DOI: 10.52694/ThPSR.2023.16

Radosław Jakubek

Ochrona informacji niejawnych – analiza wybranych zagadnień

Protection of classified information – analysis of selected issues

Celem artykułu jest przedstawienie wybranych zagadnień związanych z ochroną informacji niejawnych. W opracowaniu przedstawiono najistotniejsze elementy systemu ochrony informacji niejawnych, których prawidłowe stosowanie przyczyni się do zwiększenia bezpieczeństwa informacji niejawnych w danej jednostce organizacyjnej.

Artykuł nie będzie szczegółowym komentarzem do poszczególnych przepisów ustawy o ochronie informacji niejawnych, jednak da praktyczny pogląd, na co powinna zwrócić uwagę osoba, która jest zaangażowana w system ich ochrony, a w szczególności osoba wyznaczona do realizacji zadań przypisanych pełnomocnikowi do spraw ochrony informacji niejawnych, akcentując jednocześnie wielość i złożoność podstawowych zadań w tym zakresie.

Słowa kluczowe: informacje niejawne, ochrona informacji niejawnych, pełnomocnik ochrony, bezpieczeństwo, Służba Więzienna.

The aim of the article is to present selected issues related to the protection of classified information. The study presents the most important elements of the classified information protection system, the correct use of which will contribute to increasing the security of classified information in a given organizational unit.

The article will not be a detailed commentary on individual provisions of the Act on the protection of classified information, however, it will give a practical view of what a person who is involved in the protection system should pay attention to, and in particular a person designated

to carry out the tasks assigned to the representative for the protection of classified information, while emphasizing the multiplicity and complexity of basic tasks in this area.

Key words: classified information, protection of classified information, security representative, security, Prison Service.

Wprowadzenie

Funkcjonariusz Służby Więziennej w myśl art. 41 ustawy o Służbie Więziennej[1] składa pisemne ślubowanie, w którym zobowiązuje się m.in. przestrzegać Konstytucji Rzeczypospolitej Polskiej i wszystkich przepisów prawa, jak również tajemnic związanych ze służbą. Funkcjonariusz realizuje więc zadania, które mogą być związane z bezpieczeństwem informacji niejawnych, a zatem, musi mieć elementarną wiedzę dotyczącą prawideł w zakresie ich ochrony. W szczególności duża odpowiedzialność spoczywa na pełnomocniku do spraw ochrony informacji niejawnych (zwany dalej pełnomocnikiem ochrony), który podlega bezpośrednio kierownikowi jednostki organizacyjnej.

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[2] (zwana dalej ustawą OIN) stawia przed pełnomocnikiem ochrony mnóstwo zadań. Na jego zadania znaczący wpływ ma klauzula tajności informacji niejawnych przetwarzanych w jednostce organizacyjnej, od której będzie zależała ilość dokumentacji, jaką musi przygotować. Mając na uwadze fakt, że w jednostce organizacyjnej, w której są przetwarzane informacje niejawne[3] za ich ochronę, a w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony odpowiada nie kto inny jak kierownik jednostki organizacyjnej[4], kluczowe znaczenie ma jednak rola pełnomocnika ochrony, który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych[5].

[1] Ustawa z dnia 9 kwietnia 2010 r. o Służbie Więziennej (t.j. Dz. U. z 2023 r., poz. 1683 z późn. zm.).
[2] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).
[3] Ibidem, art. 2 pkt 5, przetwarzanie informacji niejawnych – są to wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie.
[4] Ibidem, art. 14 ust. 1.
[5] Ibidem, art. 14 ust. 2.

W myśl art. 15 ust. 4 ustawy OIN kierownik jednostki organizacyjnej może powierzyć pełnomocnikowi ochrony wykonywanie innych zadań, jeżeli ich realizacja nie naruszy prawidłowego wykonywania zadań pełnomocnika. Praktyka taka jest często stosowana w jednostkach organizacyjnych Służby Więziennej, w których funkcjonariusze, pełniąc służbę w różnych komórkach organizacyjnych, zostają wyznaczeni do pełnienia funkcji pełnomocnika ochrony. Biorąc powyższe pod uwagę, aby realizacja zadań przypisanych pełnomocnikowi ochrony przebiegała prawidłowo, musi on mieć specjalistyczną wiedzę w zakresie zapewnienia bezpieczeństwa informacji niejawnych, i dlatego podlega ustawowemu przeszkoleniu przeprowadzanemu przez Agencję Bezpieczeństwa Wewnętrznego (zwana dalej ABW).

Należy zaznaczyć, iż zgodnie z art. 10 ust. 3 ustawy OIN, ABW realizuje swoje zadania w odniesieniu do tzw. sfery cywilnej, czyli jednostek organizacyjnych i osób podlegających ustawie OIN, a więc podmiotów, które zostały określone w art. 1 ust. 2 ustawy OIN, z wyłączeniem:

1) Ministerstwa Obrony Narodowej oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;
2) ataszatów obrony w placówkach zagranicznych;
3) żołnierzy w służbie czynnej wyznaczonych na stanowiska służbowe w innych jednostkach organizacyjnych niż wymienione powyżej[6].

W jednostkach organizacyjnych wymienionych w pkt. 1-3, organem nadzoru w zakresie funkcjonowania systemu ochrony informacji niejawnych jest Służba Kontrwywiadu Wojskowego. Tym samym Służba Więzienna podlega nadzorowi ze strony ABW, która ma nadzór nad tzw. sferą cywilną. Biorąc pod uwagę powyższe, przy omawianiu poszczególnych zagadnień, będę się zawsze odnosił do organu właściwego dla Służby Więziennej, jakim jest ABW.

W niniejszym artykule przedstawione zostały wybrane obszary związane z ochroną informacji niejawnych, których prawidłowe rozumienie i odpowiednie wdrożenie w jednostce organizacyjnej ma istotne znaczenie dla organizacji systemu ochrony informacji niejawnych.

[6] *Wobec jakich podmiotów właściwą rzeczowo jest Agencja Bezpieczeństwa Wewnętrznego?,* https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/organizacja-ochrony-in/145,ORGANIZACJA-OCHRONY-INFORMACJI-NIEJAWNYCH.html#11 [dostęp: 18.09.2023].

Informacje niejawne – definicja

Regulacja art. 1 ust. 1 ustawy OIN wprowadza przedmiotowe rozumienie pojęcia „informacje niejawne". Treść powyższego artykułu wskazuje, że są to takie informacje, „których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania".

Ujawnienie informacji jest pojęciem szerokim. Swoim zakresem obejmuje to, co nazywamy wyjawieniem tajemnicy, udzieleniem komuś wiadomości, która stanowi tajemnicę, czy też zakomunikowaniem takiej wiadomości, rozpowszechnieniem oraz opublikowaniem[7]. Nieuprawnione ujawnienie informacji należy rozumieć, jako takie, które odbywa się bez prawnej legitymacji, co w konsekwencji spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne[8]. Należy zwrócić uwagę, iż działanie w postaci ujawnienia ma charakter jednorazowy, gdyż osoba, która ujawnia informację niejawną, czyni ją jawną dla kolejnych odbiorców[9]. Forma ujawnienia informacji niejawnej, nie została sprecyzowana przez ustawodawcę. Należy zatem przyjąć, iż ewentualne ujawnienie może nastąpić w każdej możliwej formie. Jako przykład można wskazać formę ustnej wypowiedzi, ujawnienie za pośrednictwem środków masowego przekazu lub jako ujawnienie dokumentu w postaci pisemnej (okazanie dokumentu) czy również za pośrednictwem technicznych środków przekazu, np. faksu[10].

Należy zaznaczyć, iż w ustawie OIN zrezygnowano z podziału informacji niejawnych na tajemnicę państwową i tajemnicę służbową. Dla ustawodawcy istotą ochrony informacji niejawnych jest interes państwa. Tym samym zrezygnowano z wykazu rodzajów informacji, które mogą stanowić tajemnicę państwową, stanowiącego załącznik do poprzednio obowiązującej ustawy o ochronie informacji niejawnych[11]. Biorąc pod uwagę filozofię przyjętą przez ustawodawcę, należy stwierdzić, iż

[7] I. Stankowska, *Komentarz. Ustawa o ochronie informacji niejawnych*, Warszawa 2014, s. 15.
[8] Ł. Nosarzewski, B. Opaliński, P. Szustakiewicz, *Ustawa o ochronie informacji niejawnych. Komentarz.*, Warszawa 2023, s. 3.
[9] I. Stankowska, op. cit., s. 15.
[10] Ł. Nosarzewski, B. Opaliński, P. Szustakiewicz, op. cit., s. 3.
[11] I. Stankowska, op. cit., s. 16.

w obowiązującym stanie prawnym informacje niejawne klasyfikujemy na podstawie dyspozycji wynikającej z art. 5 ustawy OIN.

Wprowadzenie zwrotu informacje niejawne i rezygnacja z podziału na tajemnicę państwową i służbową skutkuje zatem koniecznością zmiany przepisów ustawy o Służbie Więziennej. Artykuł 161 przedmiotowej ustawy, który merytorycznie odpowiada za sprawy dotyczące oświadczeń majątkowych funkcjonariuszy, w ust. 5 brzmi następująco: „Informacje zawarte w oświadczeniu, o którym mowa w ust. 1, stanowią tajemnicę służbową w rozumieniu przepisów o ochronie informacji niejawnych, chyba że funkcjonariusz, który złożył oświadczenie, wyraził pisemną zgodę na ich ujawnienie. (…)". Biorąc pod uwagę rezygnację z podziału informacji niejawnych na tajemnicę państwową i tajemnicę służbową, zasadna jest zmiana wyżej wymienionego przepisu.

Bezpieczeństwo osobowe

Sprawy związane z bezpieczeństwem osobowym zostały uregulowane przez przepisy ustawy OIN w rozdziale piątym – Bezpieczeństwo osobowe. Kluczowe znaczenie w tym obszarze bezpieczeństwa informacji niejawnych ma jednak art. 4 ust. 1 ustawy OIN zgodnie, z którym „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 wykonywania czynności zleconych."

Biorąc pod uwagę powyższą normę, należy zwrócić uwagę dwa elementy:

1) rękojmię zachowania tajemnicy
2) zasadę „need to know"[12].

Definicja rękojmi zachowania tajemnicy została określona w art. 2 pkt 2 ustawy OIN, zgodnie z którym „rękojmią zachowania tajemnicy jest zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego".

Natomiast zasada „need to know" oznacza, że dostęp jest ograniczony tylko i wyłącznie do konkretnych informacji, które są niezbędne

[12] Ibidem, s. 31.

do wykonywania przez daną osobę obowiązków służbowych[13]. Zgodnie ze wskazaną zasadą osoba, która w wyniku przeprowadzonego względem niej postępowania sprawdzającego uzyskuje dostęp do informacji niejawnych o klauzuli „tajne", nie jest jednocześnie upoważniona do dostępu do wszystkich informacji niejawnych oznaczonych klauzulą „tajne" lub niższą, ale ma dostęp do tych, które są jej niezbędne do realizacji zadań służbowych[14].

