Ewa Gwardzińska

Bezpieczeństwo teleinformatyczne informacji niejawnych

We współczesnym świecie informacja stanowi wyjątkowo cenne dobro. Większość informacji przekazywanych jest w formie elektronicznej. Zapewnienie bezpieczeństwa teleinformatycznego ma priorytetowe znaczenie, ze względu na szybko rozwijający się cyberterroryzm. Szczególnie dotyczy to tak specyficznej kategorii informacji, jaką stanowią informacje niejawne[1)].

Ustawa o ochronie informacji niejawnych nie zawiera prawnej definicji informacji niejawnych. Należy przyjąć że informacje niejawne to te, którym wytwórca nadał jedną z czterech klauzul tajności: ściśle tajne, tajne, poufne lub zastrzeżone. Klasyfikacja informacji niejawnych oparta jest na kryterium szkody, która może powstać w wyniku jej ujawnienia. I tak w przypadku informacji niejawnych mających klauzulę *ściśle tajne*, ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej, przez to, że:

1) zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej;
2) zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej;
3) zagrozi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej;
4) osłabi gotowość obronną Rzeczypospolitej Polskiej;
5) doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie;
6) zagrozi lub może zagrozić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie;
7) zagrozi lub może zagrozić życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych albo świadków, o których mowa w art. 184 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555, z późn. zm. 5), lub osób dla nich najbliższych.

Informacjom niejawnym nadaje się klauzulę *tajne*, jeżeli ich nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej, przez to, że:
1) uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej;

2) pogorszy stosunki Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi;
3) zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych Rzeczypospolitej Polskiej;
4) utrudni wykonywanie czynności operacyjno-rozpoznawczych, prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby albo instytucje do tego uprawnione;
5) w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości;
6) przyniesie stratę znacznych rozmiarów w interesach ekonomicznych Rzeczypospolitej Polskiej.

Informacjom niejawnym nadaje się klauzulę *poufne,* jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej, przez to, że:

1) utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
2) utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;
3) zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli;
4) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;
5) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli, lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
6) zagrozi stabilności systemu finansowego Rzeczypospolitej Polskiej;
7) wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

Informacjom niejawnym nadaje się klauzulę *zastrzeżone*, jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości, albo interesów ekonomicznych Rzeczypospolitej Polskiej.

Informacje niejawne, którym nadano określoną klauzulę tajności:
1) mogą być udostępnione wyłącznie osobie uprawnionej, i tylko w zakresie niezbędnym do wykonywania obowiązków służbowych,
2) muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do nadanej klauzuli tajności;
3) muszą być chronione odpowiednio do nadanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w ustawie i w przepisach wykonawczych wydanych na jej podstawie.

Klauzula *ściśle tajne* potwierdza zdolność do ochrony informacji niejawnych o klauzuli:

a) *ściśle tajne* przez okres 5 lat od daty wystawienia,

b) *tajne* przez okres 7 lat od daty wystawienia,

c) *poufne* przez okres 10 lat od daty wystawienia;

Klauzula *tajne* potwierdza zdolność do ochrony informacji niejawnych o klauzuli:
a) t*ajne* przez okres 7 lat od daty wystawienia,

b) *poufne* przez okres 10 lat od daty wystawienia.

Klauzula „poufne" potwierdza zdolność do ochrony informacji niejawnych o tej klauzuli przez okres 10 lat od daty wystawienia.

Świadectwa akredytacji bezpieczeństwa

Instytucja ta wprowadzona została nowymi regulacjami ustawy o ochronie informacji niejawnych, która obowiązuje od 2 stycznia 2011 r.[6)] Jest ona potwierdzeniem udzielenia przez Agencję Bezpieczeństwa Wewnętrznego (ABW) lub Służbę Kontrwywiadu Wojskowego (SKW), akredytacji dla systemu przetwarzającego informacje niejawne o klauzuli *poufne* lub wyższej, oraz określa warunki ważności świadectwa i zasady przeprowadzania audytów związanych z nadzorem nad systemem teleinformatycznym. Zastąpi to obowiązujący do tej pory certyfikat bezpieczeństwa teleinformatyczny[7)], pozostawiając pojęcie certyfikat tylko dla urządzeń i narzędzi kryptograficznych oraz środków ochrony elektromagnetycznej.

