# Obowiązujące akty normatywne

**USTAWA z dnia 05.08.2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 nr 182 poz. 1228, t.j. Dz. U. 2023 r. poz. 756) (**[**http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20101821228**](http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20101821228)**)**

* **Akty normatywne wydane przez Prezesa Rady Ministrów:**

ROZPORZĄDZENIE  PREZESA RADY MINISTRÓW  z dnia 20  lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. 159, poz. 948) (<http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20111590948>)

ROZPORZĄDZENIE  PREZESA  RADY  MINISTRÓW  z dnia 20 lipca 2011 r. w sprawie wzoru świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego  (Dz. U. 156, poz. 926) (<http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20111560926>)

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW  z dnia 4 października 2011 r. w sprawie współdziałania Szefa  Agencji Bezpieczeństwa Wewnętrznego i Szefa Służby Kontrwywiadu Wojskowego  w zakresie wykonywania funkcjonowania funkcji krajowej władzy bezpieczeństwa  (Dz. U. 22, poz. 1302) (<http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20112201302>)

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW  z dnia 09 lipca 2020 r.  w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez ABW lub SKW  (Dz. U. 2020, poz. 1256) (<https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20200001256>)

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne  (Dz. U. 2011 nr 271, poz. 1603) (<http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20112711603>)

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW  z dnia 9 lipca 2020 r. w sprawie opłat za przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego czynności z zakresu  bezpieczeństwa teleinformatycznego  (Dz. U. 2020 poz.1236) (<http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20200001236>)

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. 2011 nr 288, poz. 1692) (<http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20112881692>)

ROZPORZĄDZENIE RADY MINISTRÓW z dnia 7 grudnia 2011 r.  w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. 2011 nr 276, poz. 1631, tj. Dz. U. 2017 poz. 1558)  (<http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20170001558>)

ROZPORZĄDZENIE  RADY MINISTRÓW  z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania  informacji niejawnych (Dz. U. 2012, poz. 683) (<http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20120000683>)

* **Akty normatywne wydane przez Ministra Obrony Narodowej:**

ROZPORZĄDZENIE MINISTRA OBRONY NARODOWEJ z dnia 19 grudnia 2013 r.  w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w  jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych  (Dz. U. 2013, poz. 1660) (<http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20130001660>)

ROZPORZĄDZENIE MINISTRA OBRONY NARODOWEJ z dnia 4 lutego 2015  r. zmieniające rozporządzenie w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w  jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych  (Dz. U. 2015, poz. 236) (<http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20150000236>)

ROZPORZĄDZENIE MINISTRA OBRONY NARODOWEJ z dnia 25 listopada 2020  r. zmieniające rozporządzenie w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w  jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych  (Dz. U. 2020, poz. 2101) ([https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20200002101)](https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20200002101)

OBWIESZCZENIE MINISTRA OBRONY NARODOWEJ z dnia 14 stycznia 2022 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Ministra Obrony Narodowej w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych (DZ. U. z 9 lutego 2022 r., poz. 322) (<https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20220000322>)

ROZPORZĄDZENIE MINISTRA OBRONY NARODOWEJ z dnia 29 września 2022 r. w sprawie trybu oceny i sposobu dopuszczania rozwiązań informatycznych, w których mają być przetwarzane informacje niejawne (Dz. U. 14 października  2022, poz. 2098) (<https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20220002098>)

ZARZĄDZENIE Nr 46/MON MINISTRA OBRONY NARODOWEJ  z dnia 24 grudnia 2013 r. w sprawie szczególnego sposobu organizacji  i funkcjonowania kancelarii kryptograficznych (Dz. Urz. z 30 grudnia 2013 r. poz. 401) (<http://www.dz.urz.mon.gov.pl/dziennik/pozycja/zarzadzenie-401-zarzadzenie-nr-46mon-z-dnia-24-grudnia-2013-r-w-sprawie-szczegolnego-sposobu-organizacji-i-funkcjonowania-kancelarii-kryptograficznych/>)

ZARZĄDZENIE Nr 24/MON MINISTRA OBRONY NARODOWEJ z dnia 28 grudnia 2020 r. zmieniające zarządzenie w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii kryptograficznych (Dz. Urz. z 29 grudnia 2020 r. poz. 210) (<https://www.dz.urz.mon.gov.pl/dziennik/pozycja/zarzadzenie-210-zarzadzenie-nr-24mon-z-dnia-28-grudnia-2020-r-zmieniajace-zarzadzenie-w-sprawie-szczegolnego-sposobu-organizacji-i-funkcjonowania-kanc/>)

ZARZĄDZENIE Nr 58/MON MINISTRA OBRONY NARODOWEJ  z dnia 11 grudnia 2017 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych,  sposobu i trybu przetwarzania informacji niejawnych  (Dz. Urz. z 12 grudnia 2017 r. poz. 226) (<http://www.dz.urz.mon.gov.pl/dziennik/pozycja/zarzadzenie-226-zarzadzenie-nr-58mon-z-dnia-11-grudnia-2017-r-w-sprawie-szczegolnego-sposobu-organizacji-i-funkcjonowania-kancelarii-tajnych-oraz-inny/>)

ZARZĄDZENIE Nr 24/MON MINISTRA OBRONY NARODOWEJ z dnia 17 lipca 2019 r. zmieniające zarządzenie w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych, sposobu i trybu przetwarzania informacji niejawnych (Dz. Urz. z 19 lipca 2019 r. poz. 137) (<https://www.dz.urz.mon.gov.pl/dziennik/pozycja/zarzadzenie-137-zarzadzenie-nr-24mon-z-dnia-17-lipca-2019-r-zmieniajace-zarzadzenie-w-sprawie-szczegolnego-sposobu-organizacji-i-funkcjonowania-kancel/>)

ZARZĄDZENIE Nr 59/MON MINISTRA OBRONY NARODOWEJ  z dnia 11 grudnia 2017 r. w sprawie doboru i stosowania środków bezpieczeństwa fizycznego do ochrony informacji niejawnych (Dz. Urz. z 12 grudnia 2017 r. poz. 227) (<http://www.dz.urz.mon.gov.pl/dziennik/pozycja/zarzadzenie-227-zarzadzenie-nr-59mon-z-dnia-11-grudnia-2017-r-w-sprawie-doboru-i-stosowania-srodkow-bezpieczenstwa-fizycznego-do-ochrony-informacji-ni/>)

ZARZĄDZENIE Nr 25/MON MINISTRA OBRONY NARODOWEJ z dnia 17 lipca 2019 r. zmieniające zarządzenie w sprawie doboru i stosowania środków bezpieczeństwa fizycznego do ochrony informacji niejawnych (Dz. Urz. z 19 lipca 2019 r. poz. 138) (<http://www.dz.urz.mon.gov.pl/dziennik/pozycja/zarzadzenie-138-zarzadzenie-nr-25mon-z-dnia-17-lipca-2019-r-zmieniajace-zarzadzenie-w-sprawie-doboru-i-stosowania-srodkow-bezpieczenstwa-fizycznego-do/>)

ZARZĄDZENIE Nr 14/MON MINISTRA OBRONY NARODOWEJ z dnia 9 czerwca 2020 r. zmieniające zarządzenie w sprawie doboru i stosowania środków bezpieczeństwa fizycznego do ochrony informacji niejawnych (Dz. Urz. z 10 czerwca 2020 r. poz. 95) (<http://www.dz.urz.mon.gov.pl/dziennik/pozycja/zarzadzenie-95-zarzadzenie-nr-14mon-z-dnia-9-czerwca-2020-r-zmieniajace-zarzadzenie-w-sprawie-doboru-i-stosowania-srodkow-bezpieczenstwa-fizycznego-do/>)

ZARZĄDZENIE Nr 4/MON MINISTRA OBRONY NARODOWEJ z dnia 19 lutego 2021 r. zmieniające zarządzenie w sprawie doboru i stosowania środków bezpieczeństwa fizycznego do ochrony informacji niejawnych (Dz. Urz. z 22 lutego 2021 r. poz. 22) (<https://www.dz.urz.mon.gov.pl/dziennik/pozycja/zarzadzenie-22-zarzadzenie-nr-4mon-z-dnia-19-lutego-2021-r-zmieniajace-zarzadzenie-w-sprawie-doboru-i-stosowania-srodkow-bezpieczenstwa-fizycznego-do/>)

ZARZĄDZENIE Nr 10/MON MINISTRA OBRONY NARODOWEJ z dnia 6 lipca 2022 r. zmieniające zarządzenie w sprawie doboru i stosowania środków bezpieczeństwa fizycznego do ochrony informacji niejawnych (Dz. Urz. z 7 lipca 2022 r. poz. 111) (<https://www.dz.urz.mon.gov.pl/dziennik/pozycja/zarzadzenie-111-zarzadzenie-nr-10mon-z-dnia-6-lipca-2022-r-zmieniajace-zarzadzenie-w-sprawie-doboru-i-stosowania-srodkow-bezpieczenstwa-fizycznego-do/>)

DECYZJA Nr  7/MON  MINISTRA OBRONY NARODOWEJ  z dnia 20 stycznia 2012 r. w sprawie organizacji  ochrony systemów  teleinformatycznych  przeznaczonych do przetwarzania informacji niejawnych w resorcie obrony narodowej  (Dz. Urz. z 9 lutego 2012 r. poz. 8) (<http://www.dz.urz.mon.gov.pl/dziennik/pozycja/decyzja-8-decyzja-nr-7mon-z-dnia-20-stycznia-2012-r-w-sprawie-organizacji-ochrony-systemow-teleinformatycznych-przeznaczonych-do-przetwarzania-informa/>)

DECYZJA Nr 77/MON MINISTRA OBRONY NARODOWEJ z dnia 09 czerwca 2020 r. w sprawie zasad używania urządzeń do przetwarzania obrazu i dźwięku oraz organizacji ochrony informacji niejawnych podczas przedsięwzięć realizowanych w komórkach i jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych (Dz. Urz. Z 10 czerwca 2020 r. poz. 94) (<http://www.dz.urz.mon.gov.pl/dziennik/pozycja/decyzja-94-decyzja-nr-77mon-z-dnia-9-czerwca-2020-r-w-sprawie-zasad-uzywania-urzadzen-do-przetwarzania-obrazu-i-dzwieku-oraz-organizacji-ochrony-infor/>)

