ARTYKUŁY
Studenckie Zeszyty Naukowe 2019, Vol. XXII, nr 42
DOI: 10.17951/szn.2019.22.42.143-153

płk mgr inż. Janusz Parczewski
Akademia Sztuki Wojennej w Warszawie
parczewj@wp.pl

Zagrożenia związane z działaniem człowieka w systemie ochrony informacji niejawnych

The threats related to human activity in the system of protecting classified information

STRESZCZENIE

Autor zwrócił uwagę na zobowiązania międzynarodowe Polski, szczególnie te, związane z dostosowaniem regulacji prawnych do standardów obowiązujących w państwach członkowskich NATO dotyczących bezpieczeństwa informacji, które zaowocowały wprowadzeniem do porządku prawnego w Polsce Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Zostało podkreślone, iż zgodnie z przepisami tej ustawy, każda jednostka organizacyjna przetwarzająca informacje niejawne zobowiązana jest do zorganizowania systemu ochrony tych informacji przed nieuprawnionym ujawnieniem. Zostały wymienione podstawowe zagrożenia dla bezpieczeństwa klasyfikowanych informacji, szczególnie te, które wynikają z działania człowieka. Zdaniem autora, trudno jest wyeliminować wszystkie zagrożenia związane z działaniem człowieka, pomimo dotkliwych sankcji karnych, jakie grożą za ujawnienie lub wykorzystywanie wbrew przepisom cytowanej ustawy informacji niejawnych. Należy jednak podjąć próby, aby pojawiające się zagrożenia i ich możliwe skutki ograniczyć do minimum, Szczegółową analizę omawianej problematyki autor zawarł w swojej dysertacji, która wkrótce zostanie zaprezentowana.

Słowa kluczowe: zagrożenia, bezpieczeństwo osobowe, ochrona informacji niejawnych

WSTĘP

Obecny stan zobowiązań międzynarodowych RP w świetle umów międzynarodowych jak i sojuszy wojskowych szczególną uwagę przywiązuje do warstwy informacji. Pojęcie przedmiotowe i podmiotowe obszaru informacji jest wyjątkowo istotne z punktu widzenia bezpieczeństwa zewnętrznego i wewnętrznego państwa. O istotnej wadze problemu świadczy fakt, iż większość państw należących do ONZ posiada własne, niezależne regulacje prawne, które szczególną wagę poświęcają

sferze „ochrony informacji". Również organizacje międzynarodowe, w tym Sojusz Północnoatlantycki NATO, za cel nadrzędny stawiają kompleksową ochronę wrażliwych dla nich informacji formułując nowe rozwiązania w tym zakresie, które *ex lege* stanowią podstawę do ich przestrzegania przez państwa członkowskie.

Zainteresowanie informacją oraz sposobami i możliwościami jej przetwarzania, to efekt postępu technicznego, szczególnie na przełomie XX i XXI wieku. To dzięki niemu informacja stała się nie tylko dobrem współczesnej cywilizacji, ale również pożądanym towarem za który płaci się przysłowiowe ciężkie pieniądze. Termin „informacja" pochodzi od łacińskiego słowa *„informatio"*, które oznacza: przedstawienie, wizerunek oraz od czasownika *„informare"*, co oznacza: kształtować, przedstawiać. Jest to termin interdyscyplinarny, definiowany różnie w różnych dziedzinach nauki. Najogólniej mówiąc, to właściwość pewnych obiektów, relacja między elementami zbiorów pewnych obiektów, której istotą jest zmniejszenie niepewności[1].