Biorąc pod uwagę definicję rękojmi zachowania tajemnicy, należy stwierdzić, że nie zawsze dostęp do informacji niejawnych będzie związany z przeprowadzeniem postępowania sprawdzającego. Ustawodawca zdecydował o rezygnacji z przeprowadzenia postępowania sprawdzającego i wydawania dokumentu w postaci poświadczenia bezpieczeństwa dla informacji niejawnych do poziomu „zastrzeżone"[15]. Zgodnie z rozstrzygnięciami wynikającymi z art. 21 ust. 4 ustawy OIN, dostęp do informacji niejawnych o klauzuli „zastrzeżone" możliwy jest, jeżeli są spełnione następujące warunki:

1) upoważnienie w formie pisemnej wydane przez kierownika jednostki organizacyjnej, jeżeli dana osoba nie posiada poświadczenia bezpieczeństwa,
2) odbycie szkolenia w zakresie ochrony informacji niejawnych.

Ustawa OIN ani żaden akt wykonawczy do ustawy nie określa wzoru upoważnienia do dostępu do informacji niejawnych o klauzuli „zastrzeżone". Warto w tym zakresie korzystać z materiałów udostępnionych do pobrania przez ABW na stronach Biuletynu Informacji Publicznej ABW[16].

W przypadku konieczności dopuszczenia do pracy lub pełnienia służby na stanowiskach albo zlecenia prac związanych z dostępem do *informacji niejawnych* o klauzuli „poufne" lub wyższej, również muszą być spełnione kumulatywnie dwa warunki:

1) uzyskanie poświadczenia bezpieczeństwa w wyniku przeprowadzonego postępowania sprawdzającego;

[13] *Jakie są warunki dostępu do informacji niejawnych NATO, UE i ESA?,* https://bip.abw.gov.pl/bip/informacje-niejawne-1/ochrona-informacji-nie/153,OCHRONA-INFORMACJI-NIEJAWNYCH-MIEDZYNARODOWYCH-W-SFERZE-CYWILNEJ-I-WOJSKOWEJ.html [dostęp:18.09.2023].

[14] I. Stankowska, op. cit., s. 31.

[15] Ibidem, s 82.

[16] *wzór upoważnienia do dostępu do informacji „zastrzeżone"*, https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/materialy-do-pobrania/152,MATERIALY-DO-POBRANIA.html [dostęp: 18.09.2023].

2) odbycie szkolenia w zakresie ochrony informacji niejawnych[17].

Efektem pozytywnie zakończonego postępowania sprawdzającego będzie wydanie osobie sprawdzanej przez organ prowadzący postępowanie poświadczenia bezpieczeństwa uprawniającego do dostępu do informacji niejawnych[18]. W postępowaniu sprawdzającym bierze się pod uwagę klauzulę tajności informacji niejawnych, które mają być udostępnione osobie sprawdzanej. Rozróżniamy dwa rodzaje postępowań sprawdzających:

1) zwykłe postępowanie sprawdzające – przeprowadzane w sytuacji ubiegania się o poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych o klauzuli „ poufne", oraz
2) poszerzone postępowanie sprawdzające – przeprowadzane w sytuacji ubiegania się o wydanie poświadczenia bezpieczeństwa uprawniającego do dostępu do informacji niejawnych o klauzuli „tajne" lub „ściśle tajne".

Analizując przepisy ustawy OIN, należy zaznaczyć, iż mimo że ustawodawca wprowadza jednoznaczny podział postępowań sprawdzających, to jednak wprowadza pewne wyłączenie. Z postępowań zwykłych wyłącza, wpisując je do postępowań poszerzonych, te, które, mimo iż mogą łączyć się z dostępem do informacji niejawnych o klauzuli „poufne", są postępowaniami sprawdzającymi prowadzonymi wobec osób mających istotną rolę w ochronie informacji niejawnych. Wyłączenie ustawowe dotyczy:

1) pełnomocników ochrony, ich zastępców, a także kandydatów na te stanowiska;
2) kierowników jednostek organizacyjnych, w których są przetwarzane informacje niejawne o klauzuli „poufne" lub wyższej,
3) osób ubiegających się o dostęp do *informacji niejawnych* międzynarodowych lub o dostęp, który ma wynikać z umowy międzynarodowej zawartej przez Rzeczpospolitą Polską.

Celem ustawodawcy było, aby wyżej wymienione osoby podlegały sprawdzeniu przez właściwą służbę (w przypadku SW przez ABW), a nie przez pełnomocnika ochrony. Wynika, to głównie z ich szczególnej roli i znaczenia dla systemu ochrony informacji niejawnych, zobowiązań

[17] Art. 21 ust. 1 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.), Wyjątek – zgodnie z przepisem art. 34 ust.1 ustawy OIN nie przeprowadza się postępowania sprawdzającego, jeżeli osoba, której ma ono dotyczyć, przedstawi poświadczenie bezpieczeństwa odpowiednie do wymaganej klauzuli tajności, z wyjątkiem poświadczeń bezpieczeństwa wydanych w wyniku przeprowadzenia postępowań sprawdzających przez AW, CBA, Służbę Ochrony Państwa, Policję, Służbę Więzienną, SWW, Straż Graniczną oraz Żandarmerię Wojskową, które zachowują ważność wyłącznie w podmiotach, w których zostały wydane.

[18] Ibidem, art. 29 ust. 1.

międzynarodowych względem organizacji międzynarodowych oraz uniknięcia sytuacji, gdzie pełnomocnik ochrony prowadzi postępowanie sprawdzające wobec swojego przełożonego[19].

Należy zaznaczyć, iż w myśl art. 23 ust. 5 ustawy OIN m.in. Służba Więzienna samodzielnie przeprowadza postępowania sprawdzające oraz kontrolne postępowania sprawdzające. Powyższe uprawnienie dotyczy przeprowadzania postępowań sprawdzających wobec funkcjonariuszy i pracowników oraz osób ubiegających się o przyjęcie do służby lub pracy w Służbie Więziennej[20]. Znacząca rola w ramach prowadzonych postępowań sprawdzających (w szczególności poszerzonych postępowań sprawdzających) została przypisana pełnomocnikowi ochrony Centralnego Zarządu Służby Więziennej. Przeprowadza on poszerzone postępowania sprawdzające wobec funkcjonariuszy i pracowników oraz osób ubiegających się o przyjęcie do służby lub pracy w Służbie Więziennej. Powyższe zadanie nie dotyczy jednak postępowań przeprowadzanych wobec Dyrektora Generalnego Służby Więziennej, Szefa Inspektoratu Wewnętrznego Służby Więziennej oraz osób przewidzianych na te stanowiska, a także pełnomocników ochrony, zastępców pełnomocników ochrony oraz osób przewidzianych na te stanowiska[21]. Poszerzone postępowanie sprawdzające względem wyżej wymienionych przeprowadza ABW[22].

Należy pamiętać, iż poświadczenia bezpieczeństwa uzyskane w ramach postępowań sprawdzających prowadzonych przez podmioty określone w art. 23 ust. 5 ustawy OIN (m.in. Służbę Więzienną), zachowują ważność tylko i wyłącznie w okresie pracy lub służby w podmiocie, w którym były wydane. Sytuacja taka oznacza, że po zakończeniu służby lub pracy w Służbie Więziennej osoba, która będzie starała się podjąć pracę związaną z dostępem do informacji niejawnych w innej instytucji, będzie zobowiązana do poddania się ponownemu postępowaniu sprawdzającemu[23].

[19] I. Stankowska, op. cit., s. 83-84.

[20] W ramach Służby Więziennej obowiązuje Zarządzenie nr 58/23 Dyrektora Generalnego Służby Więziennej z dnia 31 sierpnia 2023 r. w sprawie przeprowadzania postępowań sprawdzających wobec funkcjonariuszy i pracowników oraz osób ubiegających się o przyjęcie do służby lub pracy w Służbie Więziennej (wcześniej Zarządzenie nr 4/2011 Dyrektora Generalnego Służby Więziennej z dnia 11 stycznia 2011 r. w sprawie przeprowadzania postępowań sprawdzających wobec funkcjonariuszy i pracowników oraz kandydatów do służby lub pracy w Służbie Więziennej).

[21] § 3 pkt 1 i 2 zarządzenia nr 58/23 Dyrektora Generalnego Służby Więziennej z dnia 31 sierpnia 2023 r. w sprawie przeprowadzania postępowań sprawdzających wobec funkcjonariuszy i pracowników oraz osób ubiegających się o przyjęcie do służby lub pracy w Służbie Więziennej.

[22] Art. 23 ust. 3 pkt 1 i 2 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).

[23] I. Stankowska, op. cit., s. 87.

Elementem bezpieczeństwa osobowego, którego nie można pominąć, jest monitorowanie okresów ważności wydanych poświadczeń bezpieczeństwa. Kluczowy w tym zakresie jest art. 32 ust. 1 ustawy OIN, zgodnie z którym „na pisemny wniosek kierownika jednostki organizacyjnej lub osoby uprawnionej do obsady stanowiska, złożony co najmniej na 6 miesięcy przed upływem terminu ważności poświadczenia bezpieczeństwa, właściwy organ przeprowadza kolejne postępowanie sprawdzające". Kierownik jednostki organizacyjnej jest organem, który odpowiada za ochronę informacji niejawnych w swojej jednostce. W praktyce dużą rolę w tym zakresie odgrywa pełnomocnik ochrony, który przygotowuje wymagane wnioski. To pełnomocnik ochrony, jako osoba odpowiadająca za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych czuwa nad okresami ważności poświadczeń bezpieczeństwa, gdyż jednym z jego zadań jest prowadzenie aktualnego wykazu osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do *informacji niejawnych*, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto[24]. Tym samym prowadzenie wyżej wymienionego wykazu znacząco ułatwia monitorowanie wymogów określonych w art. 32 ust. 1 ustawy OIN.

Istotny w zakresie rozumienia dostępu do informacji niejawnych jest również art. 29 ust. 3 ustawy OIN, który określa terminy ważności poświadczeń bezpieczeństwa[25] oraz art. 29 ust 4 ustawy OIN, z którego można wywieść pojęcie tzw. kaskady poświadczeń bezpieczeństwa. Przedmiotowe pojęcie oznacza, iż osoba, która dla przykładu ma poświadczenie bezpieczeństwa do klauzuli „ściśle tajne" przez okres 5 lat, będzie mogła na tej podstawie mieć również dostęp do informacji niejawnych o klauzuli „tajne" przez 7 lat, a o klauzuli „poufne" przez 10 lat. Należy również zaznaczyć, iż zgodnie z art. 21 ust. 4 pkt 1 ustawy OIN dokumentem, który uprawnia daną osobę do dostępu do informacji niejawnych o klauzuli „zastrzeżone" oprócz pisemnego upoważnienia wydanego przez kierownika jednostki organizacyjnej, może być również posiadanie przez tę osobę ważnego poświadczenia bezpieczeństwa. Nasuwa się zatem wniosek,

[24] Ibidem, s. 130.

