. Informacje takie z zasady są niedostępne dla szerokiego grona osób oraz muszą być dobrze chronione. Przy tym szpiedzy nie szczędzą starań, by okradziony z tajemnic nie zorientował się, iż dotarły do nich osoby nieuprawnione. Wiadomo, iż z dużym powodzeniem można uprawiać działalność wywiadowczą wobec innych państw z terenu własnego kraju, unikając kłopotliwych zabiegów w celu werbowania agentury szpiegowskiej spośród cudzoziemców.

[4] R. Faligot, R. Kauffer, *Służby specjalne. Historia wywiadu i kontrwywiadu na świecie,* Wyd. Iskry, Warszawa 2006.
[5] Zob. N. Polmar, T. B. Allen, *Księga szpiegów. Encyklopedia,* Warszawa MAGNUM 2000, s. IX-XII.

Możliwości takie stwarzają przede wszystkim:

- międzynarodowy ruch osobowy o dużej skali i zasięgu;
- wysoki rozwój nauki i techniki, umożliwiający między innymi szpiegostwo kosmiczne;
- swobodny przepływ idei i kapitału;
- transformacje ustrojowe w byłych państw demokracji ludowej.

Znaczna część obywateli naszego kraju dysponuje wiadomościami, informacjami lub dokumentami niejawnymi oznaczonymi różnymi klauzulami tajności, od zastrzeżonych po ściśle tajne. Posiadanie takich wiadomości lub dostęp do nich wynika głównie z tytułu zatrudnienia i zajmowanych stanowisk w administracji państwowej, przedsiębiorstwach o znaczeniu strategicznym (przemysł zbrojeniowy, energetyczny, paliwowy, informatyczny), instytucjach kierujących gospodarką państwa, jego systemem bankowym oraz polityką zagraniczną RP i wypełnianiem zobowiązań wynikających z porozumień i umów zawartych z innymi krajami i organizacjami międzynarodowymi.

Osoby zaliczane do tego kręgu obywateli RP winny mieć zatem świadomość, że mogą stać się obiektem zainteresowania zarówno obcych służb specjalnych, jak i organizacji terrorystycznych. Symptomy tego zagrożenia przybierają różne formy - czasem trudno ocenić, czy stawiane przez cudzoziemców pytania stanowią przejaw zwykłej ciekawości, zainteresowań handlowych, dziennikarskich, czy też mają już charakter indagacji wywiadowczej. Jeśli uświadomimy sobie, że w trakcie rozmowy zainteresowania naszego rozmówcy zbliżają się do obszaru objętego tajemnicą, to bezpieczniej jest przyjąć założenie, że właśnie mamy do czynienia z próbą uzyskania konkretnej informacji lub jej potwierdzenia przez pracownika obcych służb specjalnych.

Okazją do tego typu indagacji są najczęściej zwykle kontakty służbowe i prywatne z cudzoziemcami o różnym statusie, w tym przede wszystkim z dyplomatami akredytowanymi w RP. Do

sytuacji takich może również dochodzić w czasie pobytu (służbowego lub prywatnego) obywateli naszego kraju za granicą.

Do zdobywania informacji, w coraz większym stopniu wykorzystywane są również różnego rodzaju spotkania i rozmowy z przedstawicielami interesujących wywiad środowisk, także te prowadzone w ramach kontaktów służbowych i prywatnych. Takie działania, zwłaszcza indagacja wywiadowcza, czy też próby zdobywania istotnych informacji przy okazji rozmów dotyczących różnych spraw, są z reguły podejmowane przez dyplomatów akredytowanych w Polsce, członków oficjalnych delegacji, przedstawicieli firm handlowych, ośrodków naukowych, dziennikarzy itp. Znaczna część tych osób może być właśnie kadrowymi pracownikami wywiadu lub działać na zlecenie obcych służb specjalnych. Także cudzoziemcy niezwiązani bezpośrednio z wywiadem zbierają informacje o naszym kraju. Z reguły mają oni obowiązek składania w swoich placówkach sprawozdań dotyczących kontaktów z polskimi partnerami, w tym m.in. sporządzania charakterystyk osób, z którymi zawarły znajomość.