Ciekawą definicję rozważanego terminu przedstawił P. Sienkiewicz, według którego informacja[2] to zbiór faktów, zdarzeń, cech, obiektów ujęty i podany w takiej formie, że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działanie umysłowe lub fizyczne. Biorąc powyższe definicje pod uwagę można zauważyć, że posiadanie dobra, czyli wiarygodnej i aktualnej informacji, a także możliwości jej szybkiego przetworzenia stało się gwarantem sprawnego funkcjonowania jednostki organizacyjnej i kluczem do osiągnięcia przez nią sukcesu w danym obszarze działalności np. w prowadzeniu biznesu i utrzymaniu konkurencyjności. Dlatego też informacja powinna być zaliczana do aktywów biznesowych i w odpowiedni sposób chroniona przed zagrożeniami[3]. Z tego samego powodu, jak zauważył M. Strzoda, informacje są zasadniczym składnikiem i podstawą zarządzania, stanowią element integrujący funkcje kierownicze oraz wszystkie zadania i cele, dla realizacji których powoływane są organizacje. Informacje pełnią funkcje inspirujące, wspierające, podtrzymujące, rozstrzygające, monitorujące, a tym samym są podstawą trafnych decyzji[4].

W rozważanej przez autora problematyce mamy do czynienia z informacjami, które z racji posiadania pewnej właściwości tzn. nadanej klauzuli tajności, będziemy nazywać informacjami niejawnymi lub klasyfikowanymi. Takie informacje nie mogą funkcjonować w przestrzeni publicznej bez należytej ochrony, gdyż ujawnie-

---

[1] Ryszkowski M., Ryszkowska M., Ryszkowska M., O wybranych tajemnicach bez tajemnic, Instytut Ochrony Informacji i Danych Osobowych, Katowice 2011, s. 36 i n.

[2] Sienkiewicz P., Systemy kierowania, Państwowe Wydawnictwo „Wiedza Powszechna", Warszawa 1989, s. 128.

[3] Cienińska B., Łunarski J., Perłowski R., Stadnicka D., Systemy zarządzania bezpieczeństwem w przedsiębiorstwie, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2006, s. 69.

[4] Strzoda M., Zarządzanie informacjami w organizacji, Akademia Obrony Narodowej, Warszawa 2004, s. 6.

nie tych informacji osobom lub podmiotom nieuprawnionym mogłoby wyrządzić szkody nie tylko w jednostce organizacyjnej, gdzie taka informacja została wytworzona, ale również mogłaby spowodować zagrożenia dla bezpieczeństwa kraju. Między innymi dlatego w polskim prawodawstwie funkcjonuje ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[5], której przepisy szczegółowo określają zasady ochrony klasyfikowanych informacji. Należy nadmienić, że aktualny tekst jednolity tej ustawy został ogłoszony w Obwieszczeniu Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 9 lutego 2018 r. w sprawie ogłoszenia jednolitego tekstu ustawy o ochronie informacji niejawnych (Dz. U. z 2018 r., poz. 412).

Autor zwraca uwagę na konieczność zorganizowania systemu ochrony informacji niejawnych w jednostce organizacyjnej, gdy zachodzi potrzeba przetwarzania w niej informacji klasyfikowanych. Ponadto przedstawia filary tego systemu i opisuje relacje, jakie zachodzą między jego elementami składowymi. W dalszej części zostały przedstawione zagrożenia związane z działaniem człowieka, które mogą negatywnie wpłynąć na sprawne działanie systemu ochrony informacji niejawnych w jednostce organizacyjnej.

FILARY SYSTEMU OCHRONY INFORMACJI NIEJAWNYCH

Przed rozpoczęciem rozważań na temat filarów systemu ochrony informacji niejawnych należałoby zdefiniować pojęcie „system", gdyż w szerokim odbiorze jest ono różnie interpretowane. Spośród wielu dostępnych definicji wybrałem jedną, która moim zdaniem najlepiej przedstawia rozważaną problematykę, autorstwa P. Sienkiewicza, według którego systemem[6] jest każdy złożony obiekt wyróżniony w badanej rzeczywistości, stanowiący całość tworzoną przez zbiór obiektów elementarnych (elementów) i powiązań (relacji) między nimi.

