Ochrona danych i systemów

Ochrona danych tajnych

Łukasz Brewczyński Filip Dziedzic Rafał Studnicki

Informatyka
Wydział Elektrotechniki, Automatyki, Informatyki i Inżynierii Biomedycznej
Akademia Górniczo-Hutnicza im. St. Staszica w Krakowie

---

1. Wstęp

Dokument przedstawia wymagania dotyczące potencjalnego systemu informatycznego, który miałby zdolność do przetwarzania danych niejawnych zgodnie z wymogami polskiego prawa. Trzeba zwrócić uwagę, iż systemy do przetwarzania danych niejawnych o klauzuli wyższej od zastrzeżone, wymagają indywidualnego postępowania akredytacyjnego, prowadzonego przez uprawniony do tego organ państowy, jakim w tym przypadku jest Agencja Bezpieczeństwa Wewnętrznego. Ze względu na uwarunkowania prawne nie można zagwarantować, iż system spełniający wymagania przedstawione w ninejszym dokumencie zostanie dopuszczony do użytku.

2. Definicje

Informacja niejawna – polski termin prawniczy, który został zdefiniowany w ustawie o ochronie informacji niejawnych z 5 sierpnia 2010 roku. Oznacza informację, która wymaga ochrony przed nieuprawnionym ujawnieniem, niezależnie od formy i sposobu jej wyrażenia, także w trakcie jej opracowania.

Przetwarzanie informacji niejawnych – wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie.

Agencja Bezpieczeństwa Wewnętrznego (ABW) – służba specjalna powołana do ochrony porządku konstytucyjnego Rzeczypospolitej Polskiej.

Służba Kontrwywiadu Wojskowego (SKW) – służba specjalna właściwa w sprawach ochrony przed zagrożeniami wewnętrznymi dla obronności Rzeczypospolitej Polskiej oraz bezpieczeństwa i zdolności bojowej Sił Zbrojnych Rzeczypospolitej Polskiej.

System TI – system teleinformatyczny

UODO – Ustawa o ochronie danych osobowych

GIODO – Generalny Inspektor Ochrony Danych Osobowych

3. Uwarunkowania prawne

3.1 Zgodność z ustawią o ochronie danych osobowych

Zgodnie z ustawą o ochronie danych osobowych (dalej zwaną UODO), która obowiązuje w Polsce od 1997 r., a dokładnie artykułem 40, administrator danych jest zobowiązany zgłosić zbiór danych do rejestracji GIODO, chyba że zachodzi jeden z wyjątków przewidzianych w UODO (przykładem takiego wyjątku mogą być dane przetwarzane w celu zatrudnienia pracownika u administratora danych).

Poniżej lista wymogów dotyczących rejestracji w GIODO:

- zebranie danych w zgodzie z którąś z przesłanek określonych w art. 23 ust. 1 UODO. Aby zachować zgodność z tym zapisem, należy w formularzu rejestracyjnym dołączyć klauzulę o zgodzie na przetwarzanie danych osobowych.
- dopełnienie obowiązków informacyjnych (art. 24 i 25 UODO). Administrator danych jest zobowiązany do przekazania użytkownikowi informacji o:
  - Siedzibie i pełnej nazwie firmy
  - Celu zebrania danych osobowych
  - Prawie do wglądu do swoich danych i ich poprawiania
  - Dobrowolności podania tych danych
- podjęcie środków technicznych niezbędnych do zabezpieczenia przetwarzanych danych osobowych (art. 36 ust. 1 UODO oraz przepisy wskazane w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych)
  - Administrator ma obowiązek zadbać o to aby żadna osoba niepowołana nie miała fizycznego dostępu do sytemu przetwarzającego dane osobowe, jak również ma obowiązek zabezpieczenia przed wyciekiem danych (atak hakerski)
- podjęcie środków organizacyjnych niezbędnych do zabezpieczenia przetwarzanych danych osobowych (art. 36, art. 37, art. 38, art. 39 oraz przepisy wskazane w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych)
- zadbanie o legalne powierzenie przetwarzania danych osobowych, jeżeli firma ma zamiar wykorzystywać w procesie przetwarzania danych także inne firmy (np. w przypadku hostingu, biura rachunkowego, call center)
- udostępniać dane osobowe zgodnie z wymogami UODO