DECYZJA Nr 345/MON MINISTRA OBRONY NARODOWEJ z dnia 27 sierpnia 2015 r. w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz w komórkach organizacyjnych Ministerstwa Obrony Narodowej (Dz. Urz. z 27 sierpnia 2015 r., poz. 252) (<http://www.dz.urz.mon.gov.pl/dziennik/pozycja/decyzja-252-decyzja-nr-345mon-z-dnia-27-sierpnia-2015-r-w-sprawie-sprawowania-nadzoru-nad-ochrona-informacji-niejawnych-w-jednostkach-organizacyjnych-/>)

DECYZJA NR 160/MON MINISTRA OBRONY NARODOWEJ z dnia 2 października 2019 r. zmieniająca decyzję w sprawie nadzoru nad ochroną informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz organizacyjnych Ministerstwa Obrony Narodowej (Dz. Urz. z 03 października 2019 r., poz. 196) (<http://www.dz.urz.mon.gov.pl/dziennik/pozycja/decyzja-196-decyzja-nr-160mon-z-dnia-2-pazdziernika-2019-r-zmieniajaca-decyzje-w-sprawie-sprawowania-nadzoru-nad-ochrona-informacji-niejawnych-w-jedno/>)

DECYZJA Nr 158/MON MINISTRA OBRONY NARODOWEJ z dnia 19 listopada 2020 r. zmieniająca decyzję w sprawie nadzoru nad ochroną informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz komórkach organizacyjnych Ministerstwa Obrony Narodowej (Dz. Urz. z 19 listopada 2020 r., poz. 184) (https://www.dz.urz.mon.gov.pl/dziennik/pozycja/decyzja-184-decyzja-nr-158mon-z-dnia-19-listopada-2020-r-zmieniajaca-decyzje-w-sprawie-sprawowania-nadzoru-nad-ochrona-informacji-niejawnych-w-jednost/)

DECYZJA Nr 62/DK WOC MINISTRA OBRONY NARODOWEJ z dnia 14 marca 2023 r.  w sprawie organizacji i funkcjonowania systemu cyberbezpieczeństwa w resorcie obrony narodowej (decyzja niepublikowana)

DECYZJA NR 37/MON Ministra Obrony Narodowej z dnia 6 lutego 2015 r. w sprawie dokumentacji szkolenia w zakresie ochrony informacji niejawnych w resorcie obrony narodowej (Dz. Urz. z 10 lutego 2015 r., poz. 35) (<http://www.dz.urz.mon.gov.pl/dziennik/pozycja/decyzja-35-decyzja-nr-37mon-z-dnia-6-lutego-2015-r-w-sprawie-dokumentacji-szkolenia-w-zakresie-informacji-niajawnych-w-resorcie-obrony-narodowej/>)

DECYZJA Nr 107/MON MINISTRA OBRONY NARODOWEJ z dnia 18.08.2021 r. w sprawie organizowania współpracy międzynarodowej w resorcie obrony narodowej  (Dz. Urz. 2021 r., poz. 177) (https://www.dz.urz.mon.gov.pl/dziennik/pozycja/decyzja-177-decyzja-nr-107mon-z-dnia-18-sierpnia-2021-r-w-sprawie-organizowania-wspolpracy-miedzynarodowej-w-resorcie-obrony-narodowej/)

DECYZJA Nr 56/SG MINISTRA OBRONY NARODOWEJ z dnia 17 grudnia 2021 r. w sprawie wprowadzenia do użytku „Instrukcji o gospodarowaniu sprzętem informatyki i oprogramowaniem w resorcie obrony narodowej”. DU-4.22.3.1 (B)

WYMAGANIA bezpieczeństwa dla SI ETAT; wersja dokumentu 2.1 LAN i ASK

* **Zalecenia wydane przez Służbę Kontrwywiadu Wojskowego:**

ZALECENIA SKW w zakresie bezpieczeństwa teleinformatycznego dotyczące podstawowych wymagań dla systemów teleinformatycznych przetwarzających informacje niejawne ZBT-105 (z dnia 20.03.2023 r.)

ZALECENIA SKW w zakresie bezpieczeństwa autonomicznych stacji roboczych oraz sieci lokalnych przetwarzających informacje niejawne DBBT-803

ZALECENIA SKW w zakresie zarządzania bezpieczeństwem systemów teleinformatycznych DBBT-811.1 Organizacja zarządzania bezpieczeństwem teleinformatycznym. Wprowadzenie i podstawy teoretyczne

ZALECENIA SKW w zakresie zarządzania bezpieczeństwem systemów teleinformatycznych DBBT-811.2 Metodologia szacowania ryzyka dla systemów teleinformatycznych przetwarzających informacje niejawne

ZALECENIA SKW w zakresie zarządzania bezpieczeństwem systemów teleinformatycznych DBBT-811.3 Przykład dokumentacji wstępnego szacowania ryzyka prowadzonego zgodnie z zalecaną metodologią dla typowego systemu teleinformatycznego przetwarzającego informacje niejawne

ZALECENIA SKW w zakresie zawartości dokumentacji bezpieczeństwa systemów teleinformatycznych przetwarzających informacje niejawne. Szczególne wymagania bezpieczeństwa ZIBT-818A

ZALECENIA SKW w zakresie zawartości dokumentacji bezpieczeństwa systemów teleinformatycznych przetwarzających informacje niejawne. Procedury bezpiecznej eksploatacji ZIBT-818B

ZALECENIA SKW w zakresie sanityzacji informatycznych nośników danych ZIBT-810

ZALECENIA SKW w zakresie ustawień zabezpieczeń systemu operacyjnego Windows 10 w systemach przetwarzających informacje niejawne ZIBT-142

ZALECENIA ogólne SKW w zakresie zapewniania ochrony elektromagnetycznej systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych ZOBT-500A

ZALECENIA SKW w zakresie ustawień zabezpieczeń w środowisku domenowym opartym o system operacyjny Windows Server 2016 w systemach przetwarzających informacje niejawne ZBT-101

ZALECENIA SKW w zakresie urządzeń i narzędzi kryptograficznych przeznaczonych do ochrony informacji niejawnych ZBT-401

ZALECENIA SKW w zakresie bezpieczeństwa teleinformatycznego dotyczące certyfikacji urządzeń, narzędzi oraz środków do ochrony informacji niejawnych ZBT-402

ZALECENIA SKW w zakresie bezpieczeństwa teleinformatycznego dotyczące zarządzania materiałami kryptograficznymi ZBT-601A

ZALECENIA SKW w zakresie powoływania i odwoływania kancelarii kryptograficznej ZBT-602A

ZALECENIA SKW w zakresie stosowania przełączników KVM DBBT-830A

ZALECENIA SKW w zakresie certyfikacji urządzeń i narzędzi kryptograficznych będących rozwiązaniem sprzętowym (elektronicznym), programowym lub sprzętowo-programowym oraz urządzeń służących do składania i weryfikacji podpisu elektronicznego DBBT-901A

Uwaga! Zalecenia SKW dystrybuowane są za pośrednictwem Departamentu Ochrony Informacji Niejawnych MON.

* **Akty normatywne międzynarodowe:**

UMOWA między Stronami Traktatu Północnoatlantyckiego o ochronie informacji sporządzona w Brukseli dnia 6 marca 1997 r. (Dz. U. z 2000 r. Nr 64, poz. 740)

Security within NATO CM(2002)49 wraz z dyrektywami pomocniczymi

DECYZJA Rady z dnia 23 września 2013 r. (2013/488/UE) w sprawie przyjęcia przepisów Rady dotyczących bezpieczeństwa wraz z dokumentami wykonawczymi

UMOWY bilateralne zawierane przez Rząd RP z innymi krajami o wzajemnej ochronie informacji niejawnych

* **Materiały pomocnicze:**

Aktualne akty normatywne (w tym Zalecenia SKW) do pobrania w systemie teleinformatycznym MILNET-Z (http://witryna.ron.int/?doin&strona=dokumenty)

Informacje SKW odnośnie akredytacji, certyfikacji (<http://www.bip.skw.gov.pl/skw/bezpieczenstwo-teleinfo/5107,Bezpieczenstwo-teleinformatyczne.html>)

Aktualny raport o stanie bezpieczeństwa cyberprzestrzeni RP (<https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi>)

Strategia cyberbezpieczeństwa RP na lata 2019-2024 (<https://www.dziennikustaw.gov.pl/MP/rok/2019/pozycja/1037>)

Katalog wykorzystywanego sprzętu teleinformatycznego w NATO ([www.ia.nato.int/niapc](http://www.ia.nato.int/niapc))

Kodeks karny – rozdział XXXIII (Dz. U. z dnia 2 sierpnia 1997 r.) (<http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19970880553>)

* **Dodatkowe informacje:**

   Podstawowym aktem normatywnym regulującym zagadnienia związane z ochroną informacji niejawnych, także w systemach teleinformatycznych jest Ustawa z dnia 05.08.2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 nr 182 poz. 1228, t.j. Dz. U. 2023 r. poz. 756) zwana dalej Ustawą. Jest to podstawowy dokument normatywny, do którego nawiązują inne akty prawne, wydawane na różnych szczeblach, takie jak np.: Rozporządzenia Prezesa Rady Ministrów, Monitor Polski, Zarządzenia Ministra Obrony Narodowej, Decyzje Ministra Obrony Narodowej, Zalecenia SKW, wymagania, instrukcje i inne. Rozdz. 8 Ustawy przedstawia szczegółowo zagadnienia związane z bezpieczeństwem teleinformatycznym. Wskazany rozdział stanowi podstawowe źródło informacji niezbędnych do zrozumienia treści przekazywanych podczas przedmiotowego szkolenia specjalistycznego.

   Należy zwrócić uwagę na konieczność posługiwania się aktualną wersją Ustawy. Najnowszy tekst Ustawy o ochronie informacji niejawnych (jak też innych aktów normatywnych) można pobrać ze strony <http://isap.sejm.gov.pl/>. Podczas zapoznawania się z dokumentami normatywnymi zamieszczonymi na ww. stronie internetowej, w prawym górnym rogu pierwszej strony dokumentu znajduje się bieżący zapis Ustawy.