[25] Poświadczenie bezpieczeństwa wydaje się na okres 10 lat – w przypadku dostępu do informacji niejawnych o klauzuli „poufne"; 7 lat – w przypadku dostępu do informacji niejawnych o klauzuli „tajne"; 5 lat – w przypadku dostępu do informacji niejawnych o klauzuli „ściśle tajne".

że ważne poświadczenie bezpieczeństwa będzie uprawniało do dostępu do klauzuli „zastrzeżone" przez 10 lat od dnia jego wydania[26].

Wzór poświadczeń bezpieczeństwa został określony w rozporządzeniu Prezesa Rady Ministrów w sprawie wzorów poświadczeń bezpieczeństwa[27].

Szkolenia w zakresie ochrony informacji niejawnych

Kolejnym warunkiem koniecznym do dostępu do informacji niejawnych jest odbycie szkolenia w zakresie ich ochrony. Problematyka szkoleń z zakresu ochrony informacji niejawnych wynika z przepisów ustawy OIN zawartych w rozdziale czwartym – Szkolenia w zakresie ochrony informacji niejawnych. Dodatkowo ustawa OIN przewiduje w art. 52 ust. 4 konieczność odbycia szkoleń specjalistycznych przez osoby zajmujące stanowiska inspektora systemu teleinformatycznego oraz administratora systemu.

Szkolenia wynikające z art. 19 ustawy OIN przeprowadza się nie rzadziej niż raz na 5 lat[28]. Okres na przeprowadzenie kolejnego szkolenia jest jednakowy dla wszystkich osób mających dostęp do informacji niejawnych. Nie ma tutaj znaczenia zajmowane stanowisko ani klauzula tajności dokumentów, do jakich ma mieć dostęp dana osoba. Wydaje się jednak, że przeprowadzanie częstszych szkoleń jest w niektórych przypadkach w pełni uzasadnione. Dotyczy to przede wszystkim sytuacji, gdzie dochodzi do istotnych zmian przepisów regulujących problematykę związaną z ochroną informacji niejawnych[29]. Za znaczące zmiany można uznać np. nowelizacje ustawy OIN, zmiany aktów wykonawczych do ustawy OIN, zmiany zarządzeń wydanych przez kierowników podmiotów, o których mowa w art. 47 ust. 3 ustawy OIN. Zamiany przepisów w zakresie ochrony informacji niejawnych są względnie częste. Interpretacja przepisów bywa zróżnicowana i nawet z tego powodu szkolenie nie może być traktowane jako akt jednorazowy. Za powtarzalnością szkoleń przemawia

[26] *Co oznacza pojęcie kaskady ważności poświadczeniabezpieczeństwa?,* https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/bezpieczenstwo-osobowe/146,BEZPIECZENSTWO-OSOBOWE.html#11 [dostęp: 25.09.2023].

[27] Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa (t.j. Dz. U. z 2015 r., poz. 220).

[28] Art. 19 ust. 3 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).

[29] M. Anzel, *Poradnik specjalisty ochrony informacji niejawnych*, Poznań 2015, s. 30.

również potrzeba ciągłego identyfikowania zagrożeń i szacowania ryzyka w aspekcie zarządzania bezpieczeństwem informacji niejawnych[30].

Celem przeprowadzenia szkolenia w zakresie ochrony informacji niejawnych jest zapoznanie osoby szkolonej z:

1) przepisami dotyczącymi ochrony informacji niejawnych, a także odpowiedzialności karnej, dyscyplinarnej i służbowej za ich naruszenie, w szczególności za nieuprawnione ujawnienie informacji niejawnych;
2) zasadami ochrony informacji niejawnych w zakresie, który jest niezbędny do wykonywania pracy lub pełnienia służby, z uwzględnieniem zasad zarządzania ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowania ryzyka;
3) sposobami ochrony informacji niejawnych, a także postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia[31].

Szkolenie z zakresu ochrony informacji niejawnych, zgodnie z art. 20 ust. 1 ustawy OIN kończy się wydaniem zaświadczenia o przeszkoleniu. Osoba, która odbyła szkolenie, odbierając zaświadczenie, składa pisemne oświadczenie o zapoznaniu się z przepisami o ochronie informacji niejawnych[32]. Wzory zaświadczeń stwierdzających odbycie odpowiedniego szkolenia określa rozporządzenie Prezesa Rady Ministrów w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego[33]. Natomiast w odniesieniu do oświadczenia o zapoznaniu się z przepisami o ochronie informacji niejawnych, możliwe jest jego złożenie w formie oddzielnego dokumentu albo w formie adnotacji złożonej na kopii zaświadczenia lub na drugim egzemplarzu zaświadczenia[34]. Ustawa OIN nie narzuca wzoru przedmiotowego oświadczenia, ale

[30] S. Zalewski, *Informacje niejawne we współczesnym świecie*, Warszawa 2017, s. 70.
[31] Art. 19 ust. 1 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.)
[32] Ibidem, art. 20 ust. 1.
[33] Rozporządzenie Prezesa Rady Ministrów z dnia 9 lipca 2020 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego (Dz. U. z 2020 r., poz. 1256).
[34] *Jaki dokument potwierdza przeprowadzenie szkolenia?*, https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/szkolenia/147,SZKOLENIA.html [dostęp: 18.09.2023].

warto w tym zakresie korzystać z materiałów udostępnionych do pobrania przez ABW na stronach Biuletynu Informacji Publicznej ABW[35].

Pełnomocnik ochrony, choć nie wynika to z ustawy OIN oraz aktów wykonawczych wydanych na jej podstawie, może prowadzić dodatkową dokumentację dotyczącą prowadzonych przez siebie szkoleń z zakresu ochrony informacji niejawnych, która będzie porządkowała całokształt prac związanych ze szkoleniami w jednostce organizacyjnej. Praktycznym wydaje się prowadzenie następującej dokumentacji dotyczącej realizowanych szkoleń: ramowego programu szkoleń w jednostce, konspektu szkolenia dla osób mających mieć dostęp do informacji niejawnych w jednostce, listy obecności uczestników szkolenia, wykazu osób przeszkolonych oraz rejestru zaświadczeń o odbyciu przeszkolenia.

Zakres podmiotowy szkolenia dotyczącego ochrony informacji niejawnych został określony w art. 19 ust. 2 ustawy OIN. Szkolenia pełnomocników ochrony i ich zastępców oraz osób przewidzianych na te stanowiska przeprowadza w odniesieniu do Służby Więziennej — ABW. Kolejną grupą są kierownicy jednostek organizacyjnych, w których przetwarzane są informacje niejawne o klauzulach „tajne" i „ściśle tajne", gdzie szkolenia przeprowadza ABW wspólnie z pełnomocnikiem ochrony. Natomiast dla kierowników jednostek organizacyjnych, w których przetwarza się tylko informacje niejawne o klauzuli „zastrzeżone" lub „poufne", a także dla pozostałych osób zatrudnionych, pełniących służbę lub wykonujących czynności zlecone w jednostce organizacyjnej, odpowiednie szkolenie przeprowadza pełnomocnik ochrony.

Szkolenia w zakresie ochrony informacji niejawnych przeprowadzane przez ABW względem funkcjonariuszy i pracowników Służby Więziennej są odpłatne. Koszty szkolenia prowadzonego przez ABW pokrywa jednostka organizacyjna, w której osoba szkolona jest zatrudniona, pełni służbę lub wykonuje czynności zlecone[36].

Pełnomocnik ochrony, zgodnie z przepisami ustawy OIN, organizuje szkolenia dla osób zatrudnionych, pełniących służbę w jednostce organizacyjnej lub wykonujących na jej rzecz czynności zlecone. Sformułowanie „organizacja szkolenia" w opinii ABW oznacza, iż pełnomocnik ochrony nie zawsze musi samodzielnie, bezpośrednio przeprowadzać szkolenie z zakresu ochrony informacji niejawnych, w szczególności w przypadku

[35] *oświadczenie o zapoznaniu się z przepisami o.i.n.*, https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/materialy-do-pobrania/152,MATERIALY-DO-POBRANIA.html [dostęp: 18.09.2023].
[36] Art. 19 ust. 4 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).

tych jednostek organizacyjnych, które mają rozbudowaną strukturę. Obowiązkiem pełnomocnika ochrony lub jego zastępcy jest jednak wystawienie i podpisanie zaświadczenia stwierdzającego odbycie szkolenia w zakresie ochrony informacji niejawnych[37], a omówienie niektórych zagadnień może zlecać osobom mającym odpowiednie wykształcenie i doświadczenie np. radcom prawnym[38].

Ustawa OIN przewiduje możliwość odstąpienia od szkolenia z zakresu ochrony informacji niejawnych. W takiej sytuacji osoba podejmująca pracę lub rozpoczynająca pełnienie służby albo wykonywanie czynności zleconych musi przedstawić pełnomocnikowi ochrony aktualne zaświadczenie o odbyciu szkolenia[39]. Zwrot „może odstąpić" wynikający z art. 19 ust. 3 ustawy OIN oznacza zatem fakultatywność decyzji pełnomocnika ochrony w zakresie przeprowadzenia szkolenia.

Ustawodawca wprowadza również obowiązki w zakresie odbycia specjalistycznych szkoleń z zakresu bezpieczeństwa teleinformatycznego. Szkolenia specjalistyczne określone są w art. 52 ust. 4 ustawy OIN, zgodnie z którym stanowiska lub funkcje inspektora bezpieczeństwa teleinformatycznego[40] oraz administratora systemu[41] mogą zajmować lub pełnić osoby spełniające wymagania określone w art. 16 ustawy OIN, po odbyciu specjalistycznych szkoleń z zakresu bezpieczeństwa teleinformatycznego[42]. Szkolenia specjalistyczne prowadzone są względem Służby Więziennej przez ABW. Ustawa OIN nie wskazuję, że szkolenia specjalistyczne w powyższym zakresie muszą być przeprowadzane co 5 lat jak szkolenia, które wynikają z art. 19 ustawy.

Należy zaznaczyć, że stanowiska lub funkcję inspektora bezpieczeństwa teleinformatycznego oraz administratora systemu mogą więc zajmować lub pełnić tylko osoby, które odbyły dwa rodzaje szkoleń, czyli szkolenie

---

[37] *Co to oznacza, że pełnomocnik ochrony organizuje szkolenia w zakresie ochrony informacji niejawnych?,* https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/szkolenia/147,SZKOLENIA.html [dostęp: 18.09.2023].