Mówiąc o filarach systemu ochrony informacji niejawnych, zarówno w sferze cywilnej jak i wojskowej, zawsze powinniśmy mieć na myśli kierownika jednostki organizacyjnej oraz zatrudnionego przez niego pełnomocnika ochrony. Taki stan rzeczy wynika wprost z przepisów ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[7], które w przypadku zaistnienia potrzeby przetwarzania informacji niejawnych w danej jednostce organizacyjnej, szczegółowo regulują kwestie zorganizowania i zapewnienia ochrony informacjom niejawnym w tej jednostce.

Osobą odpowiedzialną za pierwsze przedsięwzięcie, czyli zorganizowanie i funkcjonowanie systemu ochrony informacji niejawnych, jest kierownik jed-

[5] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228).

[6] Sienkiewicz P., Analiza systemowa. Podstawy i zastosowania, Bellona, Warszawa 1994, s. 16.

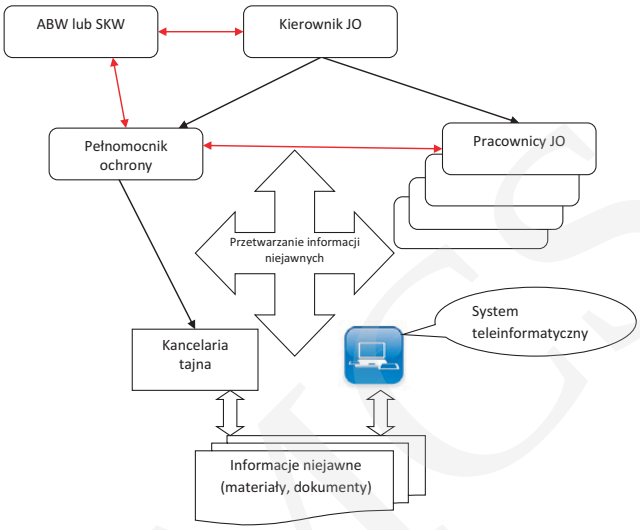
[7] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, *op. cit.*

nostki organizacyjnej, w której przetwarzane są klasyfikowane informacje. W celu realizacji szeregu czynności związanych z tym przedsięwzięciem, w szczególności za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych, kierownik jednostki organizacyjnej zatrudnia pełnomocnika ochrony, który jemu bezpośrednio podlega. Właśnie ta bezpośrednia podległość, która w ujęciu cytowanej definicji systemu niewątpliwie jest relacją pomiędzy dwoma kluczowymi elementami systemu ochrony informacji niejawnych tj. pomiędzy kierownikiem a pełnomocnikiem ochrony, nadaje temu drugiemu stosunkowo wysoką rangę w strukturze organizacyjnej danej jednostki.

Równie ważnym elementem systemu ochrony informacji niejawnych są pracownicy danej jednostki organizacyjnej, którzy po uzyskaniu odpowiednich uprawnień tj. poświadczenia bezpieczeństwa lub upoważnienia oraz odbyciu szkolenia w zakresie ochrony informacji niejawnych, mogą uczestniczyć w procesie przetwarzania informacji niejawnych, ale tylko takich, które wynikają z zakresu wykonywanych obowiązków służbowych i zlecanych każdorazowo przez swoich przełożonych. Uzyskanie odpowiednich uprawnień do dostępu do informacji niejawnych w postaci poświadczenia bezpieczeństwa uzależnione jest od wyniku postępowania sprawdzającego, które realizuje: Agencja Bezpieczeństwa Wewnętrznego (ABW) lub Służba Kontrwywiadu Wojskowego (SKW) w zakresie dostępu do informacji niejawnych o klauzuli „tajne" lub „ściśle tajne" oraz pełnomocnik ochrony w zakresie dostępu do informacji niejawnych o klauzuli „poufne". W przypadku dostępu tylko i wyłącznie do informacji niejawnych o klauzuli „zastrzeżone" kierownik jednostki organizacyjnej może wydać podległym pracownikom stosowne upoważnienie.

