Certyfikowanie procesów wytwórczych oprogramowania

Certyfikacja sprzętu i systemów teleinformatycznych do przetwarzania danych niejawnych

Łukasz Brewczyński Filip Dziedzic Rafał Studnicki

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

---

1. 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

2. Wstęp

Polskie prawo reguluje pewne wymagania dotyczące systemów oraz sprzętu informatycznego wykorzystywanego do przetwarzania danych niejawnych. Głównym dokumentem regulującym te obostrzenia jest ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. W dokumencie tym znajdują się definicje danych niejawnych (wyróżnione są cztery poziomy tajności danych: zastrzeżone, poufne, tajne oraz ściśle tajne), ograniczenia w zakresie dostępu do takich danych, definicja odpowiednich organów prawnych udzielających upoważnień oraz akredytacji we wspomnianych zakresach. Ważna kwestią jest to, że ustawa sama w sobie nie precyzuje konkretnych wymagań stawianych systemom informatycznym. Określa natomiast podmioty odpowiedzialne za stawianie takich wymagań i akredytowanie konkretnych systemów informatycznych. Podmiotami tymi są:

- Agencja Bezpieczeństwa Wewnętrznego (ABW)
- Służba Kontrwywiadu Wojskowego (SKW)

Do ich kompetencji należy weryfikowanie składowych elementów systemów takich jak: generatory kluczy, algorytmy oraz urządzenia szyfrujące, urządzenia komunikacyjne itp. Więcej informacji na ten temat można znaleźć na oficjalnej stronie internetowej. Przykładem może być lista aktualnie dostępnych narzędzi oraz urządzeń kryptograficznych, które zostały dopuszczone do przetwarzania i składowania informacji niejawnych.

Każdy system teleinformatyczny przetwarzający dane niejawne musi posiadać akredytację wydaną przez ABW lub SKW. Podstawą do uzyskania tego typu zaświadczenia jest przygotowania niezwykle obszernej dokumentacji systemu oraz złożenia szeregu wniosków. Ponadto niezbędne jest przeprowadzenie analizy ryzyka związanego z przechowywaniem informacji niejawnych, czyli przeprowadzenia tzw. analizy ryzyka (metoda jej przeprowadzenia nie jest wyspecyfikowana i jej wybór leży w gestii składającego wniosek).

Mówi się, że nawet najbezpieczniejszy system teleinformatyczny nie jest w pełni bezpieczny, a najsłabszym jego ogniwem często okazuje się człowiek. ABW również doskonale o tym wie, stąd też poza technicznymi aspektami systemu, w składanym wniosku należy również zamieścić listę użytkowników, administratorów oraz wszystkich innych osób mających styczność z danym systemem. Wszystkie te osoby muszą posiadać odpowiednie poświadczenia bezpieczeństwa dostępu do danych niejawnych (również wydawane przez ABW). Poziom dostępu do danych niejawnych musi odpowiadać poziomowi tajności przetwarzanych przez dany system danych.

3. Akredytacja

Akredytacja bezpieczeństwa teleinformatycznego systemów teleinformatycznych przeznaczonych do przetwarzania krajowych informacji niejawnych nie jest łatwa ani tania (kosztują szkolenia użytkowników / administratorów systemu, a także samo przygotowanie dokumentacji SWB i PBE). Co więcej, pomimo deklarowanego okresu trzech miesięcy, w ciągu których ABW zobowiązuje się do odpowiedzi na składany wniosek, proces akredytacji systemu wcale nie musi się zakończyć. Spowodowane jest to tym, że ustawowy termin trzech miesięcy mówi jedynie o pierwszej iteracji składanej dokumentacji oraz wniosków, a nie o cały procesie akredytacji. Przed przystąpieniem do próby certyfikowania systemu teleinformatycznego w zakresie przetwarzania danych niejawnych należy się w stu procentach upewnić, że taki certyfikat jest niezbędny danej organizacji / danemu przedsiębiorstwu. Należy również pamiętać, że akredytacja nie jest „dożywotnia", a najdłuższy okres na jaki można uzyskać akredytację wynosi 5 lat.