[38] A. Smykla, *Zmiany w przepisach dotyczących ogólnych zasad systemu oraz klasyfikowania informacji niejawnych,* [w:] Z. Nawrocki(red.) *Ochrona informacji niejawnych. Poradnik praktyczny dla osób i instytucji przetwarzających informacje niejawne*, Warszawa 2011, s. 24.

[39] Art. 19 ust. 3 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).

[40] Inspektor bezpieczeństwa teleinformatycznego jest odpowiedzialny za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego, w którym przetwarza się informacje niejawne ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji.

[41] Administrator systemu jest odpowiedzialny za funkcjonowanie systemu teleinformatycznego, w którym przetwarza się informacje niejawne oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego. Nie może jednocześnie pełnić funkcji inspektora bezpieczeństwa teleinformatycznego.

[42] Art. 52 ust. 4 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).

określone w art. 19 ust. 1 ustawy OIN oraz szkolenie specjalistyczne wynikające z art. 52 ust. 4 ustawy OIN[43].

Bardzo ważnym elementem w ramach zapewnienia bezpieczeństwa teleinformatycznego jest również szkolenie użytkowników systemu teleinformatycznego służącego do przetwarzania informacji niejawnych. Obowiązek ten nie wynika wprost z przepisów ustawy OIN, tylko z rozporządzenia Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego[44]. Zgodnie z §7 wyżej wymienionego rozporządzenia „Przed dopuszczeniem osób do pracy w systemie teleinformatycznym kierownik jednostki organizacyjnej zapewnia ich przeszkolenie z zakresu bezpieczeństwa teleinformatycznego oraz zapoznanie z procedurami bezpiecznej eksploatacji w zakresie, jaki ich dotyczy". Szkolenie w powyższym zakresie jest przeprowadzane przez administratora systemu[45].

Należy zaznaczyć, iż zagadnienia związane z ochroną informacji niejawnych stanowią również element szkoleń funkcjonariuszy i pracowników Służby Więziennej. Zarządzenie Dyrektora Generalnego Służby Więziennej w sprawie programów szkolenia wstępnego, zawodowego i specjalistycznego w Służbie Więziennej dla funkcjonariuszy i pracowników[46] zawiera tematykę związaną z ochroną informacji niejawnych. Na różnych etapach służby lub pracy, w ramach różnych rodzajów szkoleń, omawiane są zagadnienia związane z ochroną informacji niejawnych. Na szczególną uwagę zasługują szkolenia specjalistyczne dla kierowników kancelarii tajnych w jednostkach organizacyjnych Służby Więziennej, które są organizowane przez Zespół Ochrony Informacji Niejawnych Centralnego Zarządu Służby Więziennej[47]. Przedmiotowe szkolenia przygotowują odpowiednio kierowników kancelarii tajnych do wykonywania przydzielonej funkcji, co wymaga zdobycia przez nich wiedzy z zakresu głównych uregulowań prawnych dotyczących ochrony

[43] W celu objęcia stanowiska lub funkcji inspektora bezpieczeństwa teleinformatycznego albo administratora systemu oprócz wymogu posiadania odpowiednich szkoleń, należy spełnić inne wymogi określone w art. 16 ustawy OIN – posiadanie obywatelstwa polskiego; posiadanie odpowiedniego poświadczenia bezpieczeństwa lub upoważnienia do przetwarzania informacji niejawnych o klauzuli „zastrzeżone".

[44] Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego, (Dz. U. z 2011 r. nr 159 poz. 948).

[45] Ibidem, § 13 pkt 1.

[46] Zarządzenie nr 61/18 Dyrektora Generalnego Służby Więziennej z dnia 20 grudnia 2018 r. w sprawie programów szkolenia wstępnego, zawodowego i specjalistycznego w Służbie Więziennej dla funkcjonariuszy i pracowników (z późn. zm.).

[47] Zespół Ochrony Informacji Niejawnych stanowi jedną z komórek organizacyjnych Centralnego Zarządu Służby Więziennej.

informacji niejawnych oraz organizacji i zasad funkcjonowania kancelarii tajnych w jednostkach organizacyjnych Służby Więziennej. Podczas szkoleń nabywana jest również wiedza i umiejętności praktyczne dotyczące właściwego prowadzenia rejestrów dokumentów, ich wewnętrznego obiegu, a także ekspediowania dokumentów zawierających informacje niejawne na zewnątrz jednostki organizacyjnej[48].

Znaczenie ochrony informacji niejawnych w Służbie Więziennej przejawia się również poprzez organizowanie kursokonferencji dla kierowników jednostek organizacyjnych Służby Więziennej, dotyczących szeroko rozumianego bezpieczeństwa informacyjnego, którego element stanowi m.in. ochrona informacji niejawnych. Ponadto, dla pełnomocników ochrony i kierowników kancelarii tajnych oraz funkcjonariuszy realizujących zadania w ramach poszerzonych postępowań sprawdzających organizowane są narady instruktażowo – szkoleniowe. Przedmiotowe kursokonferencje i narady organizowane są przez Zespół Ochrony Informacji Niejawnych Centralnego Zarządu Służby Więziennej. W opinii autora, jako osoby mającej doświadczenie w pełnieniu funkcji pełnomocnika ochrony w dwóch jednostkach organizacyjnych Służby Więziennej i uczestnika tego rodzaju narad instruktażowo – szkoleniowych, uczestnictwo w nich przekłada się pozytywnie na realizację obowiązków przypisanych pełnomocnikowi ochrony.

Jedynym z zadań pełnomocnika ochrony wynikającym z art. 15 ust. 1 pkt 2 ustawy OIN jest także zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne[49]. Podczas szkolenia przeprowadzanego przez ABW względem kandydata na pełnomocnika ochrony, a następnie dalszych okresowych szkoleń, omawiane są zagadnienia dotyczące bezpieczeństwa teleinformatycznego. Sama ustawa OIN nie przewiduje jednak obowiązku odbycia przez pełnomocnika ochrony specjalistycznego szkolenia z zakresu bezpieczeństwa teleinformatycznego, jakie muszą odbyć inspektor bezpieczeństwa teleinformatycznego i administrator systemu. Biorąc pod uwagę zadania pełnomocnika w zakresie bezpieczeństwa teleinformatycznego, zasadnym

[48] Szczegółowe założenia szkolenia specjalistycznego dla kierowników kancelarii tajnych w jednostkach organizacyjnych Służby Więziennej określające m.in. cele, czas, plan, program szkolenia zostało określone w załączniku nr 3 – Programy szkoleń specjalistycznych w Służbie Więziennej dla funkcjonariuszy i pracowników, do zarządzenia nr 61/18 Dyrektora Generalnego Służby Więziennej z dnia 20 grudnia 2018 r. w sprawie programów szkolenia wstępnego, zawodowego i specjalistycznego w Służbie Więziennej dla funkcjonariuszy i pracowników (z późn. zm.).

[49] Art. 15 ust. 1 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).

wydaje się jednak odbycie takiego szkolenia. Oczywiście istotna jest tutaj kwestia możliwości finansowych jednostki organizacyjnej. Praktyka autora w zakresie pełnienia funkcji pełnomocnika ochrony, który odbył przedmiotowe szkolenie, pokazuje, że korzyści płynące ze szkolenia mają pozytywny wpływ na realizację ustawowych zadań pełnomocnika ochrony, a tym samym na bezpieczeństwo teleinformatyczne jednostki.

Środki bezpieczeństwa fizycznego

Istotnym przepisem ustawy OIN dotyczącym bezpieczeństwa fizycznego jest art. 8, z którego można wywieść ogólne zasady ochrony informacji niejawnych. Zarówno pkt 2 i 3 art. 8 odwołuje się do bezpieczeństwa fizycznego informacji niejawnych. W szczególności istotny jest przepis art. 8 pkt 3[50], zgodnie z którym „Informacje niejawne, którym nadano określoną klauzulę tajności: (…) muszą być chronione, odpowiednio do nadanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w ustawie i przepisach wykonawczych wydanych na jej podstawie". Powyższy przepis wskazuje, iż elementem kluczowym jest klauzula tajności przetwarzanych informacji niejawnych, która wyznacza poziom ich ochrony. Tym samym, wyższa klauzula tajności generuje koszty związane z zapewnieniem odpowiedniego poziomu ochrony informacji niejawnych[51].

Przepisy, które bardziej precyzyjnie regulują obszar bezpieczeństwa fizycznego, określone zostały w innym rozdziale ustawy OIN, a dokładniej w rozdziale 7 zatytułowanym: Kancelarie tajne. Środki bezpieczeństwa fizycznego. Celem uregulowań tego rozdziału jest wprowadzenie przede wszystkim zasad racjonalnego stosowania metod oraz środków, które mają służyć ochronie informacji niejawnych, a także adekwatności rozwiązań dedykowanych określonym klauzulą tajności[52].

Kluczowym celem zabezpieczenia w jednostkach organizacyjnych informacji niejawnych jest uniemożliwienie osobom nieuprawnionym dostępu do takich informacji. Wprowadzony obowiązek stosowania środków bezpieczeństwa fizycznego dotyczy głównie zabezpieczenia informacji niejawnych przed działaniem obcych służb specjalnych, zamachem

[50] M. Anzel, op. cit., s. 110.
[51] I. Stankowska, op. cit., s. 45.
[52] Ibidem, s. 177.

terrorystycznym lub sabotażem, a także kradzieżą lub zniszczeniem materiału, próbą wejścia osób nieuprawnionych do pomieszczeń, w których są przetwarzane informacje niejawne oraz nieuprawnionym dostępem do informacji o wyższej klauzuli tajności, niewynikającym z posiadanych uprawnień[53]. Należy podkreślić, że stosowanie odpowiednich środków bezpieczeństwa fizycznego jest uzależnione od poziomu zagrożeń związanego z nieuprawnionym dostępem do informacji niejawnych lub ich utratą[54]. Określając poziom zagrożeń, należy uwzględnić w szczególności występujące rodzaje zagrożeń, klauzulę tajności i liczbę informacji niejawnych, a w uzasadnionych przypadkach uwzględnia się również wskazania właściwej służby (w przypadku Służby Więziennej to ABW)[55]. Podstawowe kryteria i sposób określania poziomu zagrożeń zostały uregulowane w rozporządzeniu Rady Ministrów w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych[56], gdzie poziom zagrożeń należy ocenić w skali trójstopniowej (niski, średni, wysoki). Każdy z czynników, który ma wpływ, lub może mieć wpływ na ochronę informacji niejawnych, podlega indywidualnej ocenie pod kątem znaczenia dla zagrożenia ujawnieniem lub utratą informacji niejawnych w danej jednostce organizacyjnej. Określony poziom zagrożeń determinuje dobór odpowiednich do zagrożeń środków bezpieczeństwa fizycznego. Takie podejście pozwala zatem na racjonalne stosowanie odpowiednich środków, które będą służyły ochronie informacji niejawnych[57]. Dokumentację określającą poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą opracowuje pełnomocnik ochrony. Przedmiotowa dokumentacja podlega zatwierdzeniu przez kierownika jednostki organizacyjnej[58]. Obowiązek taki dotyczy kierowników tych jednostek organizacyjnych, w których przetwarza się informacje niejawne o klauzuli „poufne" lub wyższej[59].