   Sejmowa strona <http://isap.sejm.gov.pl/>pozwala sprawdzić aktualny status aktu normatywnego w tym, czy akt jest aktualny, czy został uchylony, czy posiada poprawki, czy posiada tekst ujednolicony. Przedstawiona strona pozwala pobrać akt normatywny w formacie pliku .pdf. Istotnym jest powoływanie się na właściwy zapis Ustawy o ochronie informacji niejawnych wraz z wymienieniem aktualnych pozycji Dzienników Ustaw, które pojawiają się przy okazji zmian w przepisach. Obecny zapis Ustawy wygląda następująco:

- Ustawa z dnia 05.08.2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 nr 182 poz. 1228, t.j. Dz. U. 2023 r. poz. 756).

   W przypadku zmian do Ustawy, zamiast wypisywać kolejne pozycje Dz. U., właściwszym byłoby podanie pozycji Dziennika Ustaw tekstu ujednoliconego (obecnie poz. 756) i dopisać zwrot: „z późn. zm.” Taki zapis zwolni z konieczności wypisywania wszystkich zmian do ustawy i uchroni przed dokonywaniem korekt w dokumentacji bezpieczeństwa, za każdym razem, gdy zapis Ustawy ulegnie zmianie.

   Przy opracowaniu dokumentacji bezpieczeństwa należy zwrócić szczególną uwagę na Decyzję Ministra Obrony Narodowej z dnia 14 marca 2023 r. w sprawie organizacji i funkcjonowania systemu cyberbezpieczeństwa w resorcie obrony narodowej, która określa procedurę reagowania na incydenty teleinformatyczne w systemach. W decyzji określa się zasady uzgadniania dokumentacji bezpieczeństwa dotyczących systemów rozległych z DKWOC poprzez Szefa CSIRT MON, w zakresie doboru środków do rejestracji i analizy zdarzeń oraz zapewnienia właściwego poziomu odporności systemu na zagrożenia pochodzące z cyberprzestrzeni.

  DECYZJA Nr 56/SG MINISTRA OBRONY NARODOWEJ z dnia 17 grudnia 2021 r. w sprawie wprowadzenia do użytku „Instrukcji o gospodarowaniu sprzętem informatyki i oprogramowaniem w resorcie obrony narodowej”. DU-4.22.3.1 (B) m.in. normuje gospodarkę informatycznych nośników danych (IND) i opisuje postępowanie w przypadku ich wycofania lub przekazania poza jednostkę organizacyjną. Wycofane IND powinny trafić do właściwych terytorialnie Regionalnych Baz Logistycznych lub Brygad Logistycznych. Do przedmiotowej Decyzji nawiązują Zalecenia SKW – ZIBT-810.

   W przypadku potrzeby posługiwania się oprogramowaniem SI ETAT należy skorzystać z Wymagań bezpieczeństwa dla SI ETAT; wersja dokumentu 2.1 LAN i ASK z 12 maja 2021 r. dotyczących przedmiotowego oprogramowania. Wymagania zostały wykonane z uwzględnieniem zapisów ZIBT-142.

   Należy zauważyć, że zgodnie z porozumieniem Szefa SKW z Dyrektorem Departamentu Ochrony Informacji Niejawnych, wszystkie Zalecenia SKW są przekazywane do DOIN i przez DOIN dystrybuowane do podległych lub nadzorowanych Ministrowi Obrony Narodowej jednostek organizacyjnych. W przypadku konieczności pozyskania Zaleceń SKW należy wnioskować do Dyrektora DOIN o udostępnienie konkretnych dokumentów.

   Zgodnie z uprawnieniami nadanymi przez ustawodawcę w art. 52 ust. 3 Ustawy o ochronie informacji niejawnych, SKW ma prawo doprecyzować zapisy Ustawy o oin. Zgodnie ze swoją kompetencją SKW wydaje zalecenia w zakresie bezpieczeństwa teleinformatycznego, m.in. następujące:

   ZIBT-142 – dotyczy implementacji zabezpieczeń dla sytemu operacyjnego Windows 10, który jest rekomendowany do wykorzystania przy tworzeniu nowych systemów teleinformatycznych, ze względu na wsparcie producenta oprogramowania.

   ZOBT-500A – Zalecenia normujące bezpieczeństwo elektromagnetyczne systemów. Przedstawiają zasady doboru sprzętu (specjalnego klasy TEMPEST lub komercyjnego), zasady określania poziomów zabezpieczenia miejsc (PZM), klasy sprzętu (TPZU), itp.

   ZIBT-810 koresponduje z Instrukcją o gospodarowaniu sprzętem informatyki i oprogramowaniem w resorcie obrony narodowej. DU-4.22.3.1 (B) i odnosi się do postępowania z informatycznymi nośnikami danych (IND), w celu zapewnienia całkowitej sanityzacji danych (oczyszczenia dysków z pamięci) przed przekazaniem lub zniszczeniem IND.

   DBBT-811.1, DBBT-811.2, DBBT-811.3 – które normują postępowanie z ryzykiem w systemach teleinformatycznych.

   Zalecenia SKW w zakresie kryptografii przedstawiają m.in. Zalecenia DBBT-901 A, ZBT-401, ZBT-402, DBBT-830 A, ZBT-601, ZBT-602A,

   ZBT-105 i DBBT-803 przedstawiają podstawowe zasady budowy systemu teleinformatycznego, takie jak np. zasady tworzenia kont osób funkcyjnych i użytkowników, tworzenia haseł, role w systemie, tryby pracy itp.

   ZIBT-818 A i ZIBT-818 B normują układ dokumentacji bezpieczeństwa. Pierwszy dokument przedstawia wymogi, jakie są stawiane przed SWB, drugi dokument natomiast dotyczy PBE.

    Zalecenia ZBT-101 uzupełniają zalecenia DBBT-801B i dotyczą bezpieczeństwa w Windows Server 2016.

# Systemy teleinformatyczne przetwarzające informacje niejawne

* **PODSTAWOWE DEFINICJE WYNIKAJĄCE ROZDZ. 1 ART. 2 PAR. 7-12 USTAWY Z DNIA 05.08.2010 r. O OCHRONIE INFORMACJI NIEJAWNYCH (Dz. U. z 2010 nr 182 poz. 1228, t.j. Dz. U. 2023 r. poz. 756)**

- dokumentem szczególnych wymagań bezpieczeństwa (w skrócie SWB) - jest systematyczny opis sposobu zarządzania bezpieczeństwem systemu teleinformatycznego;  
  
- dokumentem procedur bezpiecznej eksploatacji systemu teleinformatycznego (w skrócie PBE) - jest opis sposobu i trybu postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych przetwarzających w systemie teleinformatycznym oraz zakres odpowiedzialności użytkowników systemu teleinformatycznego i pracowników mających do niego dostęp;  
  
- dokumentacją bezpieczeństwa systemu teleinformatycznego - jest dokument szczególnych wymagań bezpieczeństwa oraz dokument procedur bezpieczeństwa eksploatacji systemu teleinformatycznego, opracowane zgodnie z zasadami określonymi w ustawie;  
  
- akredytacja bezpieczeństwa teleinformatycznego – dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych;

- certyfikacja – proces potwierdzenia zdolności urządzenia, narzędzia lub innego środka do ochrony informacji niejawnych;

- audyt bezpieczeństwa systemu teleinformatycznego – weryfikacja poprawności realizacji wymagań i procedur, określonych w dokumentacji bezpieczeństwa systemu teleinformatycznego;

   W art. 2 Ustawy o ochronie informacji niejawnych opisano definicję dokumentacji bezpieczeństwa  systemu teleinformatycznego (§ 9) oraz składowych dokumentacji bezpieczeństwa:

- Szczególnych Wymagań Bezpieczeństwa (w skrócie SWB);

- Procedur Bezpiecznej Eksploatacji (w skrócie PBE).

   Do stworzenia kompletnej dokumentacji bezpieczeństwa niejawnego systemu teleinformatycznego wymagane jest opracowanie również dokumentacji szacowania ryzyka dla systemu.

   Zwraca się uwagę na fakt, że SWB tworzone jest dla personelu bezpieczeństwa (administratorów, pełnomocnika ds. ochrony informacji niejawnych, inspektora bezpieczeństwa teleinformatycznego, kierownika jednostki organizacyjnej itp.), natomiast PBE przeznaczone jest zarówno dla personelu bezpieczeństwa jak i użytkowników. Zapoznanie użytkowników z SWB skutkowałoby złamaniem zasady „wiedzy niezbędnej”. Rolą administratora systemu teleinformatycznego jest m.in. zapoznawanie użytkowników z PBE, a także aneksami do PBE. Rolą inspektora bezpieczeństwa teleinformatycznego jest natomiast m.in. sprawdzenie, czy wszyscy użytkownicy zapoznali się z PBE i czy nie mieli dostępu do SWB.

   W art. 2 Ustawy o ochronie informacji niejawnych przedstawiono również definicje:

- Akredytacji bezpieczeństwa teleinformatycznego;

- Certyfikacji;

- Audytu.

   Definicje zostały zamieszczone w materiale ze względu na częste pomyłki zauważone w rozmowach telefonicznych, czy też przesłanych pismach. Zdarza się, że rozmówcy mylą i stosują niezgodnie z przeznaczeniem powyższą terminologię.

   Zwraca się uwagę, że akredytacja systemu jest pojęciem najszerszym, składająca się zarówno z oceny i zatwierdzenia przesłanej dokumentacji bezpieczeństwa jak i przeprowadzenia audytu.

   Certyfikacja dotyczy sprawdzenia samych urządzeń, zwłaszcza ze względu na ryzyko ulotu elektromagnetycznego.

   Audyt natomiast jest sprawdzeniem stanu faktycznego przygotowania systemu do pracy w danej jednostce organizacyjnej, po zatwierdzeniu dokumentacji bezpieczeństwa systemu.

**SYSTEM TELEINFORMATYCZNY W MYŚL ART. 2. PKT 3 USTAWY Z DNIA 18 LIPCA 2002 R. O ŚWIADCZENIU USŁUG DROGĄ ELEKTRONICZNĄ (T.J. DZ. U. Z 2020 R. POZ. 344)**- jest to:

– zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2022 r. poz. 1648, 1933 i 2581);

**Analogiczna definicja wynika z rozdz. 3 ust. 28 Zaleceń SKW w zakresie bezpieczeństwa teleinformatycznego dotyczące podstawowych wymagań dla systemów teleinformatycznych przetwarzających informacje niejawne ZBT-105**

SYSTEM TELEINFORMATYCZNY – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2022 r. poz. 1648, 1933 i 2581).