Do wydania świadectwa bezpieczeństwa teleinformatycznego muszą być spełnione następujące kryteria[6)]:

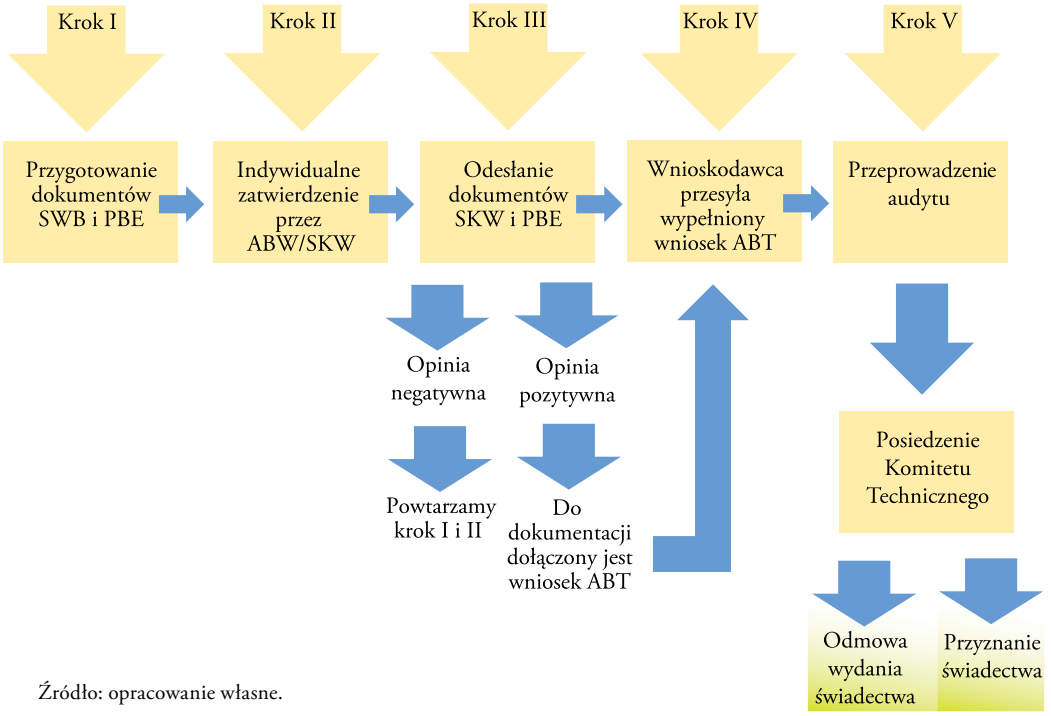
- dokonanie pozytywnej oceny dokumentacji bezpieczeństwa teleinformatycznego,
- pozytywny wynik audytu bezpieczeństwa teleinformatycznego.

Z akredytacji na zasadzie wyjątku wyłączone są systemy teleinformatyczne oraz współpracujące z nimi środki techniczne, zlokalizowane poza siedzibą podmiotów realizujących czynności operacyjno-rozpoznawcze, służące do pozyskiwania i przekazywania informacji niejawnych zdobytych w trakcie działań operacyjno-rozpoznawczych, oraz systemy przetwarzające informacje o klauzuli *poufne*, gdzie na mocy specjalnych uprawnień ABW lub SKW może odstąpić od przeprowadzenia audytu bezpieczeństwa, i akredytować system na podstawie przekazanej dokumentacji bezpieczeństwa.

W przypadku akredytacji systemów teleinformatycznych przetwarzających informacje niejawne obowiązują dwie podstawowe zasady, w zależności od kategoryzacji informacji niejawnych. W przypadku systemów przetwarzających informacje niejawne oznaczonych klauzulą *zastrzeżone,* akredytacji bezpieczeństwa teleinformatycznego udziela kierownik jednostki organizacyjnej w której będzie funkcjonował system, a w przypadku systemu obsługującego wiele podmiotów – kierownik jednostki organizującej system.