Do najczęściej stosowanych metod uzyskiwania informacji wywiadowczych w trakcie różnych kontaktów należą:

- inspirowanie interesującego dla osoby podejmującej próbę indagacji tematu rozmowy;
- wywoływanie dyskusji na określony temat;
- ferowanie przeciwstawnych opinii w celu wywołania określonej reakcji rozmówców;
- „dowartościowywanie" rozmówcy celem pozyskania jego przychylności i nakłaniania go do wyrażania swoich sądów;
- próby przeniesienia kontaktów służbowych lub oficjalnych na płaszczyznę prywatną;
- oferowanie pomocy w załatwieniu różnego rodzaju spraw lub rozwiązaniu problemów osobistych bądź wręczanie wartościowych prezentów, które mają skłonić rozmówcę do kontynuowania znajomości, również na zasadzie rewanżu;

- inicjowanie wspólnych imprez o charakterze rozrywkowym lub turystycznym, podczas których niejednokrotnie, przy alkoholu, podejmowane są rozmowy na określony temat.

Osoby wyjeżdżające służbowo za granicę powinny zatem zdawać sobie sprawę, że mogą stać się obiektem zainteresowania obcych służb specjalnych. Dotyczy to zarówno członków oficjalnych delegacji, jak i osób wyjeżdżających indywidualnie na rozmowy lub negocjacje w sprawach gospodarczych i handlowych, a także uczestników sympozjów i kongresów naukowych oraz posiedzeń różnych gremiów organizacji międzynarodowych.

Zagrożenia z jakimi mogą się tam spotkać to penetracja ich rzeczy osobistych oraz podsłuch rozmów prowadzonych w pokojach hotelowych i restauracjach, a nawet w pomieszczeniach oficjalnych siedzib delegacji rządowych lub resortowych.

Dość powszechnie, służby specjalne prowadzą też tajne przeszukania w pomieszczeniach zajmowanych przez osoby delegowane i fotografują wszelkie znalezione tam dokumenty służbowe, a nawet osobiste, jak notesy, wizytówki, korespondencję prywatną, notatki z obrad itp. W niektórych państwach mogą być podejmowane próby wikłania osób delegowanych w różnego rodzaju sytuacje kompromitujące w celu późniejszego szantażu, np. przy próbie pozyskania do stałej lub doraźnej współpracy w przyszłości.

Podczas pobytu za granicą obywatele polscy - aby nie dać się uwikłać w problemy z ulotem posiadanych przez siebie informacji - powinni przestrzegać postępowania według następujących reguł:

- nigdy nie pozostawiać bez nadzoru jakichkolwiek dokumentów służbowych lub osobistych, zwłaszcza mających związek z instytucją lub urzędem, w którym pracuje dana osoba, w pomieszczeniach hotelowych lub innych;

- nie prowadzić w pomieszczeniach zamkniętych poufnych rozmów na tematy służbowe, objęte klauzulą tajności;
- rygorystycznie przestrzegać przepisów prawa i zwyczajów obowiązujących w danym kraju;
- nie nawiązywać przypadkowych kontaktów i nie podtrzymywać znajomości z osobami, których zachowanie wskazuje na to, że mogą być one inspirowane przez służby specjalne;
- pod żadnym pozorem nie nadużywać alkoholu;
- nie uczestniczyć w prowokowanych rozmowach sondażowych na tematy dotyczące spraw służbowych;
- o wszystkich faktach i zdarzeniach mogących wskazywać na działalność służb specjalnych natychmiast informować bezpośrednich przełożonych, ambasadę lub konsulat.