**ODPOWIEDZIALNOŚĆ ZA SPORZĄDZANIE DOKUMENTACJI BEZPIECZEŃSTWA SYSTEMÓW TELEINFORMATYCZNYCH**

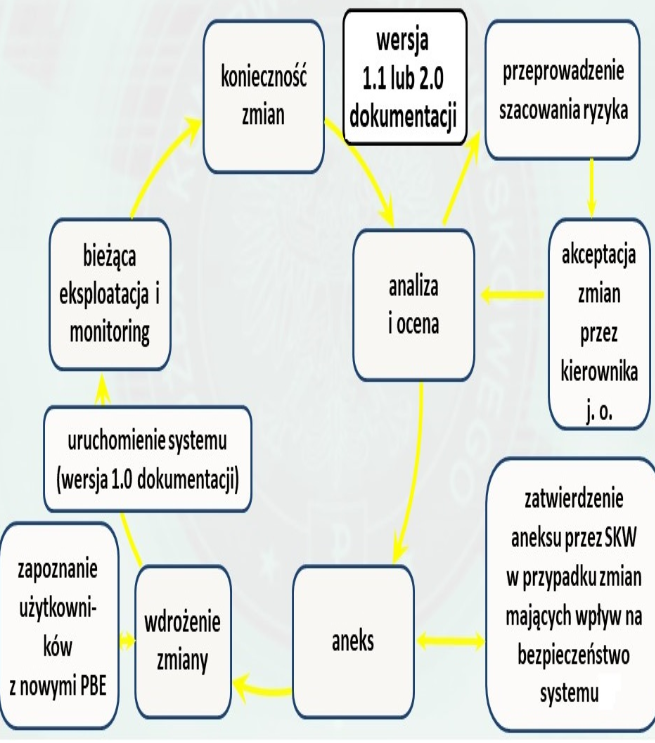


\* - w przypadku systemów kryptograficznych

   Administrator systemu (lub grupa administratorów) jest podstawową osobą funkcyjną odpowiedzialną za opracowanie dokumentacji bezpieczeństwa projektowanego systemu teleinformatycznego. Nie jest on jednak odosobniony w działaniu. Powinien współpracować z osobami funkcyjnymi wymienionymi na ww. rysunku.

   Inspektor bezpieczeństwa teleinformatycznego (IBT) może uczestniczyć w opracowaniu dokumentacji bezpieczeństwa. IBT ma obowiązek uczestniczenia w opracowaniu dokumentacji szacowania ryzyka systemu teleinformatycznego. Gdy IBT nie współtworzy dokumentacji bezpieczeństwa, powinien ją oceniać i wyrazić swoją rekomendacje pełnomocnikowi ds. ochrony informacji niejawnych przed przekazaniem jej kierownikowi jednostki organizacyjnej do podpisu.

* **WPROWADZANIE ZMIAN W DOKUMENTACJI BEZPIECZEŃSTWA SYSTEMÓW TELEINFORMATYCZNYCH**



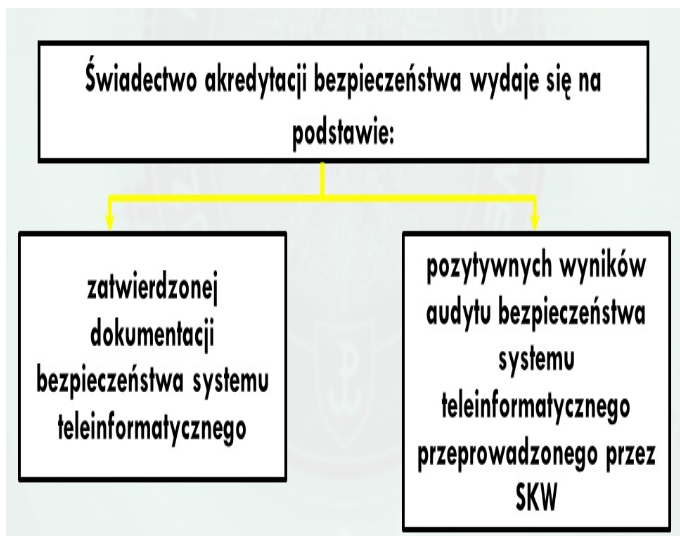
   Dotyczy systemów teleinformatycznych niejawnych od klauzuli POUFNE wzwyż. Pierwotnie wykonana dokumentacji powinna posiadać oznaczenie 1.0. W przypadku uwag do SWB lub PBE lub też stwierdzenie przez organizatora konieczności wykonania kolejnej wersji dokumentacji, nadaje się kolejne oznaczenia: 1.1, 1.2, 1.3 itd. W przypadku zmian istotnych (np. zmiana systemu operacyjnego, wykrycie nowych podatności, zmiana klauzuli tajności systemu itp.) oraz konieczność reakredytacji systemu (w przypadku zbliżania się końca terminu ważności świadectwa akredytacji) kolejna wersja dokumentacji powinna otrzymać oznaczenie 2.0. Ze względu na występujące sytuacje, że dokumentacja SWB wymaga zmian, a PBE nie, istnieje możliwość występowania innych numerów wersji dla obu składowych dokumentacji, np. SWB 1.3, PBE 1.1. Należy pamiętać, że wszelkie zmiany w systemie powinny zostać poprzedzone ponownym przeprowadzeniem szacowania ryzyka oraz, że w przypadku zmian do PBE należy zapoznać z aneksem wszystkich użytkowników systemu. W przypadku niewielkich zmian należy przesyłać aneks wyłącznie w trybie informowania, a w przypadku większych zmian, aneks wymaga zatwierdzenia przez dyrektora Zarząd VI SKW.

* **ZASADY AKREDYTACJI BEZPIECZEŃSTWA TELEINFORMATYCZNEGO**

   Akredytacja bezpieczeństwa teleinformatycznego ma na celu formalne dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych, po zrealizowaniu wymogów określonych we właściwych dokumentach normatywnych.

   SKW udziela akredytacji bezpieczeństwa teleinformatycznego dla systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli POUFNE lub wyższych.

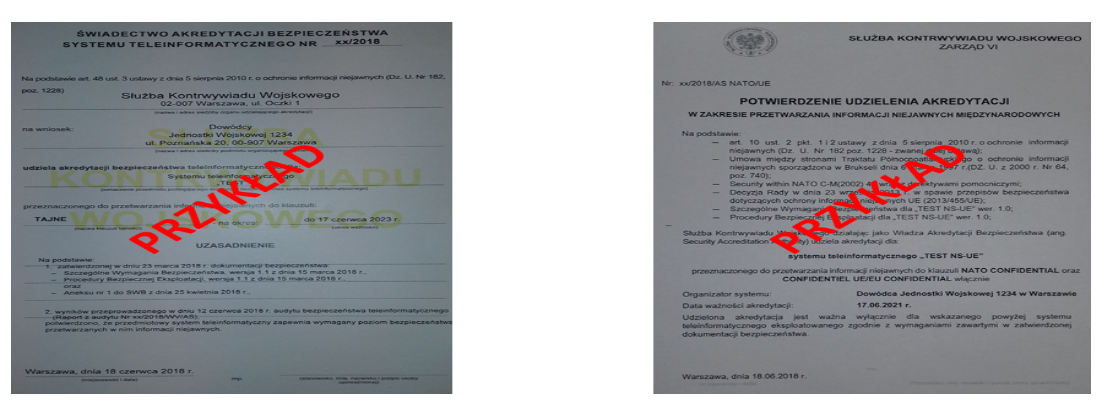
   Potwierdzeniem udzielenia przez SKW akredytacji jest Świadectwo Akredytacji Bezpieczeństwa Systemu Teleinformatycznego (wydawane na okres maksymalnie 5 lat).



   Dokumentem świadczącym o pozytywnym zakończeniu procesu akredytacji systemu teleinformatycznego jest świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego, zwane w skrócie świadectwem akredytacji. Dokument ten wystawiany jest po pozytywnej ocenie przesłanej dokumentacji bezpieczeństwa oraz pozytywnych wynikach przeprowadzonego audytu. W przypadku systemów przetwarzających informacje niejawne o klauzuli POUFNE istnieje możliwość odstąpienia od przeprowadzenia audytu. Wyjątek ten nie jest możliwy w przypadku systemów o klauzuli NATO CONFIDENTIAL, CONFIDENTIEL UE/EU CONFIDENTIAL. Świadectwo akredytacji wydawane jest na maksymalnie 5 lat. W przypadku skomplikowanych systemów, tworzonych i zatwierdzanych z problemami i uwagami, świadectwo może być wystawione na krótszy okres czasu.

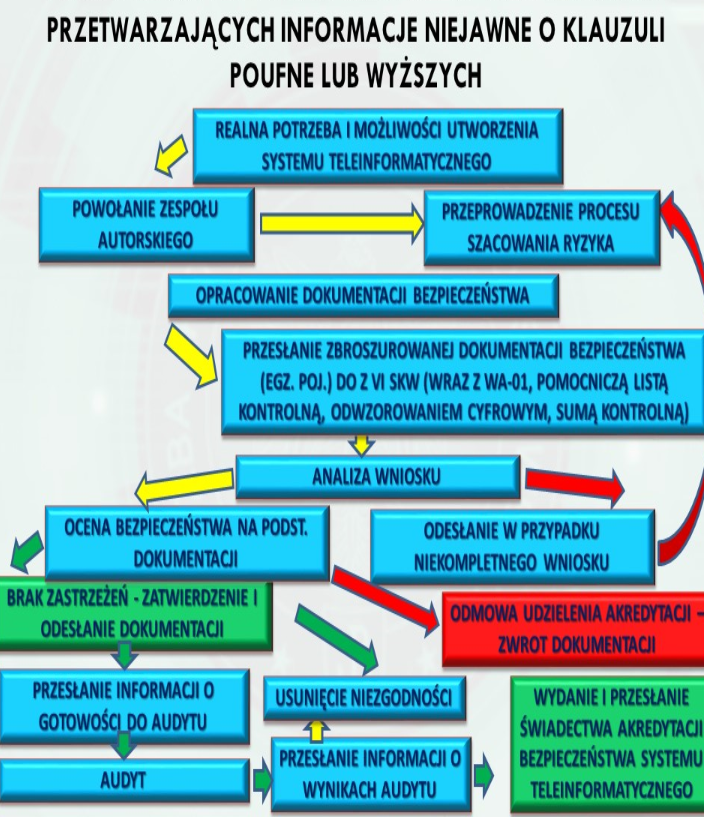


   Przykłady świadectwa akredytacji (dla systemów teleinformatycznych przetwarzających informacje niejawne narodowe) oraz potwierdzenia udzielenia akredytacji - PUA (dla systemów teleinformatycznych przetwarzających informacje niejawne międzynarodowe):