3.2 Podstawa prawna dotycząca przetwarzania danych niejawnych

Głównym dokumentem regulującym obostrzenia w zakresie dostępu do danych niejawnych, jest ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. We wspomnianym dokumencie znajdują się definicje danych niejawnych o poszczególnych klauzulach tajności, ograniczenia w zakresie dostępu do takich danych, definicja odpowiednich organów prawnych udzielających upoważnień oraz akredytacji we wspomnianych zakresach. Wartym podkreślenia jest fakt, iż ustawa nie precyzuje konkretnych wymagań względem systemów teleinformatycznych. Podmiotem odpowiedzialnym za precyzowanie wymagań oraz udzielanie akredytacji dla odpowiednich rozwiązań jest Agencja Bezpieczeństwa Wewnętrznego. Do jej kompetencji należy weryfikowanie składowych elementów systemów takich jak: generatory kluczy, algorytmy oraz urządzenia szyfrujące, urządzenia komunikacyjne, etc. Wszystkie te informacje dostępne są na stronie internetowej ABW. Chcąc wdrożyć system teleinformatyczny przetwarzającym dane niejawne, konieczne jest posiadanie odpowiedniej akredytacji wydanej przez ABW. Podstawą do uzyskania pozytywnej opinii

od tego organu, jest przygotowanie dokumentacji bezpieczeństwa systemu, zawierającej szczegółowy opis działania, architekturę systemu, oraz analizę podatności na zagrożenia zwaną analizą ryzyka. Warto dodać, że wszystkie osoby pracujące nad wdrożeniem takiego rozwiązania, utrzymaniem bądź też użytkowaniem, również muszą posiadać oficjalne uprawnienia wydane przez ABW w postaci poświadczeń bezpieczeństwa do danego poziomu danych (klauzuli tajności) które system przetwarza. Uprawnienia takie posiadają praktycznie wszyscy pracownicy administracji publicznej lub też organizacji w których system do przetwarzania danych niejawnych istnieje.

3.3. Systemy teleinformatyczne przeznaczone do przetwarzania krajowych informacji niejawnych o klauzuli „poufne" lub wyższej

Systemy takie są akredytowane przez ABW lub SKW. ABW albo SKW udziela albo odmawia udzielenia akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „poufne" lub wyższej, w terminie 6 miesięcy od otrzymania kompletnej dokumentacji bezpieczeństwa systemu teleinformatycznego. W uzasadnionych przypadkach, w szczególności wynikających z rozległości systemu i stopnia jego skomplikowania, termin ten może być przedłużony o kolejne 6 miesięcy. Od odmowy udzielenia akredytacji nie służy odwołanie.

Proces udzielania przez ABW akredytacji bezpieczeństwa teleinformatycznego systemowi teleinformatycznemu przeznaczonemu do przetwarzania informacji niejawnych o klauzuli „poufne" lub wyższej składa się z następujących etapów:

- dokonanie przez ABW oceny dokumentacji bezpieczeństwa systemu teleinformatycznego,
- złożenie do ABW wniosku WA o przeprowadzenie audytu bezpieczeństwa systemu teleinformatycznego oraz wydanie świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego,
- przeprowadzenie przez ABW audytu bezpieczeństwa systemu teleinformatycznego.

Proces udzielania przez ABW akredytacji bezpieczeństwa teleinformatycznego kończy się wydaniem świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego.

Podstawą do wydania przez ABW świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego jest:

- zatwierdzona przez ABW dokumentacja bezpieczeństwa systemu teleinformatycznego,
- wyniki audytu bezpieczeństwa systemu teleinformatycznego prowadzonego przez ABW, weryfikującego poprawność realizacji wymagań i procedur, określonych w dokumentacji bezpieczeństwa, przy czym dla systemu przeznaczonego do przetwarzania informacji niejawnych o klauzuli „poufne" ABW może odstąpić od przeprowadzenia takiego audytu.

