

BIP - Agencja Bezpieczeństwa Wewnętrznego

<https://bip.abw.gov.pl/bip/informacje-niejawne-1/bezpieczenstwo-teleinf/154,BEZPIECZENSTWO-TELEINFORMATYCZNE.html>
2023-10-04, 03:14

Agencja Bezpieczeństwa Wewnętrznego w ramach zadań wynikających z ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742) w zakresie bezpieczeństwa teleinformatycznego prowadzi:

1. Akredytację bezpieczeństwa teleinformatycznego systemów teleinformatycznych.
Kontakt: (22) 58 59 490, email: {mailto(akredytacja.dbti@abw.gov.pl,encode = secure)}
2. Ochronę elektromagnetyczną. Certyfikację środków ochrony elektromagnetycznej.
Kontakt: (22) 58 56 830, email: {mailto(certyfikacja.dbti@abw.gov.pl,encode = secure)}
3. Specjalistyczne szkolenie z zakresu bezpieczeństwa teleinformatycznego dla administratorów oraz inspektorów bezpieczeństwa teleinformatycznego.
Kontakt: (22) 58 58 773, (22) 58 58 732,
email: {mailto(szkolenia.dbti@abw.gov.pl,encode = secure)}

Wprowadzenie

Do ustawowych kompetencji Agencji Bezpieczeństwa Wewnętrznego należy, m.in. realizacja zadań w zakresie bezpieczeństwa systemów teleinformatycznych, przeznaczonych do przetwarzania informacji niejawnych. Zadania Agencji Bezpieczeństwa Wewnętrznego w tym zakresie realizuje Departament Bezpieczeństwa Teleinformatycznego ABW a także wyspecjalizowane zespoły w delegaturach ABW.

Zgodnie z definicjami zawartymi w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228) - zwanej dalej UOIN:

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

Dokumentacją bezpieczeństwa systemu teleinformatycznego - jest dokument szczególnych wymagań bezpieczeństwa (SWB) oraz dokument procedur bezpiecznej eksploatacji (PBE) systemu teleinformatycznego, opracowane zgodnie z zasadami określonymi w UOIN.

I. Organizacja ochrony systemów teleinformatycznych przeznaczonych do przetwarzania krajowych informacji niejawnych

Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne, odpowiada za ich ochronę, w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony.

Kierownik jednostki organizacyjnej wyznacza:

Pełnomocnika do spraw ochrony informacji niejawnych, zwanego „pełnomocnikiem ochrony”, który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych. Do zadań pełnomocnika ochrony należy m.in. zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne oraz zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka. W przypadku stwierdzenia naruszenia w jednostce organizacyjnej przepisów o ochronie informacji niejawnych pełnomocnik ochrony zawiadamia o tym kierownika jednostki organizacyjnej i podejmuje niezwłocznie działania zmierzające do wyjaśnienia okoliczności tego naruszenia oraz ograniczenia jego negatywnych skutków, przy czym w przypadku stwierdzenia naruszenia przepisów o ochronie informacji niejawnych o klauzuli „poufne” lub wyższej pełnomocnik ochrony zawiadamia niezwłocznie również odpowiednio ABW lub SKW;

Inspektora bezpieczeństwa teleinformatycznego - pracownika lub pracowników pionu ochrony, odpowiedzialnych za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji;

Administradora systemu - osobę lub zespół osób, niepełniących funkcji inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnych za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego.

Stanowiska lub funkcję administratora systemu i inspektora bezpieczeństwa teleinformatycznego mogą zajmować lub pełnić osoby posiadające:

1. obywatelstwo polskie, z wyjątkiem pracowników pionu ochrony zatrudnionych u przedsiębiorców;
2. odpowiednie poświadczenie bezpieczeństwa lub upoważnienie, o którym mowa w art. 21 ust. 4 pkt 1 UOIN;
3. zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych;
4. zaświadczenie o odbytym specjalistycznym szkoleniu z zakresu bezpieczeństwa teleinformatycznego prowadzonym przez ABW lub SKW.

Specjalistyczne szkolenie z zakresu bezpieczeństwa teleinformatycznego, wspólne dla administratorów systemów oraz inspektorów bezpieczeństwa teleinformatycznego, prowadzone jest przez funkcjonariuszy Departamentu Bezpieczeństwa Teleinformatycznego ABW w formie online. Udział w szkoleniu jest odpłatny w wysokości 387 złotych (trzysta osiemdziesiąt siedem złotych) z wyłączeniem jednostek organizacyjnych Policji.