Na podstawie powyższych informacji można pokusić się o przedstawienie uproszczonego modelu systemu ochrony informacji niejawnych w danej jednostce organizacyjnej, który może wyglądać następująco[8]:

[8] Podobne rozwiązania stosuje się także w odniesieniu do ochrony informacji niejawnych w sferze międzynarodowej, szerzej: https://bip.abw.gov.pl/bip/informacje-niejawne–1/ochrona-informacji-nie/153,OCHRONA-INFORMACJI-NIEJAWNYCH-MIEDZYNARODOWYCH-W-SFERZE-CYWILNEJ-I-WOJSKOWEJ.html#1 – dostęp 28.12.2018 r. Ze względu na wymogi formalne należy zasygnalizować tylko, iż NSA (National Security Authority) czyli Krajowa Władza Bezpieczeństwa, którą obecnie jest Szef ABW, została powołana do ochrony informacji niejawnych NATO. NSA jest odpowiedzialna za zapewnienie bezpieczeństwa informacji klasyfikowanych NATO, wydawanie zgody na ustanowienie lub likwidację głównych kancelarii tajnych, zapewnienie przeprowadzenia procedur sprawdzających wobec osób, które mają uzyskać dostęp do informacji niejawnych NATO.



Rys. 1. Uproszczony model systemu ochrony informacji niejawnych w jednostce organizacyjnej (źródło: opracowanie własne)

W przedstawionym powyżej uproszczonym modelu systemu ochrony informacji niejawnych w jednostce organizacyjnej, mając na uwadze definicję systemu, można wyróżnić następujące obiekty elementarne (elementy):

- kierownik jednostki organizacyjnej;
- pełnomocnik ochrony;
- pracownicy jednostki o organizacyjnej;
- kancelaria tajna (jeżeli została utworzona)[9];
- system teleinformatyczny to przetwarzania informacji niejawnych (jeżeli został utworzony);
- informacje niejawne (materiały, dokumenty);
- Agencja Bezpieczeństwa Wewnętrznego lub Służba Kontrwywiadu Wojskowego.

Pomiędzy wymienionymi obiektami elementarnymi (elementami) zachodzą następujące relacje (powiązania):

- relacja podległości służbowej przełożony – podwładny, oznaczona symbolem ⟶
- relacja zależności funkcjonalnej, oznaczona symbolem ⟷
- relacja uczestnictwa w procesie przetwarzania informacji niejawnych, oznaczona symbolem ⟺

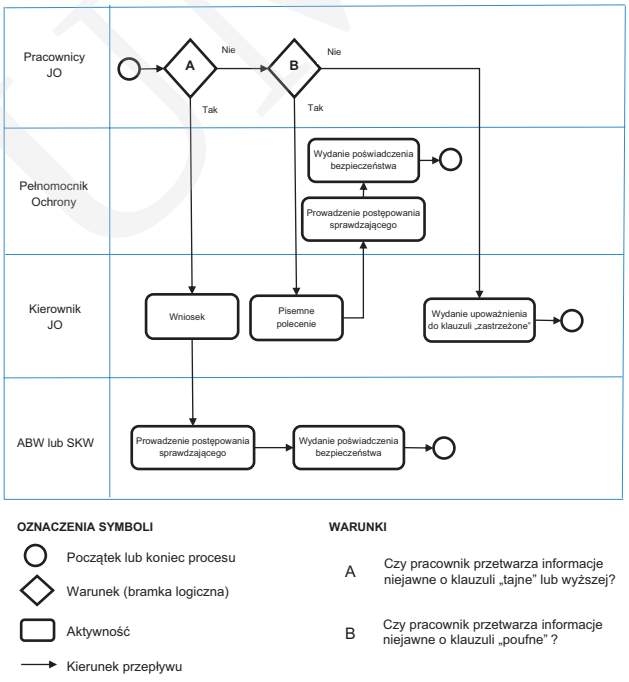
Po zidentyfikowaniu elementów systemu ochrony informacji niejawnych oraz relacji zachodzących pomiędzy tymi elementami, w celu uruchomienia procesu