4. Bezpieczeństwo teleinformatyczne systemu

Aby zapewnić bezpieczeństwo teleinformatyczne informacji niejawnych w potencjalnym systemie, należy zrealizować szereg wymaganych przedsięwzięć. Poniżej przedstawiono listę niezbędnych działań:

- organizacja i zarządzania bezpieczeństwem,
- bezpieczeństwo fizyczne,
- bezpieczeństwo osobowe,
- bezpieczeństwo nośników informacji,
- bezpieczeństwo sprzętowe,
- bezpieczeństwo oprogramowania,
- ochronę kryptograficzną,
- ochrona elektromagnetyczna,
- bezpieczeństwo transmisji,
- kontrola dostępu do systemu lub sieci teleinformatycznych

4.1 Organizacja i zarządzanie bezpieczeństwem

W celu spełnienia tego wymogu należy wyznaczyć odpowiedzialne osoby za poszczególne elementy bezpieczeństwa, a także określić dla nich zakres obowiązków i odpowiedzialności. Kierownik jednostki odpowiada za ochronę informacji niejawnych w jednostce organizacyjnej. Przestrzegania przepisów o ochronie informacji niejawnej egzekwować musi pełnomocnik ochrony. Gdy dojdzie do incydentu, w wyniku którego naruszuono procedury eksploatacji danych o klauzuli 'poufne' lub wyższej, zobowiązany jest on do poinformowania kierownika jednostki organizacyjnej, a także Służby Ochrony Państwa. Wymagane jest również przeprowadzenie procedury wyjaśniającej okoliczności zdarzenia.

Administrator systemu i Inspektor BTI jest wyznaczany przez kierownika jednostki organizacyjnej. Do ich obowiązków należy zapenienie bezpieczeństwa teleinformatycznego przed przystąpieniem do przetwarzania informacji niejawnych w jednostce organizacyjnej.

4.2 Bezpieczeństwo fizyczne

Aby zapewnić ochronę fizyczną systemu należy przeprowadzić właściwy wybór pomieszczenia w którym przetrzymywane będą urządzenia systemu, bądź sieci. Trzeba podkreślić, że dane z klauzulami 'ściśle tajne', 'tajne' oraz 'poufne' wymagają stref ochronnych.

Przy tworzeniu stref ochronnych należy pamiętać o:

- wyborze pomieszczeń, w których zainstalowane będą newralgiczne elementy systemu (należy unikać parteru, pomieszczeń od strony ulicy, bądź budynków z których można prowadzić nasłuch),
- ograniczeniu liczby wejść do stref ochronnych do jednego wejścia głównego oraz wyjścia awaryjnego, ograniczenie liczby okien,
- wzmocnieniu ścian, instalowanie drzwi i okien o zwiększonej wytrzymałości,
- stosowaniu zabezpieczeń mechanicznych, np. zamków posiadających certyfikaty,
- kontrolowaniu wejść i osób przebywających w strefach ochronnych przez pracowników ochrony,
- ścisłym stosowanie procedur kontroli wprowadzania gości do stref ochronnych,
- wspomaganiu kontroli prowadzonej przez pracowników ochrony za pomocą systemów elektronicznych – alarmowych, antywłamaniowych, kontroli dostępu, telewizji przemysłowej,
- stosowaniu środków ochrony przeciwpożarowej
- stosowaniu środków ochrony przed zalaniem

Instalacja urządzeń systemu lub sieci musi odbywać się w sposób zabezpieczający przed nieuprawnionym dostępem, podglądem czy podsłuchem. Dobrą praktyką jest szukanie rozwiązania, które zapewni należyte bezpieczeństwo, nie utrudniając przy tym pracy użytkowników systemu. Mimo to celem nadrzędnym jest ochrona informacji niejawnych przetwarzanych w systemie.

4.3 Bezpieczeństwo osobowe

Użytkownicy systemu winni są posiadać poświadczenie bezpieczeństwa osobowego do najwyższej klauzuli informacji, do jakiej mogą mieć potencjalny dostęp. Osoby, które nie są użytkownikami systemu, a będą miały dostęp do obszarów, w których przetwarzane są dane niejawne muszą być podczas pobytu nadzorowane. Środki ostrożności, które muszą zostać podjęte mają również zapobiegać podejrzeniu ekranów monitorów czy wydruków. Trzeba również pamiętać o odpowiednich szkoleniach personelu, w celu zapewnienia znajomości procedur.

4.4 Bezpieczeństwo nośników informacji

Środki ochrony nośników informacji niejawnych powinny być opisane w szczególnych wymaganiach bezpieczeństwa. Nośniki informacji należy klasyfikować i ewidencjonować odpowiednio do najwyższej klauzuli tajności informacji, które są na nich przechowywane. Za wdrożenie zasad kontroli i ewidencji wszystkich nośników elektronicznych zawierających informacje niejawne odpowiadają pracownicy odpowiedzialni za bezpieczeństwo teleinformatyczne.