Działania terrorystyczne w zasadzie nie wiążą się bezpośrednio z działalnością służb specjalnych, przynajmniej w sposób oficjalny. Można jednak zasadnie, przypuszczać, że niektóre państwa zezwalają własnym służbom specjalnym na inspirowanie działalności terrorystycznej. Najczęściej działalność terrorystyczna była i jest organizowana przez różnego rodzaju niepaństwowe ugrupowania polityczne lub organizacje przestępcze. Najogólniej, terroryzm to stosowanie lub groźba użycia przemocy (uprowadzenia samolotów, mordowanie polityków, zamachy bombowe itp.), dla celów politycznych - wywarcia presji na społeczeństwo i władze, poruszenia opinii publicznej, wymuszenia ustępstw, bądź korzystnych dla siebie decyzji politycznych.

Nową kategorią zjawisk terrorystycznych, charakterystyczną dla obecnej epoki, jest cyberterroryzm - politycznie motywowany atak lub groźba ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach określonych zachowań (postaw, decyzji). Do celów, przeciwko którym mogą zostać skierowane ataki cyberterrorystyczne należą m.in.:

- telekomunikacja: linie telefoniczne, satelity, sieci komputerowe: komercyjne, wojskowe, akademickie;
- system energetyczny: produkcja, przemysł i dystrybucja energii, a także transport i magazynowanie surowców niezbędnych do jej produkcji;
- produkcja, magazynowanie i transport gazu ziemnego i ropy naftowej: cały proces wydobycia ropy naftowej i gazu ziemnego, magazynowania, przetwarzania i transportu za pomocą rurociągów, statków, transportem kołowym i kolejowym;
- system bankowy i finansowy: system przepływu kapitałów, poczynając od indywidualnych depozytów po transfer ogromnych sum pieniędzy, obejmuje wszystkie dostępne instrumenty operacji finansowych;
- transport: transport lotniczy, kolejowy, morski, rzeczny, drogowy osób i towarów oraz cały system wsparcia logistycznego;
- system zaopatrzenia w wodę: ujęcia wody, zbiorniki wodne, wodociągi, systemy filtrowania i oczyszczania wody, dostarczania jej dla rolnictwa, przemysłu, straży pożarnych oraz indywidualnych odbiorców;
- służby ratownicze: komunikacja z policją, służbą zdrowia, strażą pożarną itd.;
- ciągłość funkcjonowania organów władzy, samorządów terytorialnych oraz służb publicznych;
- przechwycenie informacji o charakterze militarnym, technologicznym, ekonomicznym i osobistym.

Do najważniejszych zaś metod ataków cyberterrorystycznych zalicza się:

- wykorzystywanie niekompetencji osób, które mają dostęp do systemu teleinformatycznego (ang. *social engineering*),
- korzystanie z systemu bez specjalnych zezwoleń lub używanie oprogramowania z nielegalnych źródeł: komputerowe wirusy, robaki i bakterie (*bugs and backdoors*),

- podstępne metody uzyskiwania dostępu do sieci (*stealing passwords*), lub zniszczenie mechanizmu autoryzacji prawa dostępu do systemu *(authentication failures*),
- wykorzystanie luk w zbiorze reguł sterujących wymianą informacji pomiędzy dwoma lub wieloma niezależnymi procesami (*protocol failures*),
- zdobywanie informacji dostępnych tylko dla administratora, niezbędnych do funkcjonowania sieci (*information leakage*),
- bomby logiczne uruchamiające dodatkowe funkcje elementu logicznego komputera i zakłócające tym samym jego działanie,
- konie trojańskie - specjalnie opracowane podprogramy, które (wmontowane np. w oryginalne programy użytkowe) mogą na określony sygnał lub komendę niszczyć bazy danych, formatować dyski itp.
- uzyskiwanie dostępu przez doinstalowanie dodatkowych chipów (*chipping*),
- wejście do systemu z ominięciem jego warstwy ochronnej lub używanie oprogramowania z nielegalnych źródeł (*bugs and back doors* – „tylne drzwi", „zapadnie"),
- podszywanie się pod zidentyfikowany w sieci adres IT, serwer lub proces systemowy (*spoofing*),
- przechwytywanie transmisji informacji między dwoma systemami (*hijacking*),
- tropienie, podsłuchiwanie - śledzenie całego ruchu w Sieci przy pomocy specjalnych programów „*węszących*" (*sniffing*),
- receptor van Eycka - podglądanie repliki obrazów wyświetlanych na monitorze przy wykorzystaniu efektu wysyłania przez monitor silnego sygnału elektromagnetycznego,
- DOS (*Denial of Sendce*), odmowa usługi - blokowanie pojedynczej usługi sieciowej bądź blokowanie pracy

całego serwera, czasem przez przeciążenie go za pomocą niezliczonej ilości zapytań,