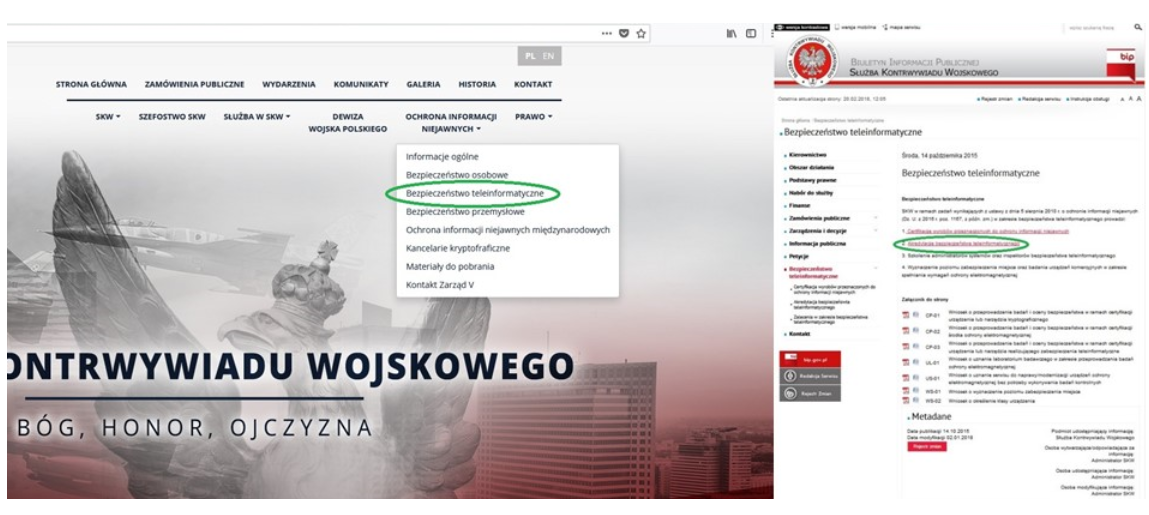


Uprawnionym do udzielenia akredytacji systemów teleinformatycznych przetwarzających informacje niejawne o klauzuli ZASTRZEŻONE jest kierownik jednostki organizacyjnej. Mimo samodzielnego udzielenia akredytacji, na kierowniku jednostki organizacyjnej ciąży obowiązek przesłania do Zarządu VI SKW w terminie 30 dni od udzielenia akredytacji, dokumentacji bezpieczeństwa w celu wyrażenia opinii, czy akredytacja została udzielona prawidłowo. SKW ma 30 dni na ocenę przesłanej dokumentacji pod kątem prawidłowości udzielenia akredytacji. W przypadku braku uwag, zwracana jest dokumentacja z informacją o odesłaniu po służbowym wykorzystaniu. W przypadku uwag, kierownik jednostki organizacyjnej otrzymuje sugestie do naniesienia poprawek w dokumentacji. Najgorszą sytuacją jest odpowiedź nakazująca natychmiastowe wstrzymanie pracy systemu, co może wiązać się z dalszymi krokami, w tym koniecznością przesłania szczegółowych wyjaśnień. Dokumentacja wykonywana jest zawsze w jednym egzemplarzu, dlatego po ocenie odsyłana jest do organizatora systemu.



    Na stronie [www.bip.skw.gov.pl](http://www.bip.skw.gov.pl/skw/bezpieczenstwo-teleinfo/5107,Bezpieczenstwo-teleinformatyczne.html) znajdą Państwo wymagania stawiane przed dokumentacją bezpieczeństwa i dokumentami pomocniczymi, które należy przesłać do oceny przez Zarząd VI SKW. Zwraca się uwagę na przesyłanie dokumentacji bezpieczeństwa systemów teleinformatycznych przetwarzających informacje niejawne o klauzuli POUFNE (oraz odpowiednikami UE i NATO) oraz wyższych klauzulach, w jednym egzemplarzu zbroszurowanej dokumentacji (oprawionej lub zszytej), z załączeniem odwzorowania cyfrowego (format .pdf na płycie CD/DVD z podaną sumą kontrolną). Zobrazowanie cyfrowe powinno być wiernym odzwierciedleniem ostatecznej wersji dokumentacji z wszystkimi podpisami osób funkcyjnych, a nie plikiem przekonwertowanym z formatu „.doc”. Na ocenę dokumentacji SKW ma czas 30 do 60 dni, a cały proces akredytacji trwa 6 do 12 miesięcy, w zależności od złożoności systemu. Zwraca się uwagę, że po zatwierdzeniu dokumentacji, organizator systemu w terminie do 6 miesięcy powinien zgłosić gotowość do audytu. W przypadku braku zgłoszenia, proces akredytacji zostaje przerwany.

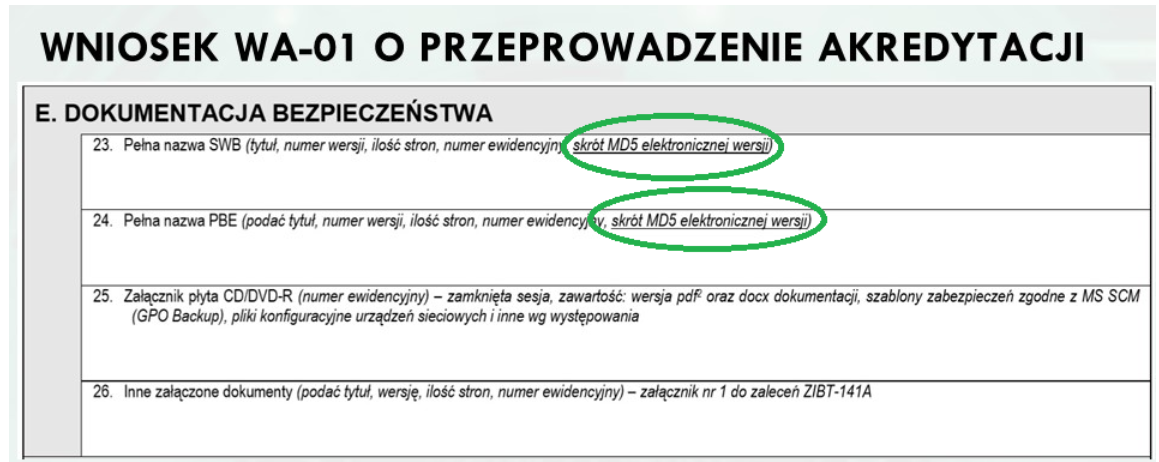
   Wnioski ZA-01 (dotyczące systemów przetwarzających informacje niejawne o klauzuli ZASTRZEŻONE) oraz WA-01 (dotyczące systemów teleinformatycznych przetwarzających informacje niejawne POUFNE i wyższe) wymagane do rozpoczęcia procesu akredytacji systemów teleinformatycznych przetwarzających informacje niejawne dostępne są do pobrania na stronie [https://www.bip.skw.gov.pl](http://www.bip.skw.gov.pl/skw/bezpieczenstwo-teleinfo/5107,Bezpieczenstwo-teleinformatyczne.html) przedstawionej poniżej:



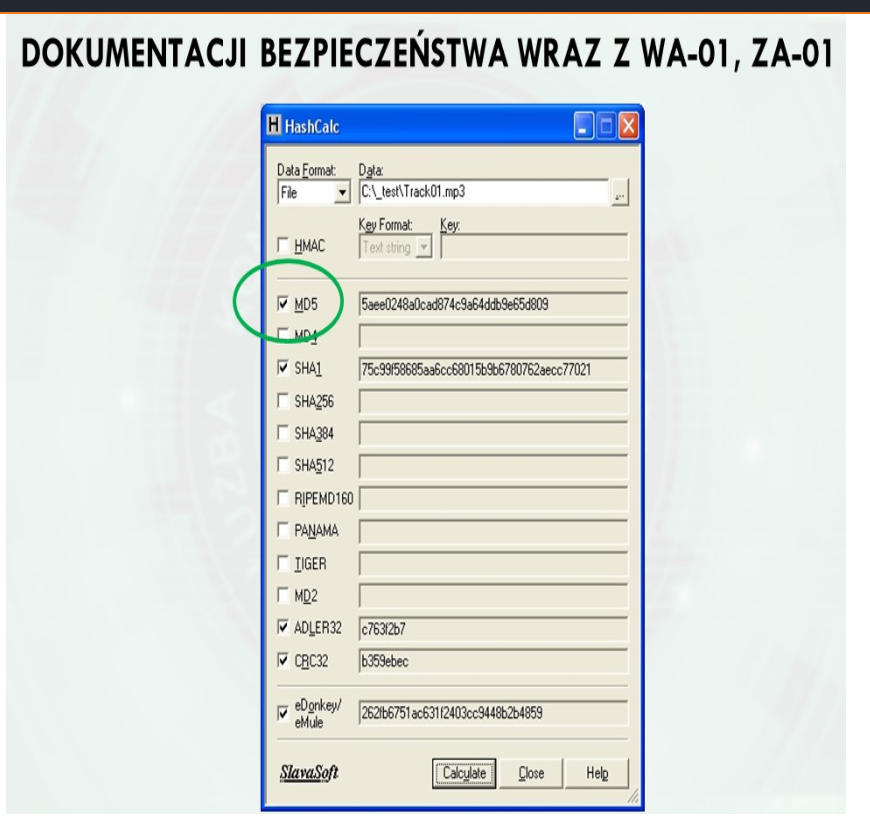
   Wygląd wniosku WA-01. Zwraca się uwagę, aby w części D zamieszczono telefony kontaktowe do osób funkcyjnych, co umożliwi kontakt w przypadku uwag do dokumentacji lub też umówienia terminu audytu.