4.5 Bezpieczeństwo sprzętowe

Sprzęt oraz urządzenia zastosowane w systemach lub sieciach teleinformatycznych przetwarzających informacje niejawne muszą być odpowiednie do warunków pracy określonych przez lokalizację oraz klauzule tajności informacji przetwarzanych w tych systemach i sieciach.

4.6 Bezpieczeństwo oprogramowania

Zastosowane oprogramowanie musi być odpowiednie do warunków pracy określonych przez klauzule tajności informacji przetwarzanych w tych systemach lub sieciach. Jednym z elementów zapewnienia bezpieczeństwa oprogramowania jest wykonanie kopii zapasowych oryginałów oprogramowania oraz weryfikowanie poprawności ich zapisu.

4.7 Ochrona kryptograficzna

Polega na stosowaniu metod i środków zabezpieczających te informacje poprzez ich szyfrowanie oraz stosowanie innych mechanizmów gwarantujących integralność i zabezpieczenie przed nieuprawnionym ujawnieniem tych informacji lub uwierzytelnienie informacji. Jednym z najefektywniejszych sposobów zabezpieczenia informacji przed dostępem osób nieupoważnionych jest wykorzystywanie technik kryptograficznych.

Techniki kryptograficzne pozwalają chronić poufność i autentyczność informacji. Poufność oznacza, że informacja może być poprawnie odczytana jedynie przez upoważnione osoby (lub programy). Autentyczność oznacza, że informacja może (mogła) być wygenerowana jedynie przez upoważnione osoby w sposób dający się później poprawnie odczytać.

W celu ochrony informacji wykonuje się na niej proces maskowania w taki sposób, aby ukryć jej treść. To działanie nazywane jest szyfrowaniem. Proces odtworzenia informacji uzyskanej w wyniku szyfrowania, nazywamy deszyfrowaniem. Wiadomość przeznaczoną do szyfrowania nazywamy tekstem jawnym lub otwartym, po zaszyfrowaniu – tekstem zaszyfrowanym lub kryptogramem.

Szyfrowanie i odszyfrowanie odbywa się w oparciu o algorytm kryptograficzny, zwany szyfrem, który jest funkcją matematyczną.

Wyróżnia się dwie grupy algorytmów: algorytm symetryczny (z kluczem prywatnym) oraz algorytm asymetryczny (z kluczem publicznym).

4.8 Ochrona elektromagnetyczna

Każde urządzenie, przez które przepływa prąd elektryczny generuje promieniowanie elektromagnetyczne o określonej częstotliwości. Emisja promieniowania odbywa się bez względu na typ komputera / monitora, a jej źródłem są również gniazdka, kable itp. Każdy z tych sygnałów niesie ze sobą pewne informację, z których może skorzystać potencjalny atakujący. Promieniowanie komputera jest na tyle silne, że za pomocą specjalnego urządzenia można je odebrać z odległości kilkuset metrów (nawet do tysiąca). Używane są przez służby specjalne wszystkich krajów świata. Urządzenia te nie występują w katalogach, a ich sprzedaż podlega restrykcjom. Dodatkowo urządzenia te są na tyle małe, że mieszczą się w samochodach osobowych.

Przed "promieniowaniem" poufnych informacji można się zabezpieczyć w różny sposób:

- kabiny elektromagnetyczne /tzw. klatki Farradaya/, w których umieszczane są urządzenia przetwarzające informacje niejawne - są odpowiednio uziemione i poziom promieniowania elektromagnetycznego wychodzący na zewnątrz jest tak niski, że nie jest możliwe jego odczytanie,
- wyklejanie ścian pomieszczeń metalowymi foliami i siatkami, spełniającymi podobną rolę, ale parametry tego zabezpieczenia są nieco niższe niż w przypadku klatek,
- metalowe pudełka, w których umieszcza się sprzęt, emitujący promieniowanie. Mogą być to nie tylko komputery, ale także urządzenia nadawczo — odbiorcze lub szyfratory,
- zabezpieczenie komputerów przenośnych, według amerykańskich norm TEMPEST.