W zakresie środków bezpieczeństwa fizycznego służących ochronie informacji niejawnych nie można pominąć faktu, że ustawa OIN upoważnia kierowników wskazanych organów do określenia w drodze zarządzenia,

[53] Art. 45 ust. 1 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).
[54] Ibidem, art. 45 ust. 2.
[55] Ibidem, art. 45 ust. 3.
[56] Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz.U. z 2012 r., poz. 683 z późn. zm.).
[57] M. Anzel, op. cit., s. 111.
[58] Art. 43 ust. 4 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).
[59] I. Stankowska, op. cit., s. 182.

doboru i stosowania środków bezpieczeństwa fizycznego[60]. Jednym z nich jest Minister Sprawiedliwości, który powyższy obszar funkcjonowania ochrony informacji niejawnych określił w zarządzeniu w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych[61]. Zatem Służba Więzienna jako formacja objęta obszarem działania Ministra Sprawiedliwości, w zależności od określonego poziomu zagrożeń, stosuje odpowiednią kombinację środków bezpieczeństwa fizycznego określoną w wyżej wymienionym zarządzeniu. Przez system środków bezpieczeństwa fizycznego należy rozumieć stosowanie rozwiązań organizacyjnych, w tym także stref ochronnych, wyposażenia i urządzeń służących ochronie informacji niejawnych, a także elektronicznych systemów pomocniczych, których zadaniem jest wspomaganie ochrony informacji niejawnych[62].

Na zakres wymogów, jakie należy spełnić, żeby odpowiednio zabezpieczyć informacje niejawne, ma wpływ klauzula tajności informacji niejawnych przetwarzanych w danej jednostce organizacyjnej. W celu odpowiedniego zabezpieczenia informacji niejawnych o klauzuli „poufne", „tajne" i „ściśle tajne" trzeba spełnić dodatkowe wymagania, które zostały określone w art. 46 ustawy OIN. Na szczególną uwagę zasługuję pojęcie strefy ochronnej. Zgodnie z opinią prezentowaną przez ABW, „strefa ochronna to obszar np.: wydzielona części budynku lub cały budynek, a także pomieszczenie wyposażone lub zabezpieczone w odpowiednie środki bezpieczeństwa fizycznego, w którym można przetwarzać informacje niejawne"[63]. Ustawa OIN wprowadza nakaz zorganizowania stref ochronnych, a także wprowadzenia systemu kontroli wejść i wyjść oraz określenie uprawnień do przebywania w tych strefach. Należy również pamiętać o stosowaniu odpowiedniego wyposażenia i urządzeń służących ochronie informacji niejawnych, którym przyznano certyfikaty[64]. Strefy ochronne powinny być zatem zorganizowane nie tylko w podmiotach, które dysponują informacjami niejawnymi o klauzuli „tajne" i „ściśle tajne", ale także w podmiotach przetwarzających informacje o klauzuli tajności

[60] Zob. art. 47 ust. 3 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).
[61] Zarządzenie Ministra Sprawiedliwości z dnia 23 stycznia 2014 r. w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz.Urz.MS z 2014 r., poz. 32).
[62] Ibidem, §3 ust. 1.
[63] *Co to jest strefa ochronna?*, https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/bezpieczenstwo-fizyczn/150,Kancelarie-tajne-Bezpieczenstwo-fizyczne.html#15 [dostęp:20.09.2023].
[64] Art. 46 pkt 4 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).

„poufne”[65]. Kryteria tworzenia stref ochronnych (strefa ochronna I,II,III) zostały określone w rozporządzeniu Rady Ministrów w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych. Akt wykonawczy określa również możliwość stworzenia dodatkowej strefy-specjalnej strefy ochronnej[66]. Wymogi wynikające z art. 46 ustawy OIN powinny być opisane w planie ochrony informacji niejawnych, który zatwierdza kierownik jednostki organizacyjnej[67]. Opracowanie i aktualizacja planu ochrony informacji niejawnych należy do zadań pełnomocnika ochrony[68].

Kancelarie tajne

Ustawa OIN, nakładając na kierownika jednostki organizacyjnej odpowiedzialność za ochronę informacji niejawnych, które są w niej przetwarzane, obliguje go do zorganizowania systemu ochrony informacji niejawnych w taki sposób, aby zapewnić im najwyższe bezpieczeństwo. Dotyczy to w szczególności tych informacji, których nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej. W tym zakresie kierownik jednostki organizacyjnej ma obowiązek utworzenia kancelarii tajnej[69]. Kancelarię tajną tworzy się w sytuacji, gdy przetwarzane są w niej informacje niejawne o klauzuli „tajne” i „ściśle tajne”[70]. Tym samym z obowiązku utworzenia kancelarii tajnej zwolnieni są kierownicy jednostek organizacyjnych, w których przetwarza się jedynie informacje niejawne o klauzuli „poufne” lub „zastrzeżone”.

Dodatkowym obowiązkiem kierownika jednostki organizacyjnej jest zatrudnienie kierownika kancelarii tajnej[71] oraz poinformowanie ABW o utworzeniu kancelarii tajnej, z podaniem klauzuli informacji niejawnych, które są w niej przetwarzane. Również w przypadku likwidacji kancelarii tajnej kierownik jednostki organizacyjnej musi poinformować

[65] J. Frąckiewicz, *Zmiany w zakresie organizacji kancelarii tajnej i stosowania środków bezpieczeństwa fizycznego*, [w:] Z. Nawrocki(red.) *Ochrona informacji niejawnych. Poradnik praktyczny dla osób i instytucji przetwarzających informacje niejawne*, Warszawa 2011, s. 167.

[66] Zob. §5 ust. 1 rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. z 2012 r., poz. 683 z późn. zm.).

[67] Ibidem, §9 ust. 1.

[68] Art. 15 ust. 1 pkt 5 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).

[69] I. Stankowska, op. cit., s. 178.

[70] Art. 42 ust. 1 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).

[71] Ibidem.

ABW o tym fakcie[72]. Realizacja powyższych obowiązków informacyjnych jest bardzo istotna, gdyż umożliwia ABW sprawowanie swoich obowiązków w zakresie nadzoru nad ochroną informacji najistotniejszych dla bezpieczeństwa państwa. Tym samym pozwoli to na uniknięcie sytuacji przekazywania dokumentów niejawnych do jednostek organizacyjnych, które są nieprzygotowane na ich przyjmowanie[73].

W myśl art. 42 ust. 4 ustawy OIN kancelaria tajna stanowi wyodrębnioną komórkę organizacyjną w zakresie ochrony informacji niejawnych, która w zakresie swojego działania podlega pełnomocnikowi ochrony. Obsługą kancelarii tajnej zajmują się pracownicy pionu ochrony[74]. Kancelaria tajna, jako że stanowi komórkę organizacyjną, która jest odpowiedzialna za właściwe rejestrowanie, przechowywanie, a także obieg i wydawanie materiałów uprawnionym osobom[75], musi więc spełniać odpowiednie wymogi lokalizacyjne i znaleźć się w strefie ochronnej. Ponadto praca w kancelarii tajnej musi być tak zorganizowana, aby umożliwić ustalenie w każdych okolicznościach, gdzie znajduje się w jednostce organizacyjnej dany materiał o klauzuli „tajne" lub „ściśle tajne" oraz kto się z tym materiałem zapoznał[76]. Takie same wymogi dotyczące organizacji pracy, ustawodawca wprowadził względem organizacji pracy innych niż kancelaria tajna komórek, w których rejestrowane są materiały o klauzuli „poufne[77]. Inne niż kancelaria tajna komórki, w których przetwarzane są informacje niejawne o klauzuli „poufne", nazywane są w różnych podmiotach np. „kancelariami niejawnymi", „kancelariami materiałów niejawnych", „kancelariami materiałów niejawnych dla klauzuli poufne".

Ustawa OIN wprowadziła rozwiązane polegające na możliwości zorganizowania kancelarii tajnej obsługującej dwie lub więcej jednostek organizacyjnych[78]. Takie rozwiązanie powinno być jednak poprzedzone głęboką analizą zasadności połączenia kancelarii tajnych uwzględniającą m.in. liczbę informacji niejawnych o najwyższych klauzulach i ich obieg,

[72] Ibidem, art. 42 ust. 6.
[73] I. Stankowska, op. cit., s. 180.
[74] Pion ochrony to wyodrębniona i podlegająca pełnomocnikowi ochrony komórka organizacyjna do spraw ochrony informacji niejawnych. W pionie ochrony zatrudnieni są pracownicy pionu ochrony, którzy podlegają pełnomocnikowi ochrony. Pracownikiem pionu ochrony w jednostce organizacyjnej może być osoba, która posiada: obywatelstwo polski; odpowiednie poświadczenie bezpieczeństwa lub upoważnienie, o którym mowa w art. 21 ust. 4 pkt 1 ustawy OIN; zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych.
[75] Art. 42 ust. 4 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).
[76] Ibidem, art. 43 ust. 1.
[77] Ibidem, art. 43 ust. 2.
[78] Ibidem, art. 42 ust. 3.

możliwości lokalizacyjne, kadrowe oraz finansowe jednostek, a także odległość między jednostkami. Możliwość łączenia kancelarii tajnych służy przede wszystkim tym jednostkom, które posiadają znikomą liczbę materiałów niejawnych. Procedura utworzenia wspólnej kancelarii tajnej musi wynikać z odpowiedniego porozumienia podpisanego między kierownikami jednostek organizacyjnych, które powinno regulować podległość, obsadę i zasady finansowania takiej kancelarii. W sytuacji gdy kancelaria tajna prowadzi obsługę więcej niż jednej jednostki organizacyjnej, wówczas informacje niejawne tych jednostek muszą być fizycznie od siebie oddzielone[79] np. poprzez przechowywane w odrębnych szafach przeznaczonych do przechowywania informacji niejawnych i spełniających odpowiednie wymagania techniczne. Zgodę na zorganizowanie kancelarii tajnej, która będzie obsługiwała dwie lub więcej jednostek organizacyjnych musi wyrazić ABW[80], która jest właściwa względem Służby Więziennej.