- wysyłanie tysięcy wiadomości e-mail w celu blokowania działania poczty elektronicznej (*e-mail bombing*),
- broń częstotliwości radiowej (*radio frequency* - RF), urządzenia emitujące promieniowanie elektromagnetyczne należące do widma radiowego, używane do niszczenia technicznych urządzeń elektronicznych oraz zbiorów informatycznych,
- wysłanie do atakowanego komputera takiej ilości żądań, której nie jest on w stanie obsłużyć (*flooding*),
- natarczywe i nieukierunkowane przesyłanie pocztą elektroniczną niezamówionych ofert handlowych (*spamming*).

Z kolei sabotaż to:

- zamierzona dezorganizacja pracy przez uchylanie się od niej lub wadliwe jej wykonywanie, bądź przez uszkadzanie lub niszczenie urządzeń zapewniających prawidłowe funkcjonowanie jednostki organizacyjnej;
- ukryte, zamaskowane działanie mające na celu przeszkodzenie w realizacji jakiegoś planu, podjęte przez osoby uczestniczące w tej realizacji[13], a także
- celowe dezorganizowanie pracy (niszczenie narzędzi, maszyn produkcyjnych, spowalnianie produkcji, wykonywanie wadliwych wyrobów) mające osłabić przeciwnika;
- tajne, podstępne działanie mające utrudnić lub uniemożliwić realizację poleceń przełożonych,
- to również, wzbudzająca niepokój metoda powtarzających się aktów przemocy, przyjęta przez działające najczęściej w sposób tajny jednostki, grupy lub podmioty państwowe, wybierana z powodów kryminalnych lub politycznych, przy czym - w odróżnieniu od zamachów na życie - bezpośrednie cele przemocy nie są głównymi celami.

Sabotaż jest zatem terminem na określenie przestępstw polegających na uniemożliwianiu lub utrudnianiu prawidłowego funkcjonowania zakładów, urządzeń lub instytucji o poważnym znaczeniu.

Natomiast dywersja, to:

- dezorganizacja sił przeciwnika polegająca na niszczeniu lub uszkadzaniu jego urządzeń obronnych, produkcyjnych, komunikacyjnych itp.;
- wroga działalność mająca na celu osłabienie sił gospodarczych i obronności państwa;
- akcje zbrojne i propagandowe zmierzające do obniżenia ich wartości bojowej i morale;
- ukryte działanie mające na celu osłabienie gospodarki wrogiego państwa, jego potencjału militarnego, zakłócenie życia politycznego, społecznego i kulturalnego[6].

Odzwierciedleniem zasad konstytucyjnych i prawnych, które mogą być stosowane w zwalczaniu działalności obcych służb specjalnych i walce z terroryzmem w Polsce są:

- Kodeks karny - ustawa z dnia 6 czerwca 1997 roku[7], oraz
- wspomniana na wstępie, ustawa o ochronie informacji niejawnych. I tak:

W art. 130 kodeksu karnego za szpiegostwo przyjęto uznawać:

- udział w działalności obcego wywiadu przeciwko Rzeczypospolitej Polskiej,
- udzielanie obcemu wywiadowi wiadomości mogących wyrządzić szkodę Rzeczypospolitej Polskiej,

[6] Zasadniczo, dywersja jest terminem na określenie przestępstwa polegającego na niszczeniu lub uszkadzaniu obiektów przeciwnika o poważnym znaczeniu dla funkcjonowania państwa.
[7] Dz.U. z 2 sierpnia 1997 r., nr 88, poz. 553 z późn. zm.