Norma TEMPEST (temporary emanation and spurious transmission) została nadana programowi ochrony przed niekontrolowaną emisją ujawniającą, który powstał w latach 50-tych w USA na zlecenie Pentagonu. Standard ten znany jest również pod nazwami NAG1A, FS222, NACSIM 5100, NSCD. Kontrolę nad normą sprawuje Amerykańska Narodowa Agencja Bezpieczeństwa (NSA). Urządzenia klasy TEMPEST są ściśle kontrolowane, mogą być używane tylko przez kilka instytucji na świecie w tym NATO (co w konsekwencji oznacza Polskę).

Polskie prawo nakłada konieczność utworzenia tzw. sprzętowej strefy ochrony elektromagnetycznej (SSOE), a co za tym idzie wykorzystywanie urządzeń klasy TEMPEST w następujących przypadkach:

- w przypadku systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „poufne", kiedy odległość od urządzeń wchodzących w skład systemu do obszaru pozostającego poza kontrolą wynosi mniej niż 8 m.,
- w przypadku systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „tajne" lub wyższej,
- w przypadku systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych NATO oraz UE oznaczonych klauzulą CONFIDENTIAL lub wyższą.

W zależności od odległości sprzętu IT od obszaru niekontrolowanego konieczne jest wykorzystywanie urządzeń certyfikowanych różnymi normami (zgodnie z tabelą poniżej).

P. ochrony ABW	P. ochrony SKW	Opis
SSOE 0	TPZU 3	Pozwala na użytkowanie sprzętu IT w odległości nie większej niż 20 m od potencjalnego intruza (przy odległości mniejszej niż 8 m wymagane dodatkowe konsultacje z właściwymi służbami ochrony państwa).
SSOE 1	TPZU 2	Pozwala na użytkowanie sprzętu IT w odległości nie mniejszej niż 20 m od potencjalnego intruza.
SSOE 2	TPZU 1	Pozwala na użytkowanie sprzętu IT w odległości nie mniejszej niż 100 m od potencjalnego intruza.

4.9 Bezpieczeństwo transmisji

Warunkiem przekazywania w formie elektronicznej informacji stanowiących tajemnicę państwową poza strefy ochronne jest zastosowanie ochrony kryptograficznej systemu lub sieci teleinformatycznej.

4.10 Kontrola dostępu do systemu

W celu zapewnienia takiej kontroli system lub sieć wyposaża się w mechanizmy kontroli dostępu odpowiednie do klauzuli tajności informacji niejawnych przetwarzanych w tych systemach lub sieciach. Należy pamiętać, aby w celu zapewnienia bezpieczeństwa informacjom niejawnym przetwarzanym w systemie lub sieci wprowadzić i stosować zasady i procedury w zakresie haseł dostępowych, a także, aby systemy i sieci teleinformatyczne przetwarzające informacje niejawne prowadziły automatyczną ewidencję zdarzeń w systemie lub sieci oraz rejestr dostępu do informacji niejawnych przechowywanych na elektronicznych lub magnetycznych nośnikach danych.

5. Eksploatacja systemów teleinformatycznych

Po udzieleniu przez właściwy organ akredytacji bezpieczeństwa teleinformatycznego oraz po jego wdrożeniu systemu teleinformatycznego, na etapie eksploatacji danego systemu należy:

- utrzymywać zgodność systemu teleinformatycznego z jego dokumentacją bezpieczeństwa,
- zapewnić ciągłość procesu zarządzania ryzykiem w systemie teleinformatycznym,
- okresowo przeprowadzać testy bezpieczeństwa w celu weryfikacji poprawności działania poszczególnych zabezpieczeń oraz usuwać ewentualne stwierdzone nieprawidłowości
- w zależności od potrzeb wprowadzać zmiany do systemu teleinformatycznego oraz, jeżeli jest to właściwe, wykonywać testy bezpieczeństwa, a także uaktualniać dokumentację bezpieczeństwa systemu teleinformatycznego, np. w formie aneksów).