Uprawnienie kierownika jednostki organizacyjnej w zakresie akredytacji podlega kontroli ABW lub SKW (zgodnie z ich kompetencją), gdzie powinien on przekazać dokumentację bezpieczeństwa teleinformatycznego akredytowanego przez siebie systemu. W trakcie weryfikacji dokumentacji przekazanej przez kierownika jednostki organizacyjnej, ABW lub SKW może zlecić przeprowadzenie dodatkowych czynności zwiększających bezpieczeństwo systemu. W tym przypadku kierownik jednostki organizacyjnej zobowiązany jest w terminie 30 dni poinformować właściwe służby o realizacji wskazanych zaleceń. W szczególnie uzasadnionych przypadkach ABW lub SKW może nakazać kierownikowi jednostki organizacyjnej wstrzymanie przetwarzania informacji niejawnych o klauzuli *zastrzeżone* w systemach akredytowanych przez kierownika jednostki organizacyjnej. Ma to zapobiec akredytowaniu przez kierownika jednostki organizacyjnej systemów, które nie spełniają podstawowych zasad bezpieczeństwa teleinformatycznego, lub zabezpieczonych niezgodnie z wymaganymi standardami.

Rysunek 1 **Algorytm audytu bezpieczeństwa teleinformatycznego**



Źródło: opracowanie własne.

Natomiast systemy teleinformatyczne przetwarzające informacje niejawne o klauzuli *poufne* lub wyższej, są akredytowane przez ABW lub SKW, zgodnie z ich kompetencjami. Akredytacja udzielana jest na czas określony, nie dłuższy niż pięć lat.

Algorytm audytu bezpieczeństwa

Procedura audytu bezpieczeństwa systemu lub sieci teleinformatycznej informacji niejawnych przebiega w pięciu krokach (rysunek 1). Pierwszy polega na przygotowaniu dokumentów Szczególnych Wymagań Bezpieczeństwa (SWB) oraz Procedur Bezpiecznej Eksploatacji (PBE). Opracowuje się je na etapie projektowania, bieżąco uzupełnia na etapie wdrażania i modyfikuje na etapie eksploatacji, przed dokonaniem zmian w systemie teleinformatycznym. Podstawą dokonania wszelkich zmian jest przeprowadzenie procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie.

Krok drugi obejmuje przesłanie dokumentacji SBW oraz PBE do Agencji Bezpieczeństwa Wewnętrznego lub Służby Kontrwywiadu Wojskowego, gdzie podlegają one procedurze indywidualnej oceny bezpieczeństwa w terminie 30 dni. Termin ten może być jednak przedłużony o kolejne 30 dni, zależnie od stopnia skomplikowania systemu.

Krok trzeci dotyczy wyniku oceny przeprowadzonego postępowania. Wynik pozytywny stanowi podstawę do zatwierdzenia przez ABW lub SKW dokumentacji bezpieczeństwa systemu teleinformatycznego, i wraz z wnioskiem Akredytacji Bezpieczeństwa Teleinformatycznego (ABT) przesyłany jest do wnioskodawcy. Wynik negatywny kończy bieg procedury na tym etapie, i całą procedurę (krok I i II) należy powtarzać od początku.

Następnie wnioskodawca odsyła wypełniony wniosek ABT do ABW lub SKW (krok IV), i uruchamiana jest procedura audytu sieci czy systemu teleinformatycznego (krok V) na Posiedzeniu Komitetu Technicznego, który po

Tablica 1 **Opłaty za badania i ocenę bezpieczeństwa urządzenia lub narzędzia przeznaczonego do ochrony informacji niejawnych realizującego zabezpieczenia teleinformatyczne**

Rodzaj opłaty	Kwota bazowa* (w PLN)	Współczynnik (%)	Wartość (w PLN)
urządzenie lub narzędzie przeznaczone jest do ochrony informacji niejawnych o klauzuli *ściśle tajne*	3 604,80	100	**3 604,80**
urządzenie lub narzędzie przeznaczone jest do ochrony informacji niejawnych o klauzuli *tajne*	3 604,80	75	**2703,60**
urządzenie lub narzędzie przeznaczone jest do ochrony informacji niejawnych o klauzuli *poufne*	3 604,80	50	**1802,40**
urządzenie lub narzędzie przeznaczone jest do ochrony informacji niejawnych o klauzuli *zastrzeżone*	3 604,80	25	**901,20**