3.1. Systemy przeznaczone do przetwarzania krajowych informacji niejawnych o klauzuli "zastrzeżone"

Systemy takie są akredytowane przez kierownika jednostki organizacyjnej przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego. W ciągu 30 dni od udzielenia akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone", kierownik jednostki organizacyjnej przekazuje odpowiednio ABW lub SKW dokumentację bezpieczeństwa akredytowanego przez siebie systemu teleinformatycznego. W ciągu 30 dni od otrzymania dokumentacji bezpieczeństwa systemu teleinformatycznego ABW albo SKW może przedstawić kierownikowi jednostki organizacyjnej, który udzielił akredytacji bezpieczeństwa teleinformatycznego, zalecenia dotyczące konieczności przeprowadzenia dodatkowych czynności związanych z bezpieczeństwem informacji niejawnych. Kierownik jednostki organizacyjnej w terminie 30 dni od otrzymania zalecenia informuje odpowiednio ABW lub SKW o realizacji zaleceń. W szczególnie uzasadnionych przypadkach ABW albo SKW może nakazać wstrzymanie przetwarzania informacji niejawnych w systemie teleinformatycznym posiadającym akredytację bezpieczeństwa teleinformatycznego.

3.2. 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. Dokumentacja bezpieczeństwa

Głównym elementem wniosków składanych do ABW lub SKW jest dokumentacja bezpieczeństwa systemu teleinformatycznego. W jej skład wchodzą dwa dokumenty:

- szczególne wymagania bezpieczeństwa (SWB),
- procedury bezpiecznej eksploatacji (PBE).

Dokumentacja bezpieczeństwa (dokumenty SWB i PBE) stanowi element procesu akredytacji. Na podstawie dokumentacji bezpieczeństwa i audytu bezpieczeństwa systemu teleinformatycznego udziela się akredytacji. Za opracowanie i przekazanie dokumentów SWB i PBE do ABW albo SKW odpowiada kierownik jednostki organizacyjnej, w której będzie funkcjonował system teleinformatyczny. Podsumowując, bez dokumentów SWB i PBE nie ma możliwości uzyskania akredytacji bezpieczeństwa systemu TI. Dokumenty te podlegają ocenie i zatwierdzeniu przez ABW albo SKW.

4.1. Dokument SWB

Dokument SWB, czyli szczególne wymagania bezpieczeństwa, jest przede wszystkim opisem sposobu zarządzania bezpieczeństwem systemu teleinformatycznego. Innymi słowy SWB jest to dokument opisujący (dokumentujący) system teleinformatyczny wraz z zastosowanymi środkami ochrony tegoż systemu.

4.1.1. Zawartość dokumentu SWB

Dokument SWB powinien zawierać:

- klauzule tajności informacji niejawnych
- grupy użytkowników i ich uprawnienia w systemie TI
- tryb bezpieczeństwa pracy
- przeznaczenie systemu TI
- funkcjonalność systemu TI
- wymagania eksploatacyjne odnoszące się do wymiany informacji
- lokalizację systemu TI

Opis procesu zarządzania ryzykiem:

- opis metodyki szacowania ryzyka
- raport z procesu szacowania ryzyka
- informacje o ryzyka szczątkowych
- deklarację akceptacji ryzyk szczątkowych

Ponadto dokument SWB powinien zawierać:

- opis zastosowanych zabezpieczeń
- informacje o poświadczeniach bezpieczeństwa
- informacje o innych formalnych uprawnieniach do dostępu do IN
- opis bezpieczeństwa fizycznego
- środki ochrony fizycznej
- granice i lokalizacje stref ochronnych
- informacje o zastosowanych urządzeniach i narzędziach kryptograficznych

- opis procesu ciągłości działania
  - tworzenie kopii zapasowej
  - odzyskiwanie systemu
  - zasilanie awaryjne
  - alternatywne łącza i urządzenia
- konfiguracja systemu TI
- konserwacja systemu TI
- przeglądy systemu TI
- serwis systemu
- środki ochrony przed incydentami bezpieczeństwa
- zastosowany antywirus
- wprowadzanie poprawek i uaktualnień w systemie TI
- informacje o ochronie nośników
  - oznaczanie
  - dostęp
  - transport
  - obniżanie klauzuli tajności
  - niszczenie nośników
- opis identyfikacji i uwierzytelnienia użytkowników
- opis identyfikacji i uwierzytelnienia urządzeń
- opis środków kontroli dostępu
- informacje o audycie wewnętrznym
- opis zarządzania ryzykiem
- informacje o zmianach w systemie TI
  - aktualizacja dokumentacji bezpieczeństwa
  - warunki ponownej akredytacji
- informacje o wycofaniu systemu z eksploatacji

Podstawa prawna: § 25 ust. 2 i 3 Rozporządzenia w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego.