Warunkiem ustawowym (art. 49 ust. 4 ustawy) dokonania w systemie teleinformatycznym jakichkolwiek zmian jest wcześniejsze przeprowadzenie procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie, przy czym wprowadzenie modyfikacji mogących mieć wpływ na bezpieczeństwo systemu teleinformatycznego wymaga zgody podmiotu, który udzielił akredytacji bezpieczeństwa teleinformatycznego. W przypadku systemów przeznaczonych do przetwarzania informacji niejawnych oznaczonych klauzulą "zastrzeżone" organizowanych przez podmioty znajdujące się we właściwości ustawowej SKW, wprowadzenie modyfikacji mogących mieć wpływ na bezpieczeństwo danego systemu, wymaga dodatkowo przekazania do SKW uaktualnionej dokumentacji bezpieczeństwa danego systemu teleinformatycznego - uaktualnioną dokumentację należy przesłać w terminie 30 dni od wprowadzenia ww. modyfikacji.

6. Certyfikaty dostępu do danych tajnych dla pracowników

Poświadczenie bezpieczeństwa to dokument tworzony w oparciu o ustawę o ochronie informacji niejawnych umożliwiający danej osobie dostęp do informacji niejawnej, czyli objętej określoną klauzulą tajności (art.5 ustawy). Wystawienie poświadczenia bezpieczeństwa odbywa się po przeprowadzeniu przez służby ochrony państwa (ABW lub SKW) oraz pełnomocnika ochrony szczegółowego postępowania sprawdzającego. 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”

Poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o wyższej klauzuli tajności uprawnia do dostępu do informacji niejawnych o niższej klauzuli tajności. Ustawa o ochronie informacji niejawnych określa:

- Zasady ochrony informacji niejawnych
- Klasyfikację informacji niejawnych
- Zasady przetwarzania informacji niejawnych
- Tryb postępowania sprawdzającego
- Zasady przeprowadzania szkolenia w zakresie ochrony informacji niejawnych
- Zasady bezpieczeństwa osobowego
- Zasady działania kancelarii tajnych
- Zasady bezpieczeństwa teleinformatycznego i przemysłowego

7. Podstawy prawne

Ustawy i rozporządzenia mające zastosowanie w przypadku ochrony danych niejawnych:

- Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych
- Ustawa z dnia 13 kwietnia 2007 r. o kompatybilności elektromagnetycznej
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z późniejszymi zmianami
- Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego
- Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie wzoru świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego

8. Podsumowanie

W niniejszym dokumencie wykazano wymagania względem systemu przetwarzającego dane niejawne. Jak udało się pokazać, iż spełnienie restrykcyjnych wymagań nie jest czynnością prostą. Proces weryfikacji przez ABW może trwać latami. Ustawa o ochronie informacji niejawnych precyzuję co prawda czas na postępowanie akredytacyjne, lecz w rzeczywistości zastosowana w nim litera prawa odnosi się jedynie do pierwszej iteracji tego procesu. W przypadku zgłoszenia uwag i wątpliwości do przedstawionej dokumentacji bezpieczeństwa, proces może trwać znacznie dłużej niż „optymistyczne" 3 miesiące. Wart podkreślenia jest także fakt, iż dopuszczenie systemu do użytku nie jest dożywotnie. W przedstawionym wykazie dopuszczonych urządzeń widnieje data ważności certyfikatu, co oznacza, iż proces certyfikacji należy sukcesywnie ponawiać. Audyty bezpieczeństwa prowadzone przez ABW dają, przynajmniej pozorną, gwarancję utrzymania tajemnic państwowych na wysokim poziomie bezpieczeństwa.

9. Bibliografia

- [Ustawa o ochronie informacji niejawnych] (http://www.iniejawna.pl/przyciski/ustawa.html#1)
- [Ochrona informacji niejawnych] (http://archiwalna.polsl.pl/adc/obrona/docs/OchrInf.pdf)
- [SKW] (http://www.skw.gov.pl/ZBIN/akredytacja.htm)
- [Przetwarzanie informacji niejawnych] (http://lexvin.pl/prawo/4614/Przetwarzanie-informacji-niejawnych)
- [ORGANIZACJA OCHRONY INFORMACJI NIEJAWNYCH] (http://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/organizacja-ochrony-in/145,ORGANIZACJA-OCHRONY-INFORMACJI-NIEJAWNYCH.html)
- [Bezpieczeństwo teleinformatyczne informacji niejawnych] (http://www.4itsecurity.pl/index.php/kategorie/informacje-niejawne/71-bezpieczenstwo-teleinformatyczne-informacji-niejawnych)