   W części E wniosku WA-01 znajduje się wymóg zamieszczenia skrótu MD5 elektronicznej wersji. Skąd go pozyskać przedstawiono na kolejnym rysunku.



   M.in. w MILNET-Z znajduje się program HASHCALC, generujący sumy kontrolne. Wystarczy podać ścieżkę do dokumentacji (pliku w formacie„.pdf”), zaznaczyć MD5 lub SHA 1, SHA 256 i wciśnąć przycisk „CALCULATE”. Wygenerowany ciąg znaków pojawiający się przy zaznaczonym trybie (MD5, SHA1, SHA256) należy wpisać do części E wnosku WA-01 (lub ZA-01). Wykorzystanie sumy kontrolnej pozwoli sprawdzić, czy w przesłanym pliku nie doszło do żadnego naruszenia zawartości (np. przez dogranie oprogramowania złośliwego).



* **PROCES PONOWNEJ AKREDYTACJI SYSTEMÓW TELEINFORMATYCZNYCH PRZETWARZAJĄCYCH INFORMACJE NIEJAWNE**

   Ponowna akredytacja systemu, wiąże się z przesłaniem do Zarządu VI SKW wniosku WA-01 wraz z nową wersją dokumentacji w terminie 6 miesięcy przed upływem ważności Świadectwo Akredytacji Bezpieczeństwa Systemu Teleinformatycznego.

   Sporządzenie nowej wersji dokumentacji bezpieczeństwa systemu jest równoznaczne z koniecznością przeprowadzenia ponownej akredytacji systemu.

   Konieczność ponownej akredytacji systemu jest wymagana w przypadku:

- podwyższenia lub rozszerzenia klauzuli przewidzianych do przetwarzania w systemie informacji niejawnych;

- zmiany trybu bezpieczeństwa pracy systemu;

- zmiany przeznaczenia systemu.

Konieczność ponownej akredytacji systemu może być wymagana w przypadku:

- wzrostu poziomu ryzyka lub identyfikacji nowych ryzyk dla bezpieczeństwa przetwarzanych w systemie teleinformatycznym informacji niejawnych;

- obniżenia poziomu ochrony lub klasy bezpieczeństwa wykorzystywanych urządzeń lub oprogramowania realizującego funkcję zabezpieczającą;

- konieczności zmiany konfiguracji sprzętowej lub programowej mogącej mieć negatywny wpływ na bezpieczeństwo przetwarzanych w systemie informacji niejawnych.

**Uwaga!**

   Zasadność przeprowadzenia ponownej akredytacji oraz decyzja o konieczności jej przeprowadzenia jest rozpatrywana indywidualnie dla każdego systemu posiadającego ważną akredytację i jest podejmowana przez organ, który akredytacji udzielił.

   W przypadku zmiany systemu operacyjnego, którego mechanizmy bezpieczeństwa oddziałują globalnie na system teleinformatyczny wymagana jest obligatoryjnie jego ponowna akredytacja (np. zmiana systemu operacyjnego w systemach autonomicznych).

* **PROCES AKREDYTACJI SYSTEMÓW TELEINFORMATYCZNYCH PRZETWARZAJĄCYCH INFORMACJE NIEJAWNE MIĘDZYNARODOWE**

   SKW pełni funkcję władzy akredytacyjnej i jest właściwa do akredytacji bezpieczeństwa systemów teleinformatycznych przetwarzających informacje niejawne międzynarodowe organizowanych przez podmioty, o których mowa w art. 10 ust. 2 pkt. 1 i 2 Ustawy.

   W przypadku systemów narodowych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „zastrzeżone”, w których dopuszcza się przetwarzanie informacji niejawnych międzynarodowych wymagane jest wcześniejsze udzielenie przez kierownika jednostki organizującej system akredytacji bezpieczeństwa w trybie art. 48 ust. 9 lub ust. 10 Ustawy.

* **WARUNKI DOPUSZCZENIA SYSTEMU DO PRZETWARZANIA INFORMACJI NIEJAWNYCH MIĘDZYNARODOWYCH**

   Systemy narodowe przeznaczone do przetwarzania informacji niejawnych o klauzuli „zastrzeżone”, w których dopuszcza się przetwarzanie informacji niejawnych międzynarodowych wymagają wcześniejszego udzielenie przez kierownika jednostki organizującej system akredytacji bezpieczeństwa oraz brak uwag SKW odnośnie udzielonej akredytacji.

   Systemy teleinformatyczne przeznaczone do przetwarzania informacji niejawnych międzynarodowych wymagają pisemnego potwierdzenia udzielenia przez SKW akredytacji określające:

- spełnienia przez system wymagań wynikających z regulacji międzynarodowych;

- zakres akredytacji (akredytowane elementy systemu, klauzule informacji itp.);

- datę ważności akredytacji;

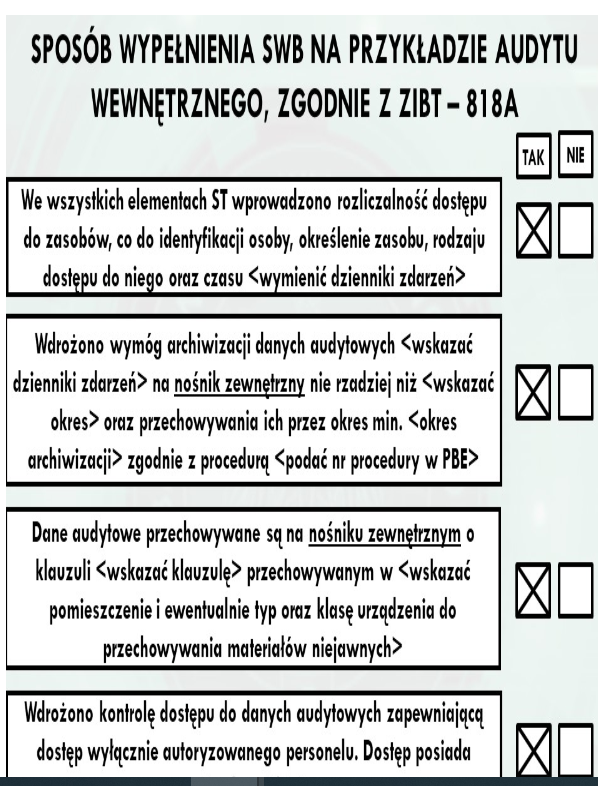
- warunki utrzymania ważności akredytacji.

* **ZAWARTOŚĆ DOKUMENTACJI BEZPIECZEŃSTWA**

   Zalecenia ZIBT-818 A i ZIBT-818 B dotyczące zawartości dokumentacji bezpieczeństwa są rewolucyjne w stosunku do wycofanych DBBT-804 A. Nowe zalecenia wprowadziły ograniczenia treści dokumentów. W miejsce szczegółowych opisów wprowadzono deklarację kierownika jednostki organizacyjnej o spełnieniu konkretnych kryteriów. Zwłaszcza ZIBT-818 A dotyczący SWB stanowi dokument opierający się na deklaracjach. Wypełnienie szablonu dokumentu jest intuicyjne i polega na zaznaczeniu konkretnych pól wyboru i wpisaniu tekstu w kwadratowe nawiasy: „<„, „>”. Dokumentację bezpieczeństwa drukuje się bez odsyłaczy i instrukcji. Nie należy samodzielnie zmieniać układu dokumentacji bez zgody Zarządu VI SKW. Dopuszczalne jest jedynie zwięzłe wyjaśnienie pod danym punktem, w przypadku gdy formularz nie przewidywał sytuacji, która zachodzi w danej jednostce organizacyjnej.



   Na poniższym rysunku przedstawiono przykładowy fragment ZIBT-818 A, poświęcony audytowi wewnętrznemu. Opracowując dokumentację należy zaznaczyć jedynie odpowiednie kwadraty oraz wpisać odpowiedni tekst, w kwadratowych nawiasach, uszczegółowiających terminy, miejsca przechowywania, klasy urządzeń, osoby funkcyjne itp.



* **ROZWIĄZANIA INFORMATYCZNE**

W przypadku potrzeby wymiany informacji niejawnych przez system teleinformatyczny posiadający akredytację bezpieczeństwa teleinformatycznego z rozwiązaniami informatycznymi dopuszczonymi na podstawie art. 51 ust. 3 ustawy niezbędne jest uwzględnienie wymagań i procedur w przedmiotowym zakresie w dokumentacji szczególnych wymagań bezpieczeństwa oraz procedur bezpiecznej eksploatacji systemu z zastosowaniem procedur określonych w dokumencie „Wymagania ochrony informacji niejawnych” które opracowane zostały na podstawie Rozporządzenia Ministra Obrony Narodowej z dnia 29 września 2022 r. w sprawie trybu oceny i sposobu dopuszczania rozwiązań informatycznych, w których mają być przetwarzane informacje niejawne (Dz. U. 14 października 2022, poz. 2098).

* **WYMAGANIA W STOSUNKU DO PERSONELU BEZPIECZEŃSTWA**

   Główne wymagania w stosunku do personelu bezpieczeństwa przedstawiono w tabeli. Zwraca się uwagę, że administrator powinien posiadać poświadczenie bezpieczeństwa osobowego wyższe niż klauzula informacji niejawnych przetwarzanych w systemie, podczas gdy inspektor bezpieczeństwa teleinformatycznego może posiadać poświadczenie bezpieczeństwa zgodne z najwyższą klauzulą informacji niejawnych przetwarzanych w systemie.  Wymagane jest również ukończenie przez administratora oraz inspektora bezpieczeństwa teleinformatycznego szkolenia podstawowego z ochrony informacji niejawnych realizowanego przez pełnomocnika ds. ochrony informacji niejawnych danej jednostki organizacyjnej, szkolenia specjalistycznego realizowanego przez SKW oraz, w przypadku gdy system przetwarza informacje niejawne o klauzuli TAJNE i wyższe, również szkolenia przeprowadzanego przez producenta oprogramowania wykorzystywanego w systemie (Windows 10 i/lub Windows Server 2016, 2019). Szkolenia organizowane u producenta oprogramowania nie są wymagane w przypadku posiadania przez ww. personel bezpieczeństwa wykształcenia informatycznego.