4.2. Dokument PBE

Dokument PBE, czyli procedury bezpiecznej eksploatacji, jest opisem sposobu i trybu postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz zakresem odpowiedzialności użytkowników systemu teleinformatycznego i pracowników mających do niego dostęp. Innymi słowy, PBE to zbiór procedur skierowanych do użytkowników oraz administratorów akredytowanego systemu.

Podstawa prawna: art. 2 pkt 8 Ustawy o ochronie informacji niejawnych

4.2.1. Zawartość dokumentu PBE

Dokument PBE powinien zawierać zbiór procedur odnoszących się do następujących zagadnień:

- administrowanie systemem TI
- administrowanie środkami ochrony
- bezpieczeństwo urządzeń

- bezpieczeństwo oprogramowania
- zarządzanie konfiguracją sprzętową
- zarządzanie konfiguracją programową
- zasady serwisowania
- zasady modernizowania
- zasady wycofania elementów systemu
- plany awaryjne
- monitorowanie systemu TI
- audyt systemu TI
- zarządzanie nośnikami
- zarządzanie materiałami kryptograficznymi
- ochrona elektromagnetyczna
- incydenty bezpieczeństwa teleinformatycznego
- szkolenia użytkowników
- wprowadzanie i wyprowadzanie danych

Podstawa prawna: § 26 ust. 2 Rozporządzenia w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego

4.2.2. Przykład procedury z dokumentu PBE

```
Procedura nr 1

Dział: Administrowanie systemem TI

Nazwa procedury: Blokowanie kont użytkowników

Osoby odpowiedzialne: Administrator Systemu

- Konto użytkownika w systemie TI blokuje administrator w następujących przypadkach:
    * na wniosek pełnomocnika do spraw ochrony informacji niejawnych
    * na wniosek kierownika jednostki organizacyjnej
    * na wniosek inspektora bezpieczeństwa TI po zatwierdzeniu przez pełnomocnika
    * na wniosek administratora systemu po zatwierdzeniu przez pełnomocnika
- Wzór wniosku znajduje się w załączniku nr 1 do procedury
- Po otrzymaniu wniosku adm. systemu blokuje konto użytkownika w systemie operacyjnym.
- Po zablokowaniu konta adm. systemu odnotowuje ten fakt w książce działań administratora.

Załącznik nr 1: wzór wniosku

Nr wniosku:
Data:
Imię i nazwisko użytkownika:
Biuro:
Login użytkownika:
Zlecający: Inspektor BTI/administrator systemu/brak
Podpis zlecającego:
Zatwierdzający: Kierownik JO/Pełnomocnik OIN
Podpis zatwierdzającego:
Powód blokady konta: brak poświadczenia/odejście z pracy/zmiana stanowiska pracy/inne:
Potwierdzenie blokady konta, podpis administratora:
Potwierdzenie wpisu do książki działań administratora, podpis administratora:
```

5. 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.

6. Bezpieczeństwo kryptograficzne

ABW w opublikowanej polityce kryptograficznej definiuje jakie algorytmy mogą być używane do szyfrowania danych o poszczególnych stopniach tajności. ABW dzieli algorytmy kryptograficzne na trzy typy:

- Algorytm typu A – niejawny algorytm kryptograficzny konstruowany w Agencji Bezpieczeństwa Wewnętrznego lub pod jej nadzorem, oceniony i dopuszczony do stosowania, którego specyfikacja techniczna i implementacja jest niejawna,
- Algorytm typu A1 – niejawny algorytm kryptograficzny opracowany w wyniku personalizacji przez ABW algorytmu pierwotnego, oceniony i dopuszczony do stosowania. Specyfikacja techniczna parametrów personalizujących algorytm i implementacja jest niejawna,
- Algorytm typu B – algorytm kryptograficzny, oceniony i dopuszczony do stosowania, którego specyfikacja techniczna jest ogólnie dostępna.

Poniżej została przedstawiona część z głównych zasad polityki kryptograficznej zdefiniowanej przez ABW.