[9] Tutaj stosuje się także dokument C-M(2002)49 – „Bezpieczeństwo w ramach organizacji Traktatu Północnoatlantyckiego".

przetwarzania klasyfikowanych informacji w jednostce organizacyjnej należy wziąć pod uwagę następujące czynniki:

1) najwyższą klauzulę przetwarzanych informacji niejawnych;
2) zapewnienie odpowiedniej ochrony fizycznej dla tych informacji;
3) możliwość utworzenia kancelarii tajnej, w przypadku przetwarzania informacji niejawnych o klauzuli „tajne" i wyższej;
4) możliwość utworzenia systemu teleinformatycznego (lub systemów teleinformatycznych) do przetwarzania informacji niejawnych o określonej klauzuli;
5) zapewnienie pracownikom niezbędnych uprawnień do dostępu do informacji niejawnych w postaci poświadczeń bezpieczeństwa lub upoważnień;
6) przeprowadzenie przez Pełnomocnika Ochrony szkolenia w zakresie ochrony informacji niejawnych.

Mając na uwadze powyższe czynniki, można podjąć próbę przedstawienia przykładowej mapy procesu przygotowania uprawnień do dostępu do informacji niejawnych dla nowozatrudnionych pracowników, którzy nie posiadają poświadczeń bezpieczeństwa, przy użyciu notacji BPMN[10] wersja 2.0.



Rys. 2. Przykładowa mapa procesu przygotowania uprawnień do dostęp do informacji niejawnych dla nowozatrudnionych pracowników, którzy nie posiadają poświadczeń bezpieczeństwa (źródło: opracowanie własne)

[10] BPMN (ang. Business Process Model and Notation) jest graficzną notacją procesu biznesowego opracowaną na podstawie normy ISO/IEC 19510:2013 Międzynarodowej Organizacji Normalizacyjnej.

ZAGROŻENIA ZWIĄZANE Z DZIAŁANIEM CZŁOWIEKA W SYSTEMIE OCHRONY INFORMACJI NIEJAWNYCH

W ujęciu encyklopedycznym „zagrożenie" to zjawisko wywołane działaniem sił natury lub człowieka, które powoduje, że poczucie bezpieczeństwa maleje bądź zupełnie znika[11]. W poruszanej problematyce zagrożenie utożsamiamy zazwyczaj z mechanizmem, który może spowodować, że rozważany system ochrony informacji niejawnych opuści stan zadowalającego działania, w którym się obecnie znajduje, i przejdzie do stanu innego, mniej zadowalającego.

Ogólnie rzecz biorąc, zagrożenia w tym systemie możemy podzielić na dwie grupy:

- zewnętrzne – wynikające z warunków otoczenia zewnętrznego systemu[12];
- wewnętrzne – wynikające z elementów składowych systemu i relacji między nimi.

Wnikliwa analiza otoczenia zewnętrznego systemu, pozwala zwykle na wyodrębnienie zagrożeń naturalnych, wynikających z działania sił przyrody oraz umyślnego lub nieumyślnego działania człowieka[13].

W poniższej tabeli zostały zaprezentowane przykłady typowych zagrożeń zewnętrznych dla systemu ochrony informacji niejawnych, które mają swoje źródło poza obszarem, gdzie jest rozmieszczona dana jednostka organizacyjna.