* **POSTĘPOWANIE W PRZYPADKU BRAKU PERSONELU BEZPIECZEŃSTWA**

Rozdział 8 Bezpieczeństwo teleinformatyczne Art. 52. Ustęp 2. Ustawy

   W uzasadnionych przypadkach, za zgodą ABW albo SKW, administrator systemu lub inspektor bezpieczeństwa teleinformatycznego może wykonywać zadania w więcej niż jednej jednostce organizacyjnej na podstawie porozumienia właściwych kierowników jednostek organizacyjnych.

   Podjęcie zadań możliwe jest po uzyskaniu zgody przez Zarząd VI SKW, a nie po zawarciu porozumienia!

   Wniosek o wyrażenie zgody wynikającej z art. 52 ust. 2 Ustawy o ochronie informacji niejawnych powinien zawierać przedstawione na poniższym rysunku dane. Należy zauważyć, że w przypadku jakiejkolwiek formy zatrudnienia (umowy o pracę, umowy o dzieło, umowy-zlecenia), nie zachodzi właściwość art. 52 ust. 2 i wówczas brak jest konieczności do ubiegania się o przedmiotową zgodę.

   Warunki otrzymania zgody:

- uzasadnienie powodu zawarcia porozumienia;

- zawarcie porozumienia pomiędzy kierownikami jednostek organizacyjnych;

- rekomendacja organizatora systemu teleinformatycznego odnośnie przesłanego wniosku;

- podanie nazwy i klauzuli sytemu teleinformatycznego;

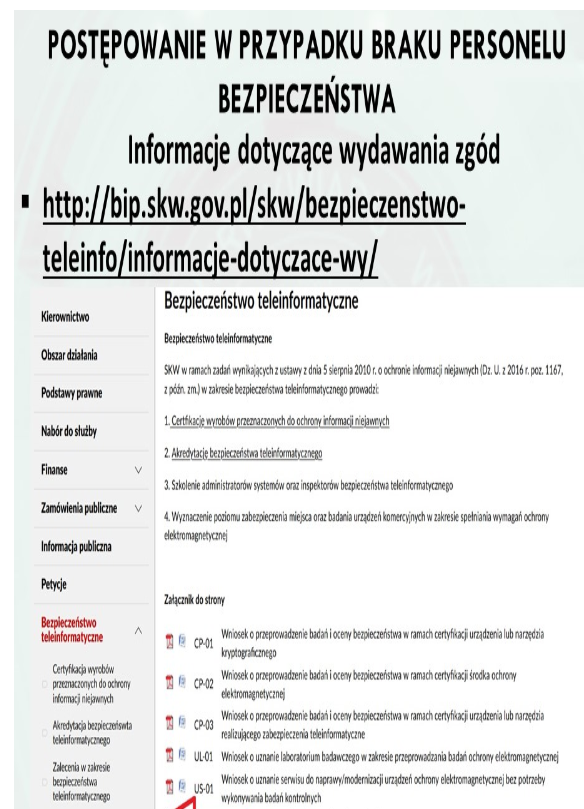
- podanie terminu ważności porozumienia;

- informacje dotyczące braku zawarcia jednej z form umowy świadczenia pracy (umowy o pracę, umowy o dzieło, umowy-zlecenia);

- określenie wymiaru czasu pracy (warunków wykonywania pracy).

- wskazanie imienne osób wraz z deklaracją odnośnie spełnienia przez nich stosownych wymagań;

- przedstawienie obowiązków osób, których porozumienie dotyczy.

   Szczegóły sporządzania wniosku o pełnienie funkcji administratora lub IBT w innej jednostce organizacyjnej przedstawiono na niżej wymienionej stronie internetowej: 

* **DANE KONTAKTOWE DO ZARZĄDU VI SŁUŻBY KONTRWYWIADU WOJSKOWEGO**

Telefon:  261-841-205

[www.bip.skw.gov.pl](http://www.bip.skw.gov.pl/skw/bezpieczenstwo-teleinfo/5107,Bezpieczenstwo-teleinformatyczne.html)

# Obowiązki Administratorów Systemów Teleinformatycznych

* **ZADANIA ADMINISTRATORA WYNIKAJĄCE Z ROZDZIAŁU 8, ART. 52 UST. 1 USTAWY O OCHRONIE INFORMACJI NIEJAWNYCH**

   Kierownik jednostki organizacyjnej wyznacza:

1) pracownika lub pracowników pionu ochrony pełniących funkcję inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnych za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji.

2) 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, zwanych dalej administratorem systemu.

* **ZADANIA ADMINISTRATORA WYNIKAJĄCE Z § 13 ROZPORZĄDZENIA PREZESA RADY MINISTRÓW Z DNIA 20 LIPCA 2011 R.**

   Administrator systemu teleinformatycznego bierze udział w tworzeniu dokumentacji bezpieczeństwa systemu teleinformatycznego oraz w procesie zarządzania ryzykiem w systemie teleinformatycznym:

1) realizując szkolenia użytkowników systemu teleinformatycznego;

2) utrzymując zgodność systemu teleinformatycznego z jego dokumentacją bezpieczeństwa;

3) wdrażając zabezpieczenia w systemie teleinformatycznym.

* **ZADANIA ADMINISTRATORA WYNIKAJĄCE Z ZAŁĄCZNIKA NR 1 UST. 5 DECYZJI NR 7/MON MINISTRA OBRONY NARODOWEJ Z DNIA 20 STYCZNIA 2012 R.**

   Administrator systemu realizuje zadania w zakresie odpowiedzialności za funkcjonowanie systemu teleinformatycznego oraz odpowiada za przestrzeganie zasad i wymagań bezpieczeństwa Przewidzianych dla systemu teleinformatycznego, w szczególności:

1) opracowuje i uaktualniania dokumentację bezpieczeństwa systemu teleinformatycznego;

2) przechowuje oryginały zatwierdzonej dokumentacji bezpieczeństwa teleinformatycznego systemu teleinformatycznego;

3) uczestniczy w procesie szacowania ryzyka;

4) wdraża procedury bezpiecznej eksploatacji;

5) szkoli użytkowników systemu teleinformatycznego  
z zakresu procedur bezpiecznej eksploatacji;

6) utrzymuje zgodność konfiguracji i parametrów systemu teleinformatycznego z dokumentacją bezpieczeństwa systemu;

7) systematycznie kontroluje funkcjonowanie mechanizmów zabezpieczeń i poprawność działania systemu teleinformatycznego;

8) informuje pełnomocnika ochrony o stwierdzonych naruszeniach bezpieczeństwa systemu teleinformatycznego;

9) zgłasza do pełnomocnika ochrony potrzeby w zakresie serwisowania i certyfikacji środków ochrony elektromagnetycznej;

10) analizuje i archiwizuje rejestr zdarzeń w systemie teleinformatycznym;

11) prowadzi wykaz osób mających dostęp do systemu teleinformatycznego zawierający co najmniej: imię i nazwisko, nazwę jednostki (komórki) organizacyjnej, posiadane poświadczenie bezpieczeństwa (jego numer, klauzulę i datę ważności) oraz przydziela użytkownikom konta, zgodnie z uprawnieniami nadanymi przez kierownika jednostki (komórki) organizacyjnej;

12) zapewnia dostęp do systemu teleinformatycznego wyłącznie użytkowników posiadających wymagane uprawnienia oraz odpowiednie i ważne poświadczenia bezpieczeństwa.

**Uwaga!**

   Zgodnie z Załącznikiem nr 2 pkt 6-10 do przedmiotowej Decyzji:

1) Do pełnienia funkcji administratora systemu zaleca się wyznaczać osoby posiadające wykształcenie informatyczne;

2) Do pełnienia funkcji administratora systemu, w którym przetwarzanie są informacje niejawne o klauzuli „TAJNE” lub „ŚCIŚLE TAJNE”, wyznacza się osoby posiadające kwalifikacje w zakresie administrowania systemami teleinformatycznymi, potwierdzone ważnym świadectwem, certyfikatem lub zaświadczeniem;

3) Kierownicy jednostek organizacyjnych kierują osoby wyznaczone do pełnienia funkcji administratorów systemów na dodatkowe szkolenia, poza określonymi w art. 52 ust. 4 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, w celu podnoszenia ich kwalifikacji w zakresie administrowania systemami teleinformatycznymi;  
4) Dodatkowe szkolenia kończące się wydaniem dokumentu, potwierdzającego nabycie umiejętności w zakresie administrowania systemem użytkowanym w jednostce organizacyjnej, są prowadzone:

- w ośrodkach kształcenia autoryzowanych przez producenta sprzętu komputerowego, oprogramowania lub urządzeń wraz z oprogramowania, zapewniających bezpieczeństwo systemów teleinformatycznych;

- przez organy wojskowe pod warunkiem uzgodnienia programu oraz formy szkolenia (przez obecne DK WOC);

5) Na szkolenia, o których mowa w pkt 8. kierownicy jednostek organizacyjnych mogą kierować (w miarę posiadanych środków) administratorów pozostałych systemów teleinformatycznych.

* **ZADANIA ADMINISTRATORA WYNIKAJĄCE Z PKT. 8.1.4 ZALECEŃ SKW W ZAKRESIE BEZPIECZEŃSTWA TELEINFORMATYCZNEGO DOTYCZĄCE PODSTAWOWYCH WYMAGAŃ DLA SYSTEMÓW TELEINFORMATYCZNYCH PRZETWARZAJĄCH INFORMACJE NIEJAWNE - ZBT-105**

   Administrator systemu realizuje zadania w zakresie zapewnienia funkcjonowania oraz przestrzegania zasad i wymagań bezpieczeństwa systemu teleinformatycznego. W szczególności odpowiada za:

a) udział w opracowywaniu dokumentacji bezpieczeństwa;

b) przechowywanie zatwierdzonej dokumentacji bezpieczeństwa teleinformatycznego oraz udostępnianie procedur bezpiecznej eksploatacji użytkownikom systemu teleinformatycznego;

c) wdrażanie procedur bezpiecznej eksploatacji systemu teleinformatycznego;

d) szkolenie użytkowników systemu teleinformatycznego z zakresu jego bezpiecznej eksploatacji;

e) utrzymywanie zgodności konfiguracji i parametrów systemu teleinformatycznego z jego dokumentacją bezpieczeństwa oraz innymi dokumentami normatywnymi;

f) systematyczne kontrolowanie funkcjonowania mechanizmów bezpieczeństwa oraz poprawności działania systemu teleinformatycznego;

g) informowanie pełnomocnika ds. ochrony informacji niejawnych oraz uprawnionych organów o stwierdzonych naruszeniach bezpieczeństwa teleinformatycznego;

h) zgłaszanie pełnomocnikowi ds. ochrony informacji niejawnych potrzeby w zakresie serwisowania i ponownej certyfikacji urządzeń i narzędzi, służących do ochrony informacji niejawnych;

i) analizowanie i archiwizację rejestru zdarzeń w systemie teleinformatycznym;

j) realizowanie określonej w dokumentacji bezpieczeństwa procedury przydzielania kont oraz mechanizmów kontroli dostępu, a także za zapewnienie ich właściwego wykorzystania;

k) prowadzenie aktualnego wykazu osób mających dostęp do systemu teleinformatycznego oraz przydzielanie użytkownikom kont, zgodnie z uprawnieniami nadanymi przez kierownika jednostki organizacyjnej.