- gromadzenie, przechowywanie lub wchodzenie do systemu informatycznego w celu uzyskania i przekazania obcemu wywiadowi takich wiadomości,
- zgłoszenie gotowości działania na rzecz obcego wywiadu, oraz –
- organizowanie lub kierowanie działalnością obcego wywiadu.

W orzecznictwie i literaturze prawniczej do form działalności szpiegowskiej zalicza się również takie zachowania jak:

- wyszukiwanie kandydatów na agentów tego wywiadu,
- rozdzielanie ról w siatce wywiadowczej,
- wydawanie instrukcji poszczególnym członkom,
- obsługa skrzynek i skrytek kontaktowych,
- pełnienie funkcji łącznika lub kuriera,
- szkolenie agenta,
- udostępnianie mieszkania lub innego pomieszczenia na potrzeby obcego wywiadu,
- organizowanie i ustalanie punktów przerzutowych
- wykonanie zadań dezinformacyjnych lub dezintegracyjnych,
- realizacja innych poleceń obcego wywiadu.

Jeśli zaś chodzi o przestępstwa sabotażu i dywersji, to nie znajdują one szczególnej regulacji karnej, gdyż termin „dywersja" służy przede wszystkim do określania działalności niebezpiecznej, niszczycielskiej, natomiast pojęciem „sabotaż" określa się zachowanie prowadzące do dezorganizacji pracy. W omawianym kodeksie karnym penalizowany jest jedynie sabotaż komputerowy (art. 269), który polega na niszczeniu, uszkadzaniu, usuwaniu lub zmianie danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowaniu administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego, albo zakłócaniu lub uniemożliwianiu automatycznego przetwarzania, gromadzenia lub przekazywania danych.

Potencjalne zagrożenia szpiegostwem, akcjami sabotażowymi lub terrorystycznymi, skierowanymi przeciwko jednostkom organizacyjnym, w tym kancelariom tajnym i ich personelowi, mogą występować głównie ze strony organizacji terrorystycznych i ugrupowań ekstremistycznych. Zarówno jedne jak i drugie mogą być sponsorowane przez jakiś kraj, który może wybrać określony obiekt/kancelarię i personel, jako cel ataków z zamiarem osiągnięcia własnych korzyści lub jego zniszczenia w czasie kryzysu.

Przewiduje się, że akcje te mogą mieć charakter:

- ataków bombowych, obejmujących również bomby umieszczane w samochodach, przenośne bomby walizkowe, urządzenia zapalające i bomby w przesyłkach;
- zabójstw, porwań, brania zakładników lub prób zastraszenia;
- demonstracji, które mogą być organizowane z zamiarem wywołania rozruchów lub powodowania konfrontacji;
- bezpośrednich ataków na pomieszczenia lub ich okupowanie;
- fałszywych alarmów - szczególnie o podłożonych bombach - z zamiarem zastraszenia bądź szykanowania.

Działania służb specjalnych lub organizacji terrorystycznych są zawsze poprzedzone rozpoznaniem danego obiektu. Rozpoznanie ma przede wszystkim ustalić, jakie metody i środki muszą być zastosowane, aby osiągnąć obrany cel. Działalność rozpoznawcza koncentruje się wówczas na:

- funkcjonujących systemach ochrony jednostki organizacyjnej, a zwłaszcza słabych punktach tych systemów;
- zastosowanych środkach fizycznej ochrony informacji niejawnych, w szczególności możliwościach ich pokonania (sforsowania);
- wykorzystywanych systemach elektronicznego alarmowania i możliwościach ich unieszkodliwienia (wyłączenia);

- możliwościach włamania do wykorzystywanych systemów lub sieci teleinformatycznych;
- osobach, które mogą udzielić wywiadowi lub organizacji terrorystycznej pomocy w osiągnięciu obranego celu.