Przywołany wcześniej art. 47 ust. 3 ustawy OIN ma również kluczowe znaczenie dla wymagań, jakie trzeba spełnić w zakresie funkcjonowania kancelarii tajnych mieszczących się m.in. w jednostkach organizacyjnych Służby Więziennej. Minister Sprawiedliwości, podobnie jak to miało miejsce w przypadku środków bezpieczeństwa fizycznego, miał obowiązek określenia szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz komórek organizacyjnych innych niż kancelaria tajna, a także sposobu i trybu przetwarzania informacji niejawnych[81]. Podstawowe zasady funkcjonowania kancelarii tajnych są oczywiście analogiczne do wymogów określonych w ustawie OIN. Bardzo ważne w tym zakresie, jest więc prawidłowe wyodrębnienie organizacyjne i lokalizacyjne kancelarii tajnej, które zapewni bezpieczne przetwarzanie informacji niejawnych, a także sprawną realizację zadań przypisanych jej do wykonania82. Ponadto, tworząc kancelarię tajną, należy zadbać o spełnienie wymagań w zakresie rejestrowania, przechowywania, obiegu i wydawania materiałów. Prawidłowa praktyka w powyższym zakresie

[79] M. Anzel, op. cit., s. 43.

[80] Art. 42 ust. 3 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).

[81] Zarządzenie Ministra Sprawiedliwości z dnia 6 września 2023 r. *w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz niektórych komórek organizacyjnych innych niż kancelaria tajna, a także sposobu i trybu przetwarzania informacji niejawnych (*Dz. Urz. MS z 2023 r., poz. 173) poprzedzone było Zarządzeniem Ministra Sprawiedliwości z dnia 29 grudnia 2011 r. *w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz niektórych komórek organizacyjnych innych niż kancelaria tajna, a także sposobu i trybu przetwarzania informacji niejawnych (*Dz. Urz. MS z 2012 r., poz. 13).

[82] Ibidem, §5 ust. 1 pkt 1.

zapewni możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał o klauzuli „tajne" lub „ściśle tajne", który pozostaje w dyspozycji jednostki organizacyjnej oraz zapewni rozliczalność w zakresie tego, kto z tym materiałem się zapoznał[83]. Zgodnie z rozstrzygnięciami powyższego zarządzenia należy również zapewnić osobne pomieszczenia przeznaczone wyłącznie na potrzeby kancelarii tajnej[84], znajdujące się w strefie ochronnej I lub II[85], gdzie nadzór nad przebywającymi osobami sprawują pracownicy kancelarii[86]. Ważnym elementem organizacyjnym jest również możliwość wydzielenia w pomieszczeniach kancelarii tajnej czytelni, co pozwoli osobom uprawnionym na zapoznawanie się z materiałami zawierającymi informacje niejawne, przy zapewnieniu jednocześnie możliwości sprawowania stałego nadzoru pracowników kancelarii nad tymi materiałami[87]. Należy również pamiętać, że w pomieszczeniach przeznaczonych na pomieszczenia kancelarii tajnej nie instaluje się kamer systemu monitoringu wizyjnego[88].

Fakt, że kancelarię tajną zgodnie z art. 42 ust. 1 ustawy OIN tworzy się w sytuacji, gdy przetwarza się informacje niejawne o klauzuli „tajne" i „ściśle tajne", nie wyklucza możliwości przetwarzania w niej również informacji niejawnych o niższych klauzulach tajności. Ustawa OIN dopuszcza przetwarzanie w kancelarii tajnej informacji niejawnych o klauzuli „poufne" i „zastrzeżone", a wyrażenie zgody w tym zakresie należy do kompetencji kierownika jednostki organizacyjnej[89]. Przedmiotowa zgoda musi być wyrażona w formie pisemnej[90].

Kierownicy kancelarii tajnych, w większości jednostek organizacyjnych Służby Więziennej, realizują zazwyczaj przydzielone obowiązki na zasadzie dodatkowej funkcji. Pełniąc na co dzień służbę w różnych komórkach organizacyjnych, wykonują obowiązki kierownika kancelarii tajnej w formie zadań dodatkowych. Uzasadnione jest więc wyznaczenie osoby, do której obowiązków należy sprawowanie zastępstwa. Stanowi

[83] Ibidem, §5 ust. 1 pkt 2.
[84] Ibidem, §11 ust. 1.
[85] Ibidem, §11 ust. 2.
[86] Ibidem, §11 ust. 3.
[87] Ibidem, §11 ust. 4.
[88] Ibidem, §11 ust. 5.
[89] Art. 42 ust. 5 ustawy z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).
[90] §5 ust. 2 zarządzenia Ministra Sprawiedliwości z dnia 6 września 2023 r. *w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz niektórych komórek organizacyjnych innych niż kancelaria tajna, a także sposobu i trybu przetwarzania informacji niejawnych (*Dz. Urz. MS z 2023 r., poz. 173).

to zabezpieczenie w sytuacji absencji kierownika kancelarii spowodowanej chorobą, urlopem czy innymi okolicznościami. Wyznaczony zastępca przejmuje wówczas obowiązki, zapewniając tym samym ciągłość funkcjonowania kancelarii. O wyznaczeniu w jednostce organizacyjnej zastępcy kierownika kancelarii tajnej powinno również decydować zjawisko naturalnej fluktuacji kadrowej. Nowy kierownik kancelarii tajnej może potrzebować trochę czasu na poznanie specyfiki jednostki, na dostosowanie się do nowej roli, natomiast zastępca jest już zaznajomiony z pełnieniem przedmiotowej funkcji w danej jednostce organizacyjnej. Kolejnym argumentem za wyznaczeniem zastępcy kierownika kancelarii tajnej jest ustawowa możliwość utworzenia kancelarii tajnej obsługującej dwie lub więcej jednostek organizacyjnych. W takiej sytuacji ilość obowiązków kierownika tzw. wspólnej kancelarii tajnej znacząco wzrasta, co czyni obecność zastępcy zasadną. Biorąc pod uwagę przytoczone argumenty, wyznaczenie zastępcy kierownika kancelarii tajnej wydaje się uzasadnione.

Mimo iż zadania pełnomocnika ochrony zostały określone w art. 15 ust. 1 ustawy OIN, to niektóre jego obowiązki można znaleźć w poszczególnych rozdziałach regulujących problematykę ochrony informacji niejawnych. Dodatkowe obowiązki wynikają również z przepisów rozdziału 7 ustawy OIN. Zgodnie z przepisami tego rozdziału, pełnomocnik ochrony ma obowiązek opracowania, dokumentacji regulującej kwestie sposobu i trybu przetwarzania informacji niejawnych o klauzuli „poufne”[91] oraz „zastrzeżone”[92]. Dodatkowo względem informacji niejawnych o klauzuli „zastrzeżone” pełnomocnik ochrony musi określić zakres i warunki stosowania środków bezpieczeństwa fizycznego[93]. Dokumentacja zawierająca odpowiednie procedury podlega zatwierdzeniu przez kierownika jednostki organizacyjnej[94].

Bezpieczeństwo teleinformatyczne

Kolejnym z obszarów bezpieczeństwa informacji niejawnych jest ochrona systemów teleinformatycznych służących do ich przetwarzania.

[91] Art. 43 ust. 3 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).
[92] Ibidem, art. 43 ust. 5.
[93] Ibidem.
[94] Ibidem, art. 43 ust. 3 i 5.

Przedmiotową problematykę reguluje rozdział 8 ustawy OIN zatytułowany Bezpieczeństwo teleinformatyczne.

Ustawa OIN unowocześniła znacząco regulacje dotyczące bezpieczeństwa teleinformatycznego. Polskie regulacje zostały tym samym zbliżone do standardów obowiązujących w państwach NATO czy Unii Europejskiej[95].

Ustawodawca już w art. 2 ustawy OIN, w słowniku ustawowym, wskazuje szereg pojęć dotyczących bezpieczeństwa teleinformatycznego takich jak m.in. system teleinformatyczny, dokument szczególnych wymagań bezpieczeństwa, dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego, dokumentacja bezpieczeństwa systemu teleinformatycznego, akredytacja bezpieczeństwa teleinformatycznego, audyt bezpieczeństwa systemu teleinformatycznego, szacowanie ryzyka, zarządzanie ryzykiem[96]. Zrozumienie elementarnych pojęć związanych z bezpieczeństwem teleinformatycznym ma kluczowy wpływ na utworzenie bezpiecznego systemu teleinformatycznego.

Osobami, które odpowiadają za kreowanie polityki bezpieczeństwa systemu teleinformatycznego, w którym będą przetwarzane informacje niejawne oraz za planowanie, wdrażanie, a także eksploatację tego systemu są kierownik jednostki organizacyjnej, pełnomocnik ochrony, inspektor bezpieczeństwa teleinformatycznego, administrator systemu[97].

W myśl art. 48 ust. 1 ustawy OIN, „Systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego". Ustawodawca wskazuje okres, w którym system teleinformatyczny może być dopuszczony do przetwarzania informacji niejawnych. Akredytacja bezpieczeństwa teleinformatycznego jest udzielna terminowo, na czas określony, jednak nie dłuży niż 5 lat[98]. Proces związany z akredytacją systemu teleinformatycznego będzie różny w zależności od klauzuli tajności informacji niejawnych, które będą w nim przetwarzane[99]. Aktualnie obowiązująca ustawa OIN, wprowadza w tym zakresie podział kompetencji, który kształtuje się pomiędzy właściwym organem – jakim w przypadku Służby Więziennej

[95] I. Stankowska, op. cit., s. 192.
[96] Zob. art. 2 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).
[97] M. Anzel, op. cit., s. 124.
[98] Art. 48 ust. 2 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).
[99] M. Anzel, op. cit., s. 84.

jest ABW, a kierownikiem jednostki organizacyjnej, w której tworzy się system teleinformatyczny.

Przede wszystkim wymagające są warunki uzyskiwania akredytacji dla systemów dedykowanych do przetwarzania informacji niejawnych oznaczonych klauzulą „poufne", „tajne" i „ściśle tajne". Dla informacji niejawnych oznaczonych klauzulą „poufne" lub wyższą, zgodnie z art. 48 ust. 5 ustawy OIN, akredytacja udzielana jest poprzez wydanie świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego. Wydanie odpowiedniego świadectwa odbywa się na podstawie zatwierdzenia przez ABW dokumentacji bezpieczeństwa systemu teleinformatycznego oraz przeprowadzenia audytu bezpieczeństwa systemu teleinformatycznego celem sprawdzenia działania systemu danej jednostki z przygotowaną dokumentacją[100]. Zgodnie z przepisami ustawy OIN, ABW może jednak odstąpić od przeprowadzenia audytu bezpieczeństwa systemu teleinformatycznego, jeżeli system jest przeznaczony do przetwarzania *informacji niejawnych* o klauzuli „poufne"[101]. Tym samym, ustawodawca wprowadził dla właściwego organu fakultatywność decyzji w powyższym zakresie.