- Do ochrony poufności informacji o klauzuli TAJNE lub wyższej stosuje się algorytmy typu A.
- Algorytm kryptograficzny typu A w postaci opisu matematycznego nie jest przekazywany producentom urządzeń przeznaczonych do kryptograficznej ochrony informacji niejawnych.
- Do ochrony poufności informacji o klauzuli POUFNE stosuje się algorytmy typu Al. Algorytm A1 może być zastosowany do ochrony informacji niejawnych o klauzuli tajne wyłącznie w sytuacjach nadzwyczajnych, określonych przez ABW, w których m.in. mogłoby nastąpić skompromitowanie algorytmu typu A.
- Wytworzone przez ABW przed 2008 r. algorytmy typu A1 w związku z postępem technologicznym i rozwojem nauk matematycznych oraz nowoczesnymi metodami obliczeniowymi, z dniem 16 sierpnia 2011 r. nie mogą być wykorzystywane przez producentów nowych urządzeń i narzędzi kryptograficznych służących do ochrony informacji niejawnych. Środki ochrony kryptograficznej zawierające implementację wyżej wymienionego algorytmu A1 zgłoszone do certyfikacji w ABW po 16 sierpnia 2011 r. nie będą poddawane procesom certyfikacji i nie uzyskają certyfikatu ABW dopuszczającego do ochrony informacji niejawnych. Certyfikaty ochrony kryptograficznej wydane przez ABW dla urządzeń kryptograficznych zawierających implementacje algorytmu A1 zachowują ważność tylko do końca okresu, na jaki zostały wydane.
- Implementacje algorytmów typu A i A1 są wgrywane do urządzeń i narzędzi kryptograficznych bezpośrednio w ABW na stanowiskach personalizacyjnych przygotowanych dla danego urządzenia lub narzędzia.
- Algorytmy publiczne - algorytmy typu B są implementowane bezpośrednio przez producenta urządzeń lub narzędzi kryptograficznych.
- W szczególnie uzasadnionych przypadkach algorytmy kryptograficzne A1 mogą być przekazane producentowi urządzeń przeznaczonych do ochrony kryptograficznej informacji niejawnych na warunkach i w oparciu o zasady określone przez ABW (. . .).

Pozostałe zasady polityki kryptograficznej zdefiniowanej przez ABW można znaleźć na oficjalnej stronie internetowej ABW.

7. Wniosek WA-01 o przeprowadzenie audytu bezpieczeństwa systemu teleinformatycznego oraz wydanie świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego

Samo wypełnienie wniosku WA-01 nie powinno stanowić problemu dla jednostki organizacyjnej starającej się o certyfikat dla własnego systemu teleinformatycznego. Co ważne, opisane w niniejszym dokumencie zagadnienia dotyczą jedynie trzech z 19 sekcji (sekcja 15 – bezpieczeństwo teleinformatyczne, sekcja 16 – bezpieczeństwo elektromagnetyczne, sekcja 17 – bezpieczeństwo kryptograficzne). Fakt ten doskonale obrazuje, że pomimo, iż sam wniosek jest dość krótki (6 stron), to w swoim zakresie obejmuje mnóstwo aspektów, które trzeba rozważyć przed jego wypełnieniem.

Oprócz powyższych informacji wniosek obejmuje m.in.:

- dane wnioskodawcy, kierownika jednostki organizacyjnej, pełnomocnika ochrony w jednostce wnioskodawcy, inspektora / inspektorów, administratora / administratorów, NIP, REGON wnioskodawcy
- klauzula informacji niejawnych przetwarzanych w STI
- bezpieczeństwo osobowe
- zarządzanie bezpieczeństwem informacji
- bezpieczeństwo fizyczne

Formularz wniosku dostępny jest na oficjalnej stronie internetowej ABW.

8. Bibliografia

- ABW Bezpieczeństwo teleinformatyczne
- Ochrona-Niejawnych - Co powinna zawierać dokumentacja bezpiczeństwa
- Informacja Niejawna - Ustawa
- Informacja Niejawna - Urządzenia klasy TEMPEST
- Ochrona-Niejawnych - Ochrona elektromagnetyczna
- Polityka Kryptograficzna Agencji Bezpieczeństwa Wewnętrznego