Działalność rozpoznawcza zazwyczaj pozostawia jakieś ślady, nie zawsze materialne, lecz możliwe do ustalenia i podjęcia skutecznego przeciwdziałania. Tymi śladami mogą być:

- obecność obcych osób w rejonie danej jednostki organizacyjnej,
- tzw. „dziwni" interesanci,
- włamania lub próby włamań do niektórych pomieszczeń,
- wypytywanie pracowników o sprawy dotyczące jednostki organizacyjnej,
- fałszywe alarmy itp.

W praktyce istnieją dwie drogi wypływu informacji niejawnych stanowiących tajemnicę istotną dla bezpieczeństwa państwa i organizacji. Nie są to drogi skomplikowane czy też nieznane. Pierwsza droga to człowiek, który jest i pozostanie głównym sprawcą wypływu informacji niejawnych z jednostki organizacyjnej.

Druga to maszyna - najczęściej chodzi tu o telefon, faks, komputer lub radio, czyli jedno z urządzeń, którymi posługuje się współcześnie człowiek, nie zawsze zdając sobie sprawę z łatwości podsłuchów telefonicznych, radiowych lub teleinformatycznych sieci łączności.

Współczesna technika umożliwia zabezpieczenie używanych urządzeń przed wypływem informacji niejawnych. Komputerów można używać w szczelnie ekranujących je kabinach, telefony, faksy i radio zakodować dwustronnie. Powyższe zabiegi istotnie zwiększają bezpieczeństwo przetwarzanych lub transmitowanych informacji.

O wiele trudniej przedstawia się sytuacja, gdy w działalności rozpoznawczej, wywiadowczej bądź terrorystycznej uczestniczy osoba zatrudniona w danej jednostce organizacyjnej. Nikt

z własnej woli nie przyzna się do prowadzenia działalności niezgodnej z prawem. Zazwyczaj na tę sytuację nakładają się jeszcze niedostatki działań kontrolnych personelu kierowniczego jednostki organizacyjnej, ułatwiające uzyskiwanie informacji niejawnych. Do niedostatków tych zalicza się m.in.:

- niewłaściwą politykę doboru i zatrudnienia pracowników w jednostce organizacyjnej;
- zatrudnianie osób, które są podatne na ich wykorzystanie do działań niezgodnych z prawem;
- brak spójnych zasad i organizacji wewnętrznej ochrony wszystkich informacji niejawnych;
- sytuację, gdy personel nie ma jasno określonych kryteriów, co mu wolno, a czego nie, gdy nikt nikogo nie kontroluje, gdy z instytucji (biura) można wynieść wszystko;
- brak kontroli (a niekiedy również zainteresowania) ze strony kierownictwa jednostki organizacyjnej stanem ochrony informacji niejawnych oraz sytuacją w zakresie bezpieczeństwa i ochrony fizycznej;
- niewytworzenie u personelu nawyku przestrzegania zasad ochrony informacji.

Stąd, bardzo ważną metodą ochrony informacji są specjalne procedury weryfikacji osób mających mieć dostęp do informacji niejawnych, określone w ustawie o ochronie informacji niejawnych „Bezpieczeństwem osobowym" (Rozdział 5 uoin, art.art. 21-34) oraz „Bezpieczeństwem przemysłowym (Rozdział 9, art.art.54-71).

Zgodnie z art. 4 ust. 1 uoin informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy, i tylko - w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo innej zleconej pracy (zasada ograniczonego dostępu). Przy czym (art. 21 ust.1), stanowi, iż dopuszczenie do pracy lub pełnienia służby na stanowisku albo zlecenie pracy z którą może

łączyć się dostęp do informacji niejawnych, może nastąpić dopiero:

1. po przeprowadzeniu postępowania sprawdzającego i uzyskaniu poświadczenia bezpieczeństwa, oraz –
2. po przeszkoleniu tej osoby w zakresie ochrony informacji niejawnych.

Przedmiotowa ustawa dokonuje podziału postępowania sprawdzającego na: zwykłe postępowanie sprawdzające i poszerzone postępowanie sprawdzające (art. 22).