Szczegółowe zasady zgłaszania kandydatów na szkolenie oraz wzajemne prawa i obowiązki stron zawieranej w tym zakresie umowy zostały określone w Warunkach szkolenia specjalistycznego, zwanych dalej „Warunkami”, [zamieszczonych na BIP](#) warunków szkolenia - jak w załączeniu.

Kierownik Jednostki Organizacyjnej chcąc skierować osobę na przeszkolenie, dokonuje pisemnego zgłoszenia kandydata, które przesyła na adres: Agencja Bezpieczeństwa Wewnętrznego, Departament Bezpieczeństwa Teleinformatycznego, Warszawa 00-993, ul. Rakowiecka 2a. Wzór zgłoszenia określony został w załączniku do Warunków. Potwierdzenie przydzielenia kandydatowi miejsca na szkoleniu w określonym przez prowadzącego szkolenie terminie dokonywane jest poprzez fax zawarcie jest równoznaczne z zawarciem umowy pomiędzy stronami o której mowa w art. 52 ust. 7 UOIN - o treści zgodnej z postanowieniami Warunków.

Przed dokonaniem zgłoszenia kandydata prosimy przedstawicieli jednostek organizacyjnych o dokładne zapoznanie się z Warunkami szkolenia specjalistycznego, wyznaczających zasady organizowania szkoleń.

Więcej informacji w sprawach powyższych szkoleń można uzyskać pod numerami telefonów: 22 585-87-73, 22 585-87-32 lub email szkolenia.dbti@abw.gov.pl

II. Akredytacja bezpieczeństwa teleinformatycznego systemów teleinformatycznych przeznaczonych do przetwarzania krajowych informacji niejawnych.

Systemy teleinformatyczne, w których mają być przetwarzane krajowe informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego, której udziela się na czas określony, nie dłuższy niż 5 lat.

- A. Systemy teleinformatyczne przeznaczone do przetwarzania krajowych informacji niejawnych o klauzuli „zastrzeżone” 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. Wraz z ww. dokumentacją bezpieczeństwa (SWB i PBE) Kierownik jednostki organizacyjnej przesyła „Oświadczenie dotyczące udzielenia akredytacji bezpieczeństwa teleinformatycznego”, w którym wskazuje termin obowiązywania udzielonej w trybie art. 48 ust. 9 UOIN akredytacji. [wstawić link]. 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.

- B. Systemy teleinformatyczne przeznaczone do przetwarzania krajowych informacji niejawnych o klauzuli „poufne” lub wyższej 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 dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej składa się z następujących etapów:

1. Przesłanie do ABW dokumentacji bezpieczeństwa (SWB i PBE) systemu teleinformatycznego wraz z oświadczeniem dotyczącym określenia, dla pomieszczenia lub obszaru, w którym przetwarzane będą informacje niejawne w systemie teleinformatycznym, poziomu zagrożeń związanych z utratą poufności, integralności i dostępności informacji niejawnych oraz zastosowania adekwatnych do wyznaczonego poziomu zagrożeń środków ochrony. Dokumentacja bezpieczeństwa oraz oświadczenie, o którym mowa powyżej, muszą zostać przed przesłaniem do ABW podpisane przez Kierownika Jednostki Organizacyjnej [wzór oświadczenia znajduje się w plikach do pobrania];
2. Przedsiębiorcy, którzy ubiegają się o udzielenie w trybie art. 48 akredytacji bezpieczeństwa teleinformatycznego przesyłają do ABW wraz z dokumentacją bezpieczeństwa (SWB i PBE) wypełniony „Kwestionariusz dotyczący przeprowadzenia procesu akredytacji bezpieczeństwa systemu teleinformatycznego przeznaczanego do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej” [wzór kwestionariusza znajduje się w plikach do pobrania].

ABW zastrzega sobie możliwość zwrócenia się do każdego podmiotu ubiegającego się o udzielenie akredytacji o wypełnienie i dołączenie do dokumentacji bezpieczeństwa (SWB i PBE) „Kwestionariusza dotyczącego przeprowadzenia procesu akredytacji bezpieczeństwa systemu teleinformatycznego przeznaczanego do przetwarzania informacji niejawnych o klauzuli „POUFNE” lub wyższej w całym cyklu funkcjonowania systemu.