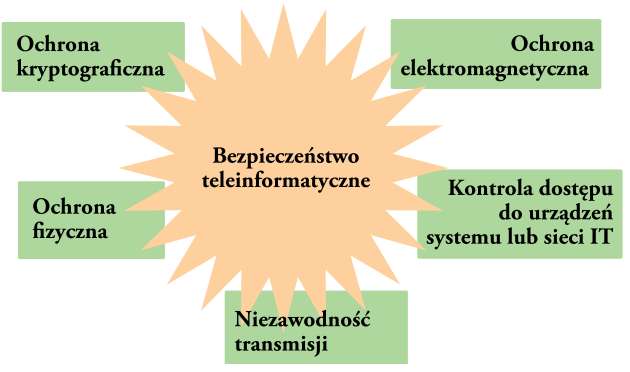
Legenda: *Podstawa kwoty bazowej: obwieszczenie Prezesa Głównego Urzędu Statystycznego z dnia 19 stycznia 2011 r. w sprawie przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw, bez wypłat nagród z zysku w czwartym kwartale 2010 r.

Źródło: opracowanie własne na podstawie projektu Rozporządzenia Prezesa Rady Ministrów z dnia 10 maja 2011 r., w sprawie opłat za przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego czynności z zakresu bezpieczeństwa teleinformatycznego.

wnikliwej analizie dostarczonych dokumentów decyduje o wydaniu świadectwa bezpieczeństwa teleinformatycznego, lub o odmowie, w terminie sześciu miesięcy. Termin ten może być przedłużony o kolejne sześć miesięcy, ze względu na stopień skomplikowania systemu lub sieci teleinformatycznej. Od odmowy udzielenia akredytacji, a tym samym wydania świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego, nie przysługuje odwołanie.

Procedura wydania świadectwa akredytacji podlega opłacie. Wyjątek dotyczy budżetowych jednostek organizacyjnych oraz przedsiębiorców, którzy na mocy odrębnych ustaw obowiązani są do wykonywania zadań publicznych na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Obecnie obowiązuje Rozporządzenie Prezesa Rady Ministrów z 30 września 2005 r., w sprawie wysokości opłat za przeprowadzenie przez służbę ochrony państwa czynności z zakresu bezpieczeństwa teleinformatycznego, wydane na podstawie już nie obowiązującej ustawy z 1998 r.; ale istnieje już nowy projekt rozporządze-

Rysunek 2 **Bezpieczeństwo teleinformatyczne**



Źródło: opracowanie własne.

nia, który niebawem wejdzie w życie. Poniższa tabela przedstawia wysokość opłat za czynności teleinformatyczne według projektu nowego rozporządzenia Prezesa Rady Ministrów z dnia 10 maja 2011 r., w sprawie opłat za przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego czynności z zakresu bezpieczeństwa teleinformatycznego.

Podstawowe wymagania bezpieczeństwa teleinformatycznego

Bezpieczeństwu informacji niejawnych przetwarzanych w systemie teleinformatycznym służy wdrożenie spójnego zbioru zabezpieczeń w celu zapewnienia poufności, integralności i dostępności tych informacji. Wdraża się go przed rozpoczęciem oraz w trakcie przetwarzania informacji w systemie lub w sieci teleinformatycznej, zarówno na etapie planowania, projektowania, wdrażania, eksploatacji, jak i wycofania.

Bezpieczeństwo teleinformatyczne informacji niejawnych zapewnione jest poprzez: ochronę fizyczną, kontrolę dostępu do urządzeń systemu lub sieci (hasła, loginy), ochronę kryptograficzną, ochronę elektromagnetyczną oraz niezawodność transmisji (patrz rysunek 2). W każdym systemie niejawnym za prawidłowe funkcjonowanie systemu są odpowiedzialni: Pełnomocnik ds. Ochrony Informacji Niejawnych, Inspektor Bezpieczeństwa Teleinformatycznego i Administrator.