Zwykłe postępowanie sprawdzające przeprowadza się - przy stanowiskach i pracach związanych z dostępem do informacji niejawnych o klauzuli „poufne, przeprowadza je pełnomocnik ochrony informacji niejawnych na pisemne polecenie kierownika jednostki organizacyjnej (art. 23).

Natomiast poszerzone postępowanie sprawdzające:

a) przy stanowiskach i pracach związanych z dostępem do informacji niejawnych o klauzuli „tajne" lub „ściśle tajne",
b) wobec pełnomocników ochrony, zastępców pełnomocników ochrony oraz kandydatów na te stanowiska,
c) wobec kierowników jednostek organizacyjnych, w których są przetwarzane informacje niejawne o klauzuli „poufne" lub wyższej,
d) wobec osób ubiegających się o dostęp do informacji niejawnych międzynarodowych lub o dostęp, który ma wynikać z umowy międzynarodowej zawartej przez Rzeczpospolitą Polską, przeprowadzają służby nadzorujące funkcjonowanie systemu ochrony informacji niejawnych w danej jednostce organizacyjnej - Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego (art. 24 uoin).

W toku poszerzonego postępowania sprawdzającego, ustala się ponadto, czy istnieją wątpliwości (art. 24 ust. 3):

- związane z wyraźną różnicą między poziomem życia osoby sprawdzanej a uzyskiwanymi przez nią dochodami;
- związane z ewentualnymi informacjami o chorobie psychicznej lub innych zakłóceniach czynności psychicznych ograniczających sprawność umysłową i mogących negatywnie wpłynąć na zdolność osoby sprawdzanej do zajmowania stanowiska albo wykonywania prac związanych z dostępem do informacji niejawnych stanowiących tajemnicę prawnie chronioną;
- związane z uzależnieniem od alkoholu, środków odurzających lub substancji psychotropowych.

Bezpieczeństwem przemysłowym określa się z kolei wszelkie działania związane z zapewnieniem ochrony informacji niejawnych udostępnianych przedsiębiorcy, jednostce naukowej lub badawczo-rozwojowej w związku z umową lub zadaniem wykonywanym na podstawie przepisów prawa, przedmiotem sprawdzenia jest:

- zdolność przedsiębiorcy do ochrony informacji niejawnych (stosowania procedur i rozwiązań zgodnie z uoin),
- czy struktura kapitału, źródła jej pochodzenia środków finansowych oraz powiązania z innymi kapitałami nie budzą podejrzeń,
- oraz, czy osoby, które winny posiadać, mają aktualne i odpowiednie poświadczenia bezpieczeństwa.

W art. 46 uoin ustawodawca określił ponadto następujące działania i środki ochrony fizycznej informacji niejawnych o klauzuli „poufne” lub wyższej:

1. organizację stref ochronnych,
2. wprowadzenie systemu kontroli wejść i wyjść ze stref ochronnych,
3. określenie uprawnień do przebywania w strefach ochronnych,

4. stosowanie wyposażenia i urządzeń zabezpieczających, którym przyznano certyfikaty.

Podsumowanie

Wydaje się oczywiste, że żaden organ kadrowy nie znajdzie „ideału" pracownika, który da kierownikowi jednostki organizacyjnej całkowitą pewność, że informacje niejawne będą przez niego należycie chronione. Trudno też o środki w pełni zabezpieczające obiekt przed podglądem, włamaniem, czy kradzieżą. Stąd szczególne zadanie w tym przedmiocie spoczywa na służbach ochrony państwa i pełnomocnikach do spraw ochrony informacji niejawnych, którzy, poprzez rzetelne prowadzenie postępowań sprawdzających wyeliminują osoby potencjalnie podatne na ewentualność ich wykorzystania niezgodnie z prawem. Cel ten można również osiągnąć poprzez:

- kontrolę postępowania i rygorystyczne przestrzeganie ustalonych przepisów w zakresie ochrony informacji niejawnych (należy przy tym pamiętać, że właściwe wypełnianie funkcji kontrolnej przez osoby funkcyjne oddziałuje także w pozytywny sposób na cały personel),
- właściwą i pryncypialną postawę, wobec ochrony informacji niejawnych, osób na stanowiskach kierowniczych i odpowiedzialnych za realizację podstawowych zadań ochronnych;
- szkolenie z zasad ochrony informacji niejawnych przed udzieleniem dostępu do takich informacji oraz cykliczne przypominanie o tych zasadach.