Tab. 1. Przykłady typowych zagrożeń zewnętrznych dla systemu ochrony informacji niejawnych w jednostce organizacyjnej (źródło: opracowanie własne)

Lp.	Typowe zagrożenia zewnętrzne	
	Naturalne	Związane z działaniem człowieka
1	Zagrożenie powodzią lub podtopieniem na skutek sąsiadujących pobliskich akwenów wodnych (np. stawy, jeziora, rzeki itp.)	Zagrożenie nieuprawnionym wtargnięciem na teren jednostki organizacyjnej osób postronnych (np. próba zamachu terrorystycznego, kradzieży itp.)
2	Zagrożenie zawaleniem się budynków na skutek: – długotrwałego braku ich remontów – silnych wichur oddziałujących na sąsiadujące z nimi stare, potężne i wysokie drzewa – uderzenia w nie samochodów ciężarowych jadących z nadmierną prędkością, które mogą stracić sterowność i wypaść z pobliskiej drogi publicznej o dużym natężeniu ruchu – intensywnych opadów śniegu mogących uszkodzić poszycie dachowe	Zagrożenie działaniem obcych służb specjalnych w postaci możliwości szczegółowej obserwacji lub podsłuchu z dogodnych miejsc w pobliskim sąsiedztwie jednostki organizacyjnej (np. okna pobliskiego budynku, ogólnodostępne parkingi itp.)

[11] Szerzej: Misiuk A., Rozważania o bezpieczeństwie, [w:] Nauka o bezpieczeństwie. Istota, przedmiot badań i kierunki rozwoju, red. Grochowski L, Letkiewicz A., Misiuk A., Szczytno 2011, s. 15–24.

[12] Obok regulacji krajowych także: Dyrektywa dotycząca bezpieczeństwa fizycznego AC/35-D/2001-REV2.

[13] Obok regulacji krajowych także: Dyrektywa dotycząca bezpieczeństwa osobowego AC/35-D/2000-REV7.

Mając na uwadze utrzymanie systemu ochrony informacji niejawnych w stanie zadowalającego działania, należy przede wszystkim zapewnić przetwarzanym informacjom następujące właściwości:

- dostępność – informacje będą dostępne dla uprawnionych interesariuszy w określonym czasie;
- integralność – informacje nie będą modyfikowane w sposób nieuprawniony;
- poufność – informacje nie będą ujawniane (przekazywane) podmiotom do tego nieuprawnionym.

W przypadku możliwej utraty którejkolwiek z powyższych właściwości, istnieje wysokie prawdopodobieństwo, że chronione informacje będą narażone na incydenty, czyli zdarzenia lub serie zdarzeń, które zagrażają ich bezpieczeństwu[14].

Szczegółowa analiza elementów składowych systemu ochrony informacji niejawnych oraz występujących między nimi relacji pozwala na wyodrębnienie zagrożeń wewnętrznych, które wynikają przeważnie z błędu człowieka. Mamy wówczas do czynienia z negatywnym zabarwieniem pojęcia „czynnika ludzkiego", przez co rozumiemy zachowanie się pojedynczej osoby lub grupy osób, należących do danej organizacji i realizujących w niej zarówno obowiązki jak i zadania wynikające z pełnionych przez siebie ról, które ma pośredni lub bezpośredni wpływ na poziom bezpieczeństwa informacji przetwarzanych w tej organizacji[15]. W poniższej tabeli zostały zaprezentowane przykłady typowych zagrożeń wewnętrznych dla systemu ochrony informacji niejawnych, które mają swoje źródło w poszczególnych elementach składowych systemu reprezentowanych przez osoby i relacjach zachodzących między nimi.

Tab. 2. Przykłady typowych zagrożeń wewnętrznych dla systemu ochrony informacji niejawnych związanych z działaniem człowieka (źródło: opracowanie własne)

Lp.	Typowe zagrożenia wewnętrzne związane z działaniem człowieka
1	Nieprzestrzeganie przepisów i procedur w zakresie ochrony informacji niejawnych przez pracowników jednostki organizacyjnej uczestniczących w procesie przetwarzania klasyfikowanych informacji (najczęściej wynikające z braku dostatecznej wiedzy)
2	Lekceważenie obowiązków przydzielonych poszczególnym pracownikom (najczęściej będące pochodną rutyny)
3	Szpiegostwo będące skutkiem udanego werbunku przez obce służby specjalne (najczęściej polega na kopiowaniu klasyfikowanych dokumentów i nieuprawnionym ich przekazywaniu osobom postronnym)
4	Wandalizm, polegający na celowym niszczeniu klasyfikowanych dokumentów lub materiałów (najczęściej będących w posiadaniu innych osób)
5	Sabotaż, jako umyślne niewypełnianie swoich obowiązków lub wypełnianie ich wadliwie z zamiarem wywołania dezorganizacji pracy jednostki organizacyjnej i wyrządzenia strat lub szkód

[14] Obok regulacji krajowych stosuje się także: Dyrektywa podstawowa INFOSEC AC/35-D/2004-REV2.