1. Dokonanie przez ABW oceny bezpieczeństwa systemu teleinformatycznego na podstawie przesłanej dokumentacji bezpieczeństwa (SWB i PBE);
2. W przypadku zatwierdzenia przez ABW dokumentacji bezpieczeństwa (SWB i PBE) systemu teleinformatycznego, złożenie do ABW wniosku [WA](#) o przeprowadzenie audytu bezpieczeństwa systemu teleinformatycznego oraz o wydanie świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego;
3. 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:

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

Dokumentacja bezpieczeństwa systemów teleinformatycznych (SWB i PBE), przeznaczonych do przetwarzania krajowych informacji niejawnych oraz wnioski WA powinny być kierowane do właściwych terytorialnie jednostek organizacyjnych Agencji Bezpieczeństwa Wewnętrznego (właściwych delegatur ABW lub Departamentu Bezpieczeństwa Teleinformatycznego ABW dla obszaru m. st. Warszawy).

Za przeprowadzenie czynności związanych z udzielaniem przez ABW albo SKW akredytacji, określonych w art. 48 ust. 3-6 UOIN pobierane są opłaty, z zastrzeżeniem art. 53 ust. 2-3 UOIN. Wysokość opłat uregulowana jest w rozporządzeniu Prezesa Rady Ministrów, wydanym na

podstawie art. 53 ust. 4 UOIN.

III. Akredytacja systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych międzynarodowych.

Szef Agencji Bezpieczeństwa Wewnętrznego pełniący funkcję Krajowej Władzy Bezpieczeństwa realizuje m.in. zadania w zakresie bezpieczeństwa systemów teleinformatycznych, przeznaczonych do przetwarzania informacji niejawnych międzynarodowych. Podstawowe zasady, dotyczące akredytacji systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych międzynarodowych są następujące:

1. Informacje niejawne międzynarodowe mogą być przetwarzane tylko w systemach teleinformatycznych, które posiadają akredytację bezpieczeństwa teleinformatycznego;
2. Akredytacji punktów dostępowych systemów przetwarzających niejawne informacje międzynarodowe, organizowanych przez podmioty międzynarodowe, dokonuje odpowiednio, zgodnie z właściwością rzeczową, Szef ABW lub Szef SKW;
3. Akredytacja systemów organizowanych przez polskie jednostki organizacyjne, w których dopuszczono przetwarzanie informacji niejawnych międzynarodowych, odbywa się z uwzględnieniem postanowień lit. B i wymagań wynikających z umów międzynarodowych.

Zasady akredytacji systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych międzynarodowych, organizowanych przez polskie jednostki organizacyjne są następujące:

1. W przypadku systemów narodowych przeznaczonych do przetwarzania wyłącznie informacji niejawnych międzynarodowych, akredytacji udziela ABW lub SKW po potwierdzeniu wymagań wynikających z regulacji międzynarodowych;
2. W przypadku systemów narodowych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „zastrzeżone”, w których dopuszcza się przetwarzanie informacji niejawnych międzynarodowych, warunkiem udzielenia przez ABW lub SKW akredytacji dopuszczającej do ich przetwarzania, jest wcześniejsze udzielenie przez kierownika jednostki organizującej system akredytacji bezpieczeństwa teleinformatycznego w trybie art. 48 ust. 9 lub 10 UOIN;
3. W ciągu 30 dni od udzielenia akredytacji, o której mowa w pkt 2 kierownik jednostki organizującej system zobowiązany jest przesłać do ABW lub SKW dokumentację bezpieczeństwa systemu teleinformatycznego;
4. W przypadku systemów narodowych, w których dopuszcza się przetwarzanie informacji niejawnych międzynarodowych, dokumentacja, o której mowa w pkt 3, uwzględniająca wymagania wynikające z regulacji międzynarodowych, przesyłana jest razem z pisemnym wnioskiem o udzielenie przez ABW lub SKW akredytacji w zakresie przetwarzania informacji międzynarodowych;
5. Akredytacji systemu, o której mowa w pkt 4 udziela się wyłącznie po potwierdzeniu przez ABW lub SKW spełnienia przez system wymagań wynikających z regulacji międzynarodowych;
6. Potwierdzeniem udzielenia akredytacji, o których mowa w pkt 2 i 5 są:

- a. W odniesieniu do informacji niejawnych narodowych – zatwierdzona (przez kierownika jednostki organizującej system) dokumentacja bezpieczeństwa systemu oraz brak zaleceń lub potwierdzenie usunięcia zaleceń ABW lub SKW (zgodnie z art. 48 ust. 12 UOIN);
 - b. W odniesieniu do informacji niejawnych międzynarodowych – pisemne potwierdzenie udzielenia przez ABW lub SKW akredytacji określające:
 - Zakres akredytacji (akredytowane elementy systemu, klauzule informacji itp.);
 - Datę ważności akredytacji;
 - Warunki utrzymywania ważności akredytacji.
7. W przypadku systemów narodowych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej, w których dopuszcza się przetwarzanie informacji niejawnych międzynarodowych:
- a. Możliwe jest równoległe prowadzenie przez ABW lub SKW procesów akredytacji dla informacji krajowych i międzynarodowych;
 - b. Akredytacji systemu dla informacji międzynarodowych udziela się wyłącznie po potwierdzeniu przez ABW lub SKW spełnienia przez system wymagań wynikających z regulacji międzynarodowych;
 - c. Potwierdzeniem udzielenia akredytacji dla informacji krajowych jest świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego, o którym mowa w art. 48 ust. 5 UOIN;
 - d. Potwierdzeniem udzielenia akredytacji dla informacji międzynarodowych jest pisemne potwierdzenie udzielenia akredytacji przez ABW lub SKW określające:
 - Zakres akredytacji (akredytowane elementy systemu, klauzule informacji itp.);
 - Datę ważności akredytacji;
 - Warunki utrzymywania ważności akredytacji.

IV. Ochrona Elektromagnetyczna

Mając na uwadze bezpieczeństwo systemów teleinformatycznych, przeznaczonych do ochrony informacji niejawnych wymagane jest stosowanie odpowiednich środków ochrony elektromagnetycznej.

Dla każdego pomieszczenia lub obiektu, w którym będą przetwarzane informacje niejawne:

krajowe, oznaczone klauzulą POUFNE lub wyższą,
międzynarodowe w szczególności NATO lub UE, oznaczone klauzulą CONFIDENTIAL lub wyższą

Należy wyznaczyć Sprzętową Strefę Ochrony Elektromagnetycznej (SSOE). W celu wyznaczenia SSOE należy złożyć odpowiedni wniosek (WS-01) do Departamentu Bezpieczeństwa Teleinformatycznego ABW. SSOE może zostać wyznaczona w oparciu o analizę przesłanej dokumentacji lub na podstawie specjalistycznych pomiarów sprzętowych w miejscu

wnioskowanego pomieszczenia.

Na podstawie wyznaczonej SSOE w pomieszczeniu lub obiekcie wymagane jest stosowanie odpowiedniej kategorii sprzętu teleinformatycznego w zależności od klauzuli przetwarzanych informacji niejawnych.

Szczegółowe informacje zostały zawarte w Zaleceniach Departamentu Bezpieczeństwa Teleinformatycznego ABW dotyczące ochrony elektromagnetycznej (wersja 5.0 z 2016r.).

V. Certyfikacja środków ochrony elektromagnetycznej, urządzenia lub narzędzia służącego do realizacji zabezpieczenia teleinformatycznego oraz urządzeń i narzędzi kryptograficznych przeznaczonego do ochrony informacji niejawnych.

Certyfikacje prowadzone są przez ABW lub SKW z pominięciem właściwości podmiotowej, o której mowa w art. 10 ust. 2 i 3 ustawy o ochronie informacji niejawnych. Zasady przeprowadzania certyfikacji w ABW będą podlegały wewnętrznym regulacjom, których celem będzie zapewnienie przejrzystości i jednolitości stosowanych procedur.