Inaczej natomiast wygląda procedura uzyskiwania akredytacji dla systemów teleinformatycznych, w których mają być przetwarzane informacje niejawne o klauzuli „zastrzeżone". Znaczącą rolę w tym zakresie odgrywa kierownik jednostki organizacyjnej, w której przetwarzane będą informacje niejawne w danym systemie teleinformatycznym. W myśl art. 48 ust. 9 ustawy OIN akredytacji bezpieczeństwa teleinformatycznego udziela kierownik jednostki organizacyjnej poprzez zatwierdzenie dokumentacji bezpieczeństwa dla tworzonego systemu teleinformatycznego. Kierownik jednostki organizacyjnej ma jednak obowiązek w ciągu 30 dni od udzielenia akredytacji bezpieczeństwa teleinformatycznego przekazać do ABW całą dokumentację bezpieczeństwa akredytowanego systemu[102]. Następnie, ABW ma prawo w terminie 30 dni od otrzymania dokumentacji przedstawić kierownikowi jednostki organizacyjnej zalecenia dotyczące konieczności wprowadzenia odpowiednich czynności, które są związane z bezpieczeństwem informacji niejawnych. Z kolei kierownik jednostki organizacyjnej w terminie 30 dni od otrzymania zaleceń ma obowiązek w zakresie poinformowania ABW o ich realizacji. Mimo że ABW nie udziela akredytacji dla systemów teleinformatycznych,

[100] Art. 48 ust. 6 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).
[101] Ibidem, art. 48 ust. 8.
[102] Ibidem, art. 48 ust. 11.

w których są przetwarzane informacje niejawne o klauzuli „zastrzeżone", ma jednak możliwość, w szczególnie uzasadnionych przypadkach nakazać wstrzymanie przetwarzania informacji niejawnych w danym systemie teleinformatycznym, który posiada akredytację bezpieczeństwa teleinformatycznego[103]. Celem tego uprawnienia jest zapobieżenie sytuacji, w której kierownik jednostki organizacyjnej udzieli akredytacji systemowi niespełniającemu podstawowych zasad bezpieczeństwa teleinformatycznego[104].

Na dokumentację bezpieczeństwa teleinformatycznego zgodnie z art. 2 pkt 9 ustawy OIN, składają się dokument szczególnych wymagań bezpieczeństwa oraz dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego. Opracowanie wymaganych dokumentów musi odbywać się zgodnie z zasadami określonymi w ustawie OIN. Elementarne wymagania dotyczące powyższej dokumentacji bezpieczeństwa teleinformatycznego zostały uregulowane w art. 49 ustawy OIN. Do opracowania powyższej dokumentacji, kierownik jednostki organizacyjnej powinien powołać zespół osób. Wynika to z faktu, iż zakres tematyczny dokumentacji bezpieczeństwa teleinformatycznego wymaga specjalistycznej wiedzy z zakresu informatyki, ochrony informacji niejawnych, łączności, ochrony fizycznej obiektu, w którym ten system będzie funkcjonował itp. Zasadne wydaje się zatem powołanie w jednostce organizacyjnej zespołu osób, fachowców reprezentujących wyżej wymienione dziedziny[105]. Przedmiotowa dokumentacja powinna być opracowana w sposób kompletny i wyczerpujący, aby opisywała cały system teleinformatyczny, w którym będą przetwarzane informacje niejawne, czyli budowę, zasady działania oraz eksploatację. Kluczowym elementem dokumentu szczególnych wymagań bezpieczeństwa jest szacowanie ryzyka dla bezpieczeństwa informacji niejawnych, a także zarządzanie ryzykiem. Dlatego też tak istotne jest przeprowadzenie szacowania ryzykiem przed przystąpieniem do sporządzenia dokumentacji bezpieczeństwa[106]. Ustawa OIN dopuszcza, aby przebieg i wyniki procesu szacowania ryzyka mogły zostać przedstawione w odrębnym dokumencie niż dokument szczególnych wymagań bezpieczeństwa[107]. Z kolei dokument procedur bezpiecznej eksploatacji

[103] Ibidem, art. 48 ust. 12.
[104] I. Stankowska, op. cit., s. 196-197.
[105] M. Anzel, op. cit., s. 86.
[106] I. Stankowska, op. cit., s. 200.
[107] Art. 49 ust. 1 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).

systemu informatycznego zawiera w swojej treści procedury, które trzeba spełnić celem zapewnienia bezpieczeństwa teleinformatycznego danego systemu. Podstawę do opracowania procedur bezpiecznej eksploatacji stanowi dokument szczególnych wymagań bezpieczeństwa. Ponadto procedury bezpiecznej eksploatacji określają także obowiązki użytkowników systemu teleinformatycznego. Uzasadnione jest więc, aby wszyscy użytkownicy systemu zapoznali się z procedurami i potwierdzili ten fakt własnoręcznym podpisem. Procedury bezpiecznej eksploatacji powinny być dostępne dla użytkowników systemu do wglądu. Dobrą praktyką jest umiejscowienie ich w pomieszczeniu eksploatacji systemu teleinformatycznego np. w postaci wyciągów dla użytkowników[108].

Przygotowując się do opracowywania dokumentacji bezpieczeństwa teleinformatycznego, należy zapoznać się z całym aktem wykonawczym, a w szczególności z wymaganiami określonymi w rozdziale 4 rozporządzenia Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego[109]. Dodatkową pomocą przy tworzeniu w jednostce organizacyjnej Służby Więziennej systemu teleinformatycznego, w którym będą przetwarzane informacje niejawne, są odpowiednie zalecenia, które zgodnie z ustawą OIN w zakresie bezpieczeństwa teleinformatycznego może wydawać ABW[110]. Wykaz zaleceń dotyczących bezpieczeństwa teleinformatycznego znajduje się na stronach Biuletynu Informacji Publicznej ABW, gdzie w sprawach ich udostępnienia, może zwrócić się wyłącznie osoba, która była przeszkolona przez ABW na specjalistycznym szkoleniu z zakresu bezpieczeństwa teleinformatycznego przeprowadzonym dla administratorów oraz inspektorów bezpieczeństwa teleinformatycznego[111].

Dokumentacja bezpieczeństwa teleinformatycznego stanowi dokument, którego opracowanie powinno odbywać przy uwzględnieniu indywidualnych potrzeb jednostki organizacyjnej oraz jej specyfiki. Istotny wpływ w tym zakresie ma rodzaj danej jednostki organizacyjnej i zadania statutowe, jakie zostały jej przypisane. Tym samym faktyczna wiedza na temat potrzeb jednostki w zakresie konieczności przetwarzania

[108] M. Anzel, op. cit., s. 93.
[109] Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011 r., nr 159, poz. 948).
[110] Art. 52 ust. 3 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).
[111] *Wykaz obowiązujących zaleceń*, https://bip.abw.gov.pl/bip/informacje-niejawne-1/bezpieczenstwo-teleinf/zalecenia-w-zakresie-bezpiecze/507,Zalecenia-w-zakresie-bezpieczenstwa-teleinformatycznego.html [dostęp: 20.09.2023].

informacji niejawnych w systemach teleinformatycznych ma istotny wpływ na wybór odpowiedniej procedury postępowania celem uzyskania akredytacji bezpieczeństwa teleinformatycznego. Inne potrzeby w zakresie przetwarzania informacji niejawnych w systemach teleinformatycznych będą miały np. Okręgowe Inspektoraty Służby Więziennej, a inne zakłady karne i areszty śledcze, a jeszcze inne ośrodki szkolenia. Biorąc pod uwagę specyfikę i zadania przypisane jednostkom organizacyjnym Służby Więziennej, zasadnym wydaje się jednak żeby każda jednostka organizacyjna miała przynajmniej możliwość przetwarzania w systemie teleinformatycznym informacji niejawnych o klauzuli „zastrzeżone".

Kontrola ochrony informacji niejawnych

Jednym z podstawowych zadań pełnomocnika ochrony określonym w art. 15 ust. 1 pkt 4 ustawy OIN jest kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, w szczególności okresowa kontrola ewidencji, materiałów i obiegu dokumentów. Ustawa OIN precyzuje, że kontrole okresowe powinny być przeprowadzane co najmniej raz na trzy lata. Kontrola ochrony informacji niejawnych jest pojęciem bardzo szerokim, zatem głębokiej analizę powinno poddać się stan ochrony informacji niejawnych w jednostce organizacyjnej. Pełnomocnik ochrony powyższe zadanie może realizować przy pomocy pionu ochrony przy założeniu, że został powołany w jednostce organizacyjnej[112]. Dobrą praktyką jest przeprowadzenie kontroli przez komisję, która może być powołana przez kierownika jednostki organizacyjnej w formie zarządzenia lub innego aktu prawa wewnętrznego (np. decyzja) albo rozkazu. W celu zachowania rozliczalności realizowanych obowiązków kontrole powinny być odpowiednio dokumentowane np. w formie protokołów.

Kontrolę okresową, o której mowa w art. 15 ust. 1 pkt 4 ustawy OIN, pełnomocnik ochrony przeprowadza w kancelarii tajnej samodzielnie albo za pośrednictwem komisji, która powinna się składać z osób uprawnionych z pionu ochrony. W skład komisji nie powinni wchodzić pracownicy kancelarii tajnej. Komisja powoływana jest przez kierownika jednostki organizacyjnej, który wskazuje jej przewodniczącego, a osobą,

[112] Art. 15 ust. 2 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).

która wnioskuje o jej powołanie, jest pełnomocnik ochrony. Dopuszcza się, aby w szczególnie uzasadnionych przypadkach, w komisji brały udział osoby uprawnione spoza pionu ochrony[113]. Istotnym elementem, na który należy zwrócić również uwagę przy powoływaniu komisji, jest posiadanie przez jej członków odpowiednich uprawnień umożliwiających dostęp do kontrolowanych informacji niejawnych (odpowiednie poświadczenie bezpieczeństwa osobowego adekwatne do kontrolowanych materiałów). Do składu komisji nie należy powoływać osób, które są odpowiedzialne za ewidencje materiałów i obieg dokumentów niejawnych[114].

Ponad to, zarówno pełnomocnik ochrony i inni pracownicy pionu ochrony, jak np. inspektor bezpieczeństwa teleinformatycznego, przeprowadzają kontrole wynikające z dokumentacji bezpieczeństwa systemu teleinformatycznego, w którym przetwarzane są informacje niejawne. Kontrole w przedmiotowym zakresie powinny być odpowiednio udokumentowane (np. protokół kontroli; wpisy w dziennik inspektora bezpieczeństwa teleinformatycznego, dziennik administratora systemu).

Do przeprowadzenia kontroli w Służbie Więziennej w zakresie stanu zabezpieczenia *informacji niejawnych* uprawnieni są również funkcjonariusze ABW. Ustawodawca wskazuje, że upoważnienie do kontroli musi mieć formę pisemną, nadając im jednocześnie szeroki zakres uprawnień[115]. Akt wykonawczy przewiduje dwa rodzaje kontroli. Pierwszą z nich jest kontrola planowa przeprowadzana na podstawie rocznego planu kontroli, który zatwierdzany jest przez Szefa ABW, po uzyskaniu opinii Kolegium do Spraw Służb Specjalnych[116]. Drugim rodzajem kontroli jest kontrola doraźna, która nie wynika z rocznego planu kontroli, i zarządzenie jej należy do kompetencji Szefa ABW. Kontrola doraźna może być zarządzona, jeżeli Szef ABW uzyska informacje, które wskazują na występowanie istotnych zagrożeń dla systemu zabezpieczenia informacji niejawnych lub nieprawidłowości w zakresie postępowań sprawdzających[117].