[15] Jako lex specialis stosuje się Rozporządzenie Prezesa Rady Ministrów z dnia 4 października 2011 r. w sprawie współdziałania Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa Służby Kontrwywiadu Wojskowego w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa (Dz. U. z 2011 r. Nr 220, poz. 1302).

W celu ograniczenia możliwości wystąpienia opisanych wyżej zagrożeń, należy przed rozpoczęciem procesu przetwarzania informacji niejawnych w danej jednostce organizacyjnej określić poziomy tych zagrożeń (niski, średni lub wysoki), co wynika bezpośrednio z postanowień Rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych[16]. Takie opracowanie powinno zostać poprzedzone wnikliwą analizą wszystkich istotnych czynników mogących mieć wpływ na bezpieczeństwo klasyfikowanych informacji przetwarzanych w jednostce organizacyjnej.

PODSUMOWANIE

W przestrzeni publicznej istnieje takie powiedzenie, że najsłabszym ogniwem w każdym funkcjonującym systemie jest człowiek. Potwierdzają to także opisane wcześniej przykładowe zagrożenia mogące pojawić się w obszarze bezpieczeństwa informacji niejawnych. W większości przypadkach dotyczących nieprzestrzegania przepisów o ochronie informacji niejawnych negatywną rolę odgrywa właśnie człowiek.

Powodów takiego stanu rzeczy zapewne jest wiele, a do tych najczęściej spotykanych możemy zaliczyć: pośpiech, roztargnienie, złą organizację pracy oraz lekkomyślność w działaniu. Nie można także wykluczyć innego powodu, a mianowicie lekceważenia przepisów dotyczących ochrony informacji niejawnych. Akurat w tym przypadku powodem takiego stanu rzeczy może być brak adekwatnej i nieuchronnej kary za popełnione czyny. Mówi się, że właśnie nieuchronność kary wpływa na zwiększenie poczucia odpowiedzialności oraz podnosi świadomość człowieka. Warto w tym miejscu nadmienić, że ustawa z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy[17] przewiduje dotkliwe sankcje za przestępstwa przeciwko ochronie informacji (art. 265 i art. 266) np. *Kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje niejawne o klauzuli „tajne" lub „ściśle tajne" podlega karze pozbawienia wolności od 3 miesięcy do lat 5*[18].

Czasami zbyt rutynowe podchodzenie do zadań i obowiązków może być przyczyną największych zagrożeń, gdyż trudno jest bowiem wytłumaczyć negatywne działania człowieka, takie jak: nielegalne sporządzanie kopii niejawnych dokumentów i wynoszenie ich do domu lub świadome ich niszczenie, tym bardziej, że

[16] Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. z 2012 r., poz. 683 z późn. zm.).

[17] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Dz. U. z 2018 r., poz. 652).

[18] Patrz: art. 265 §1 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy, *op. cit.*

dana osoba odbyła wcześniej szkolenie w zakresie ochrony informacji niejawnych i podpisała stosowne oświadczenie o zapoznaniu się z przepisami, szczególnie o odpowiedzialności karnej za złamanie tych przepisów.