Dla realizacji uprawnień Szefa ABW, wynikających z art. 50 ust. 6 ustawy o ochronie informacji niejawnych („Szef ABW... może zlecić podmiotowi zewnętrznemu badanie urządzenia lub narzędzia..., na zasadach, warunkach i w zakresie przez siebie określonym.”) w zakresie dotyczącym badań środków ochrony elektromagnetycznej zawierane będą umowy z podmiotami, spełniającymi warunki do przeprowadzania badań ochrony elektromagnetycznej. Aby podmiot mógł znaleźć się na liście laboratoriów spełniających warunki do przeprowadzania takich badań powinien między innymi:

- a. spełniać wymagania w zakresie wyposażenia w sprzęt badawczy oraz posiadania odpowiedniego personelu badawczego, które będą weryfikowane przez funkcjonariuszy ABW;
- b. podpisać z ABW umowę o wykonywaniu zleconych przez Szefa ABW badań;
- c. użyczyć ABW narzędzia pomiarowe, umożliwiające weryfikację badań przeprowadzanych przez podmiot.

Szczegółowe wymagania, jakie będą stawiane laboratorium, które będą chciały znaleźć się na liście, o której mowa powyżej, zostaną określone w wytycznych dyrektora Departamentu Bezpieczeństwa Teleinformatycznego. Wytyczne będą udostępniane zainteresowanym podmiotom przez Laboratorium Ochrony Elektromagnetycznej Departamentu Bezpieczeństwa Teleinformatycznego.

Szef Agencji Bezpieczeństwa Wewnętrznego wydał Zarządzenie Nr 57 regulujące temat badań środków ochrony elektromagnetycznej podmiotom zewnętrznym. Podmioty chcące wcześniej przeprowadzić badania, niż będzie to wynikało z przyznanej kolejności, mogą zwracać się do Szefa ABW z wnioskiem o wykonanie badań w trybie, o którym mowa w art. 50 ust. 6 ustawy, zobowiązując się jednocześnie do pokrycia kosztów badań przeprowadzonych w laboratorium zewnętrznym. W takim przypadku Szef ABW będzie zlecał przeprowadzenie badań laboratorium, znajdującemu się na liście laboratoriów spełniających warunki do ich przeprowadzania.

Przeprowadzanie certyfikacji będzie odbywało się po przesłaniu odpowiedniego z niżej wymienionych wniosków, związanych z certyfikacją środka ochrony, urządzenia lub narzędzia.

Wnioski [WS-01](#), [WE-01](#), [WUN-01](#), [WK-01](#), [WB-01](#) należy kierować na adres:

Dyrektor Departamentu Bezpieczeństwa Teleinformatycznego ABW

ul. Rakowiecka 2A

00-993 Warszawa.

Pliki do pobrania

[Zarządzenie nr 35 Szefa ABW pdf, 275.94 KB](#)

[Kwestionariusz rozpoczęcia akredytacji docx, 41.12 KB](#)

[Oświadczenie o udzieleniu akredytacji docx, 18.41 KB](#)

[Oświadczenie o doborze środków bezpieczeństwa fizycznego docx, 17.62 KB](#)

[Wniosek WA-01 docx, 80.96 KB](#)

[Wniosek WE - 01 docx, 29.5 KB](#)

[Wniosek WE - 01- K docx, 28.66 KB](#)

[Wniosek WK-01-T doc, 109 KB](#)

[wniosek WK-01-Z doc, 84 KB](#)

[Wniosek WS-01 docx, 39.11 KB](#)

[Wniosek WUN - 01 doc, 69 KB](#)

[Wniosek WB - 01 doc, 60.5 KB](#)

[Warunki szkolenia specjalistycznego z zakresu bezpieczeństwa teleinformatycznego docx, 21.34 KB](#)

[Polityka kryptograficzna pdf, 235.15 KB](#)

[Wykaz certyfikatów ochrony kryptograficznej wydanych przez ABW pdf, 109.53 KB](#)

[Zarządzenie Nr 57 pdf, 245.25 KB](#)

[Wytyczne ABW w sprawie wykonywania zadań administratora systemu lub inspektora bezpieczeństwa teleinformatycznego w więcej niż jednej jednostce organizacyjnej pdf, 344.44 KB](#)

Metadane

Data publikacji : 27.12.2010

Data modyfikacji : 29.09.2023

[Rejestr zmian](#)

Podmiot udostępniający informację:
Agencja Bezpieczeństwa Wewnętrznego

Osoba wytwarzająca/odpowiadająca za informację:
Administrator BIP

Osoba udostępniająca informację:
Administrator BIP

Osoba modyfikująca informację:
Administrator BIP