[113] §13 ust.1 i 2 zarządzenia Ministra Sprawiedliwości z dnia 6 września 2023 r. *w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz niektórych komórek organizacyjnych innych niż kancelaria tajna, a także sposobu i trybu przetwarzania informacji niejawnych (*Dz. Urz. MS z 2023 r., poz. 173).
[114] M. Anzel, op. cit., s. 107.
[115] Zob. art. 12 ust. 1 ustawy OIN (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).
[116] §2 ust. 1 rozporządzenia Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych (Dz. U. z 2011 r. nr 93 poz. 541).
[117] Ibidem, §2 ust. 2.

Kontrola doraźna może również wynikać z realizacji przez jednostkę organizacyjną obowiązku informacyjnego względem ABW, o którym mowa w art. 17 ust. 2 ustawy OIN. W razie stwierdzenia naruszenia przepisów o ochronie informacji niejawnych o klauzuli „poufne" lub wyższej pełnomocnik ochrony ma ustawowy obowiązek zawiadomienia o tym niezwłocznie właściwego organu, a w przypadku Służby Więziennej tym organem jest ABW. W oparciu o przekazane zawiadomienie, ABW może podjąć działania polegające na przeprowadzeniu kontroli doraźnej w zakresie przestrzegania przepisów o ochronie informacji niejawnych w tej jednostce organizacyjnej[118].

Podstawą przeprowadzenia kontroli w danej jednostce organizacyjnej jest imienne upoważnienie kontrolera określające jednostkę kontrolowaną, wystawione przez Szefa ABW[119]. Ustalenia dokonane w toku kontroli, są opisywane przez kontrolera w protokole kontroli, który sporządzany jest w dwóch egzemplarzach. Jeden egzemplarz protokołu przekazuje się kierownikowi jednostki kontrolowanej, natomiast drugi zostaje dołączony do akt kontroli[120]. Przeprowadzenie kontroli stanu zabezpieczenia informacji niejawnych, zostało szczegółowo uregulowane w rozporządzeniu Prezesa Rady Ministrów w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych[121].

Działania kontrolne prowadzone przez pełnomocnika ochrony w jednostce organizacyjnej Służby Więziennej oraz przez funkcjonariuszy ABW mają pozytywny wpływ na sposób wykonywania obowiązków w zakresie ochrony informacji niejawnych. W szczególności istotną rolę odgrywają pełnomocnicy ochrony, którzy na co dzień pełnią służbę w jednostce organizacyjnej, bo *de facto* od nich zależy zapewnienie odpowiedniego poziomu ochrony informacji niejawnych, adekwatnego do przetwarzanych informacji.

[118] S. Zalewski, op. cit., s. 68.
[119] §6 ust. 1 rozporządzenia Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych (Dz. U. z 2011 r. nr 93 poz. 541).
[120] Ibidem, §16 ust. 3.
[121] Rozporządzenie Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych (Dz. U. z 2011 r. nr 93 poz. 541).

Podsumowanie

Analiza przepisów ustawy OIN oraz jej aktów wykonawczych ukazuje wielość zadań i obowiązków, jakie spoczywają na kierowniku jednostki organizacyjnej oraz pełnomocniku ochrony w ramach systemu ochrony informacji niejawnych. Szczególnie istotne jest wytypowanie odpowiedniej osoby do pełnienia funkcji pełnomocnika ochrony, która po uzyskaniu poświadczenia bezpieczeństwa i odbyciu przeszkolenia w zakresie ochrony informacji niejawnych będzie filarem, w kształtowaniu systemu ochrony informacji niejawnych danej jednostki organizacyjnej, zapewniając tym samym odpowiednie przestrzeganie wymaganych przepisów. Zadania nałożone na kierownika jednostki organizacyjnej, jako organu odpowiedzialnego za ochronę informacji niejawnych, w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony, zależą więc od skuteczności działań pełnomocnika ochrony. To on jako ekspert w zakresie ochrony informacji niejawnych ma głęboką wiedzę na temat przepisów, standardów i najlepszych praktyk związanych z tym kluczowym obszarem, reagując jednocześnie na wszelkie incydenty i pomagając w ich rozwiązaniu, a także raportowaniu kierownikowi jednostki i odpowiednim instytucjom. W zakresie incydentów jego skuteczność jako eksperta jest o tyle istotna, że może pomóc minimalizować powstałe naruszenia. Ważna jest zatem odpowiednia współpraca i komunikacja na linii kierownik jednostki, a pełnomocnik ochrony celem zapewnienia właściwego poziomu bezpieczeństwa informacji niejawnych i uchronienia przed ewentualną odpowiedzialnością karną, dyscyplinarną i służbową za naruszenie przepisów ustawowych.

Biorąc również pod uwagę argumenty przytoczone przy zasadności wyznaczenia zastępcy kierownika kancelarii tajnej (wielość zadań, absencje, fluktuacja kadrowa) zasadnym w opinii autora, jest również wyznaczanie w jednostkach organizacyjnych Służby Więziennej osób do pełnienia funkcji zastępcy pełnomocnika ochrony.

Uwzględniając całą problematykę związaną z bezpieczeństwem informacji niejawnych, trzeba także pamiętać, iż stworzenie idealnego systemu ich ochrony nie będzie całkowicie możliwe, gdyż najczęstsze błędy wynikają z zawodności czynnika ludzkiego. Problematyka poruszana w niniejszym artykule stanowi zatem dla autora podstawę do szczegółowych analiz poszczególnych elementów systemu ochrony informacji niejawnych.

Bibliografia

Stankowska I., *Komentarz. Ustawa o ochronie informacji niejawnych*, Warszawa 2014.

Nosarzewski Ł., Opaliński B., Szustakiewicz P., *Ustawa o ochronie informacji niejawnych. Komentarz.*, Warszawa 2023.

Anzel M., *Poradnik specjalisty ochrony informacji niejawnych*, Poznań 2015.

Zalewski S., *Informacje niejawne we współczesnym świecie*, Warszawa 2017.

Smykla A., *Zmiany w przepisach dotyczących ogólnych zasad systemu oraz klasyfikowania informacji niejawnych,* [w:] Nawrocki Z. (red.) *Ochrona informacji niejawnych. Poradnik praktyczny dla osób i instytucji przetwarzających informacje niejawne*, Warszawa 2011.

Frąckiewicz J., *Zmiany w zakresie organizacji kancelarii tajnej i stosowania środków bezpieczeństwa fizycznego*, [w:] Nawrocki Z. (red.) *Ochrona informacji niejawnych. Poradnik praktyczny dla osób i instytucji przetwarzających informacje niejawne*, Warszawa 2011.

Akty prawne:

Ustawa z dnia 9 kwietnia 2010r. o Służbie Więziennej (t.j. Dz. U. z 2023 r., poz. 1683 z późn. zm.).

Ustawa z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych (t.j. Dz. U. z 2023 r., poz. 756 z późn. zm.).

Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa (t.j. Dz. U. z 2015 r., poz. 220).

Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011 r. nr 159 poz. 948).

Rozporządzenie Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych (Dz. U. z 2011 r. nr 93 poz. 541).

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

Rozporządzenie Prezesa Rady Ministrów z dnia 9 lipca 2020 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego (Dz. U. z 2020r., poz. 1256).

Zarządzenie Ministra Sprawiedliwości z dnia 23 stycznia 2014 r. w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. Urz. MS z 2014 r., poz. 32).

Zarządzenie Ministra Sprawiedliwości z dnia 6 września 2023 r. *w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz niektórych komórek organizacyjnych innych niż kancelaria tajna, a także sposobu i trybu przetwarzania informacji niejawnych (*Dz. Urz. MS z 2023 r., poz. 173).

Zarządzenie nr 61/18 Dyrektora Generalnego Służby Więziennej z dnia 20 grudnia 2018 r. w sprawie programów szkolenia wstępnego, zawodowego i specjalistycznego w Służbie Więziennej dla funkcjonariuszy i pracowników (z późn. zm.).

Zarządzenie nr 58/23 Dyrektora Generalnego Służby Więziennej z dnia 31 sierpnia 2023 r. w sprawie przeprowadzania postępowań sprawdzających wobec funkcjonariuszy i pracowników oraz osób ubiegających się o przyjęcie do służby lub pracy w Służbie Więziennej.

Źródła internetowe:

Wobec jakich podmiotów właściwą rzeczowo jest Agencja Bezpieczeństwa Wewnętrznego?, https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/organizacja-ochrony-in/145,ORGANIZACJA-OCHRONY-INFORMACJI-NIEJAWNYCH.html [dostęp: 18.09.2023].

Jakie są warunki dostępu do informacji niejawnych NATO, UE i ESA?, https://bip.abw.gov.pl/bip/informacje-niejawne-1/ochrona-informacji-nie/153,OCHRONA-INFORMACJI-NIEJAWNYCH-MIEDZYNARODOWYCH-W-SFERZE-CYWILNEJ-I-WOJSKOWEJ.html [dostęp:18.09.2023].

wzór upoważnienia do dostępu do informacji „zastrzeżone”, https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/materialy-do-pobrania/152,MATERIALY-DO-POBRANIA.html [dostęp: 18.09.2023].

Jaki dokument potwierdza przeprowadzenie szkolenia?, https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/szkolenia/147,SZKOLENIA.html [dostęp: 18.09.2023].

oświadczenie o zapoznaniu się z przepisami o.i.n., https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/materialy-do-pobrania/152,MATERIALY-DO-POBRANIA.html [dostęp: 18.09.2023].

Co to oznacza, że pełnomocnik ochrony organizuje szkolenia w zakresie ochrony informacji niejawnych?, https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/szkolenia/147,SZKOLENIA.html [dostęp: 18.09.2023].

Co to jest strefa ochronna?, https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/bezpieczenstwo-fizyczn/150,Kancelarie-tajne-Bezpieczenstwo-fizyczne.html#15 [dostęp:20.09.2023].

Wykaz obowiązujących zaleceń, https://bip.abw.gov.pl/bip/informacje-niejawne-1/bezpieczenstwo-teleinf/zalecenia-w-zakresie-bezpiecze/507,Zalecenia-w-zakresie-bezpieczenstwa-teleinformatycznego.html [dostęp: 20.09.2023].

Co oznacza pojęcie kaskady ważności poświadczenia bezpieczeństwa?, https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/bezpieczenstwo-osobowe/146,BEZPIECZENSTWO-OSOBOWE.html#11[dostęp: 25.09.2023].