Aby uniknąć negatywnych zdarzeń spowodowanych chociażby przez pracowników pionów ochrony należałoby się zastanowić, czy struktury organizacyjne tych komórek są wystarczająco liczne oraz czy osoby w nich zatrudnione są odpowiednio przygotowane do realizacji swoich zadań w trudnym i odpowiedzialnym obszarze. Należy także zwrócić uwagę na właściwą ocenę i wynagradzanie tych osób. Oczywiście wysokość wynagrodzenia musi iść w parze z ilością i trudnością realizowanych zadań, ale także z poziomem odpowiedzialności za ich realizację.

Na koniec pozostaje pytanie, czy można skutecznie zabezpieczyć system ochrony informacji niejawnych przed zagrożeniami związanymi z działem człowieka? Zdaniem autora, niestety nie można całkowicie wyeliminować tych zagrożeń. Jednakże można, a nawet trzeba, podjąć próby zminimalizowania wpływu czynnika ludzkiego na bezpieczeństwo informacji niejawnych przetwarzanych w jednostkach organizacyjnych.

Szczegółowa analiza przedstawionej problematyki zostanie wkrótce zaprezentowana przez autora w jego dysertacji nt. „Kierunki doskonalenia systemu ochrony informacji niejawnych w powiązaniu z ochroną danych osobowych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych".

BIBLIOGRAFIA

Cienińska B., Łunarski J., Perłowski R., Stadnicka D., *Systemy zarządzania bezpieczeństwem w przedsiębiorstwie*, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2006.

Document AC/35-D/2000-REV7 z dnia 7 stycznia 2013 r. – „Dyrektywa bezpieczeństwa osobowego".

Document AC/35-D/2001-REV2 z dnia 7 stycznia 2008 r. – „Dyrektywa bezpieczeństwa fizycznego".

Document AC/35-D/2004-REV2 z dnia 6 grudnia 2010 r. – „Dyrektywa podstawowa INFOSEC".

Document C-M(2002)49 z dnia 17 czerwca 2002 r. – „Bezpieczeństwo w ramach organizacji Traktatu Północnoatlantyckiego".

Misiuk A., *Rozważania o bezpieczeństwie, [w:] Nauka o bezpieczeństwie. Istota, przedmiot badań i kierunki rozwoju,* red. Grochowski L, Letkiewicz A., Misiuk A., Szczytno 2011.

Norma ISO/IEC 19510:2013 Międzynarodowej Organizacji Normalizacyjnej.

Rozporządzenie Prezesa Rady Ministrów z dnia 4 października 2011 r. *w sprawie współdziałania Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa Służby Kontrwywiadu Wojskowego w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa* (Dz. U. z 2011 r. Nr 220, poz. 1302).

Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. *w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych* (Dz. U. z 2012 r., poz. 683 z późn. zm.).

Ryszkowski M., Ryszkowska M., Ryszkowska M., *O wybranych tajemnicach bez tajemnic,* Instytut Ochrony Informacji i Danych Osobowych, Katowice 2011.

Sienkiewicz P., *Analiza systemowa. Podstawy i zastosowania*, Bellona, Warszawa 1994.

Sienkiewicz P., *Systemy kierowania*, Państwowe Wydawnictwo „Wiedza Powszechna", Warszawa 1989.
Strona internetowa: https://bip.abw.gov.pl/bip/informacje-niejawne–1/ochrona-informacji-nie/153,OCHRONA-INFORMACJI-NIEJAWNYCH-MIEDZYNARODOWYCH-W-SFERZE-CYWILNEJ-I-WOJSKOWEJ.html#1 – dostęp: 28 grudnia 2018 roku.
Strzoda M., *Zarządzanie informacjami w organizacji*, Akademia Obrony Narodowej, Warszawa 2004.
Ustawa z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych* (Dz. U. z 2010 r. Nr 182, poz. 1228).
Ustawa z dnia 6 czerwca 1997 r. – *Kodeks karny wykonawczy* (Dz. U. z 2018 r., poz. 652).

SUMMARY

The author describes the threats related to human activity in the system of protecting classified information. The publication also presents the pillars of the classified information protection system and its simplified model in organizational units.

Keywords: threats, personal security, protection of classified information.