Do szczególnych obowiązków kierowników jednostek organizacyjnych w omawianej dziedzinie zaliczyć zatem należy:

- dokonywanie okresowych ocen zagrożeń ze strony obcych służb specjalnych lub organizacji terrorystycznych, których podstawą winien być funkcjonujący system zabezpieczeń i barier dostępu do informacji niejawnych,

- stosowanie adekwatnych do istniejących zagrożeń, dodatkowych środków bezpieczeństwa fizycznego;
- świadomość, że zasady bezpieczeństwa powinny funkcjonować nie tylko w dziedzinach objętych ochroną informacji niejawnych, bowiem materiały niesklasyfikowane także mogą mieć znaczenie dla sfery bezpieczeństwa ogólnego jednostki organizacyjnej;
- utrzymywanie stałego kontaktu ze służbami ochrony państwa oraz służbami porządkowymi (policja, żandarmeria wojskowa), który zapewni im bieżący dopływ informacji o istniejących zagrożeniach i stopniu ich nasilania się w otoczeniu lub wewnątrz danej jednostki organizacyjnej;
- opracowanie i ustalenie systemu alarmowania i powiadamiania odpowiedniego personelu jednostki organizacyjnej oraz służb interwencyjnych;
- określenie szczegółowych obowiązków poszczególnych pracowników w zakresie zasad postępowania w sytuacji powzięcia podejrzeń o istnieniu zagrożenia oraz ustalenie hierarchii osób odpowiedzialnych za reagowanie w wypadku wystąpienia zagrożenia,
- zaplanowanie i ćwiczenie odpowiednich procedur na wypadek wystąpienia konkretnych wyspecjalizowanych zagrożeń, jak zamach na życie człowieka, podłożenie bomby, znalezienie się w roli zakładnika, otrzymanie podejrzanej przesyłki, eksplozja ładunku wybuchowego,
- opracowanie standardowej procedury ewakuacyjnej osób i kluczowych zasobów jednostki.

Bibliografia

1. Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wyd. Adam Marszałek, Toruń 2005.
2. Hoc S., *Karnoprawna ochrona informacji*, Uniwersytet Opolski, Opole 2009.
3. Hoc S., *Ustawa o ochronie informacji niejawnych. Komentarz*, Wyd. LexisNexis, Warszawa 2010.

4. Iwaszko B., *Ochrona informacji niejawnych w praktyce*, Prescom Sp. z o.o., Wrocław 2012.
5. Jabłoński M., Radziszewski T., *Bezpieczeństwo fizyczne i teleinformatyczne informacji niejawnych*, Prescom Sp. z o.o., Wrocław 2012.
6. Jabłoński M., Wygoda K., *Dostęp do informacji i jego granice. Wolność informacji, prawo dostępu do informacji publicznej, ochrona danych osobowych*, Wrocław 2002.
7. Korzeniowski L.F., *Podstawy nauk o bezpieczeństwie*, Wyd. Difin, Warszawa 2012.
8. Liderman K., *Bezpieczeństwo informacyjne*, Wyd. PWN, Warszawa 2012.
9. Nowak A., Scheffs W., *Zarządzanie bezpieczeństwem informacyjnym*, Wyd. MON, Warszawa 2010.
10. *Ochrona Informacji Niejawnych – Poradnik Praktyczny*, Warszawa 2011.
11. Stankowska I., *Ustawa o ochronie informacji niejawnych. Komentarz*, LexisNexis, Warszawa 2011.
12. Thiem P., *Bezpieczeństwo osobowe w ochronie informacji niejawnych*, Prescom Sp. z o.o., Wrocław 2011.
13. Żebrowski A., Kwiatkowski M., *Bezpieczeństwo informacji III Rzeczypospolitej* Kraków 2000.