Za właściwą organizację Bezpieczeństwa Teleinformatycznego odpowiada Kierownik Jednostki Organizacyjnej. Do jego obowiązków należy:
– 1) opracowanie dokumentacji bezpieczeństwa,
– 2) ochrona fizyczna, elektromagnetyczna, kryptograficzna,
– 3) kontrola dostępu do urządzeń systemu lub sieci teleinformatycznej,
– 4) bezpieczeństwo transmisji,
– 5) szkolenia z zakresu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy,
– 6) powiadamianie ABW lub SKW o zaistniałych incydentach dotyczących bezpieczeństwa teleinformatycznego, informacji niejawnych oznaczonych klauzulą *poufne* lub wyższej.

Użytkownicy systemu teleinformatycznego przetwarzającego informacje niejawne posiadają różne uprawnienia w dostępie do informacji niejawnych, dlatego też systemy teleinformatyczne muszą funkcjonować w różnych trybach bezpieczeństwa pracy. Są trzy takie tryby:

- Dedykowany – wszyscy użytkownicy mają uprawnienia dostępu do informacji niejawnej o najwyższej klauzuli tajności, oraz wszyscy użytkownicy mają uzasadnioną potrzebę dostępu do wszystkich informacji niejawnych przetwarzanych w systemie;
- systemowy – wszyscy użytkownicy mają uprawnienia dostępu do informacji niejawnej o najwyższej klauzuli tajności, ale nie wszyscy użytkownicy mają uzasadnioną potrzebę dostępu do wszystkich informacji niejawnych przetwarzanych w systemie;
- wielopoziomowy – nie wszyscy użytkownicy mają uprawnienia do dostępu do informacji niejawnej o najwyższej klauzuli tajności, jakie mogą być przetwarzane w tym systemie informatycznym.

Odpowiednie zabezpieczenie systemów teleinformatycznych przetwarzających informacje niejawne przed nieuprawnionym dostępem do nich osób nieuprawnionych, ma priorytetowe znaczenie dla zapewnienia bezpieczeństwa państwa, obronności kraju oraz intere-

su publicznego. Uzyskanie świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego daje gwarancję ochrony informacji niejawnych przed działaniem złośliwego oprogramowania, czy incydentami w sferze dostępu osób nieuprawnionych do informacji niejawnych. Dla zapewnienia większego bezpieczeństwa teleinformatycznego jest ono monitorowane na każdym etapie wdrażania systemu informatycznego, od planowania, poprzez projektowanie, wdrażanie, eksploatację, aż do wycofania go z użytku. Ale warto pamiętać, że świadectwo akredytacji systemów informatycznych nie daje nigdy stuprocentowej gwarancji ochrony informacji niejawnych, gdyż bezpieczeństwo teleinformatyczne zależy w dużym stopniu od ludzi obsługujących te systemy.

Bibliografia

1. *Europe and the global information society*, Bangemann report recommendations to the European Council, Brussels, 26 May 1999.
2. Obwieszczenie Prezesa Głównego Urzędu Statystycznego z dnia 19 stycznia 2011 r., w sprawie przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw, bez wypłat nagród z zysku w czwartym kwartale 2010 r.
3. Projekt Rozporządzenia Prezesa Rady Ministrów z dnia 10 maja 2011 r., w sprawie opłat za przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego, czynności z zakresu bezpieczeństwa teleinformatycznego.
4. Projekt Rozporządzenia Prezesa Rady Ministrów z dnia 21 stycznia 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego.
5. Rozporządzenie Prezesa Rady Ministrów z 30 września 2005 r w sprawie wysokości opłat za przeprowadzenie przez służbę ochrony państwa czynności z zakresu bezpieczeństwa teleinformatycznego, Dz. U. z 2005 r., Nr 200, poz. 1652.
6. *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*, Dz. U. z 2010 r., Nr 182, poz. 1228.
7. *Ustawa z dnia 22 stycznia 1998 r. o ochronie informacji niejawnych*, Dz. U. z 1998 r., Nr 11, poz. 95 z późn. zm.

Dr **Ewa Gwardzińska**, Katedra Prawa Administracyjnego i Finansowego Przedsiębiorstw, SGH.