# Obowiązki Inspektorów Bezpieczeństwa Teleinformatycznego

* **ZADANIA IBT WYNIKAJĄCE Z USTAWY O OCHRONIE INFORMACJI NIEJAWNYCH**

   Art. 16. Pracownikiem pionu ochrony w jednostce organizacyjnej może być osoba, która posiada:

- ust. 1. obywatelstwo polskie z wyjątkiem pracowników pionu ochrony zatrudnionych u przedsiębiorców;

- ust. 2. odpowiednie poświadczenie bezpieczeństwa lub upoważnienie, o którym mowa w art. 21 ust 4 pkt 1. (upoważnienie kierownika jednostki organizacyjnej do zastrzeżonych informacji niejawnych);

- ust. 3. zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych.

   Rozdział 8 Bezpieczeństwo teleinformatyczne, art. 52. Ustęp 1.

   Kierownik jednostki organizacyjnej wyznacza pracownika lub pracowników pionu ochrony pełniących funkcję inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnych za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji.

* **ZADANIA IBT WYNIKAJĄCE Z § 14 ROZPORZĄDZENIA PREZESA RADY MINISTRÓW Z DNIA 20 LIPCA 2011 R.**

  Inspektor bezpieczeństwa teleinformatycznego bierze udział w procesie zarządzania ryzykiem w systemie teleinformatycznym, weryfikując:

1) poprawność realizacji zadań przez administratora, w tym właściwe zarządzanie konfiguracją oraz uprawnieniami przydzielanymi użytkownikom;

2) znajomość i przestrzeganie przez użytkowników zasad ochrony informacji niejawnych oraz procedur bezpiecznej eksploatacji w systemie teleinformatycznym, w tym w zakresie wykorzystywania urządzeń i narzędzi służących do ochrony informacji niejawnych;

3) stan zabezpieczeń systemu teleinformatycznego, w tym analizując rejestry zdarzeń systemu teleinformatycznego.

* **ZADANIA IBT WYNIKAJĄCE Z § 4 DECYZJI NR 7/MON MINISTRA OBRONY NARODOWEJ Z DNIA 20 STYCZNIA 2012 r.**

IBT realizuje zadania w zakresie weryfikacji i bieżącej kontroli zgodności funkcjonowania eksploatowanego w danej jednostce organizacyjnej systemu teleinformatycznego z jego dokumentacją bezpieczeństwa, a w szczególności kontroluje:

1) Przestrzeganie zasad ochrony przetwarzanych w systemie teleinformatycznym informacji niejawnych;

2) Poprawność realizacji zadań wykonywanych przez administratora;

3) Zgodność konfiguracji systemu teleinformatycznego z dokumentacją bezpieczeństwa systemu teleinformatycznego;

4) Stan środków bezpieczeństwa fizycznego i ochrony elektromagnetycznej;

5) Aktualność wykazów osób mających dostęp do systemu teleinformatycznego, prawidłowość przydzielania kont użytkownikom, zakres nadanych im uprawnień i prawidłowość zabezpieczeń zastosowanych w systemie teleinformatycznym;

6) Znajomość i przestrzeganie przez użytkowników procedur bezpiecznej eksploatacji systemu teleinformatycznego.

**Ponadto IBT:**

1) Analizuje rejestry zdarzeń w systemie teleinformatycznym i prawidłowość ich archiwizowania;

2) Informuje pełnomocnika ochrony o wszelkich zdarzeniach związanych lub mogących mieć wpływ na bezpieczeństwo systemu teleinformatycznego;

3) Uczestniczy w opracowywaniu programów organizacyjno-użytkowych, projektów koncepcyjnych i technicznych planowanych do budowy systemów teleinformatycznych;

6) Do pełnienia funkcji inspektora bezpieczeństwa teleinformatycznego zaleca się wyznaczać osoby posiadające wykształcenie informatyczne;

7) Do pełnienia funkcji inspektora, w którym przetwarzanie są informacje niejawne o klauzuli „TAJNE” lub „ŚCIŚLE TAJNE”, wyznacza się osoby posiadające kwalifikacje w zakresie administrowania systemami teleinformatycznymi, potwierdzone ważnym świadectwem, certyfikatem lub zaświadczeniem;

8) Kierownicy jednostek organizacyjnych kierują osoby wyznaczone do pełnienia funkcji inspektora na dodatkowe szkolenia, poza określonymi w art. 52 ust. 4 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, w celu podnoszenia ich kwalifikacji w zakresie administrowania systemami teleinformatycznymi.

* **ZADANIA IBT WYNIKAJĄCE Z PKT. 8.1.5 ZALECEŃ SKW W ZAKRESIE BEZPIECZEŃSTWA TELEINFORMATYCZNEGO DOTYCZĄCE PODSTAWOWYCH WYMAGAŃ DLA SYSTEMÓW TELEINFORMATYCZNYCH PRZETWARZAJĄCYCH INFORMACJE NIEJAWNE - ZBT-105.**

IBT realizuje zadania w zakresie bieżącej kontroli ochrony zgodności funkcjonowania systemu teleinformatycznego z dokumentacją bezpieczeństwa teleinformatycznego. W szczególności odpowiada za kontrolę:

a) przestrzegania zasad ochrony informacji niejawnych w systemie teleinformatycznym;

b) stanu zabezpieczeń fizycznych, elektromagnetycznych i elektronicznych pomieszczeń lub obszarów, w których usytuowane są systemy teleinformatyczne;

c) aktualności wykazów osób mających dostęp do systemu teleinformatycznego;

d) poprawności przydzielania kont użytkownikom;

e) poprawności zakresu uprawnień nadanych użytkownikom;

f) znajomości i przestrzegania przez użytkowników procedur bezpiecznej eksploatacji systemu teleinformatycznego oraz urządzeń i narzędzi służących do ochrony informacji niejawnych;

g) przestrzegania zasad i wymagań w zakresie oznaczania, ewidencjonowania, przechowywania i przekazywania wytworzonych dokumentów niejawnych oraz ich terminowego rozliczania;

h) zgodności konfiguracji systemu teleinformatycznego z jego dokumentacją bezpieczeństwa;

Niezależnie od powyższych kompetencji kontrolnych IBT odpowiada za:

a) analizę rejestrów zdarzeń systemu teleinformatycznego (np. logów bezpieczeństwa);

b) informowanie pełnomocnika ds. ochrony informacji niejawnych o wszelkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem systemu teleinformatycznego;

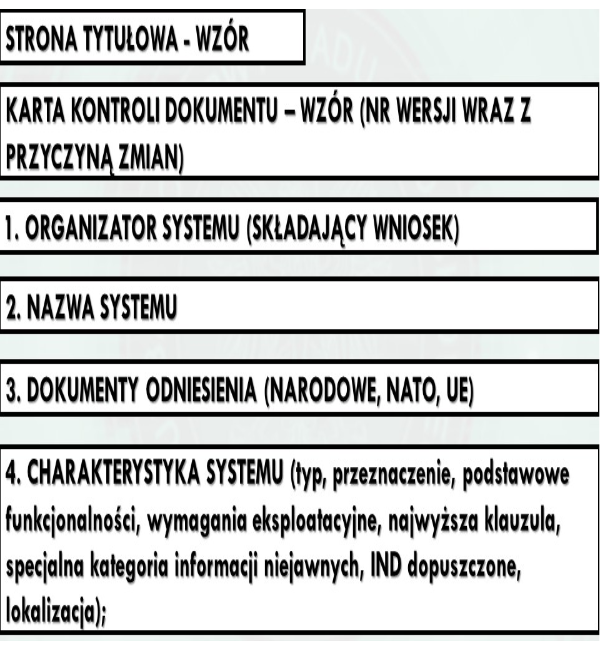
c) prowadzenie szkoleń użytkowników w zakresie ochrony informacji niejawnych oraz przestrzegania zasad bezpieczeństwa w systemie  teleinformatycznym.

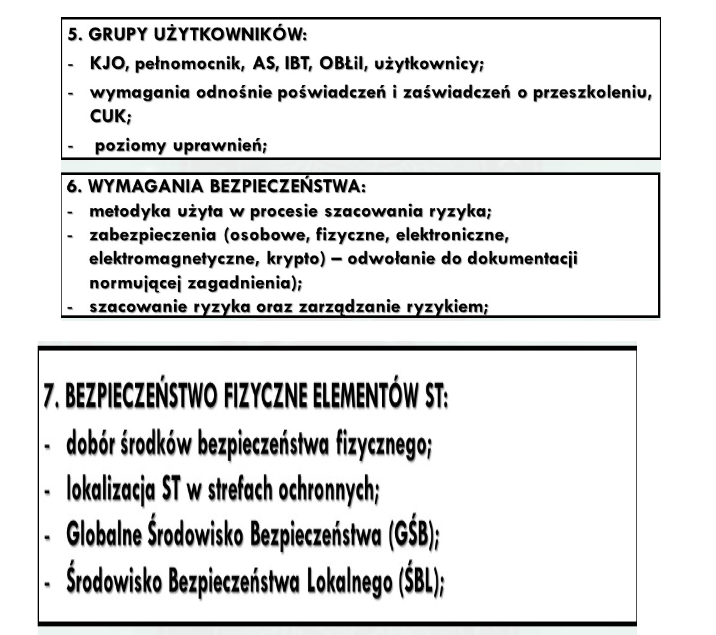
# Dokumentacja bezpieczeństwa

* **AKTY PRAWNE NORMUJĄCE SPORZĄDZANIE DOKUMENTACJI BEZPIECZEŃSTWA SYSTEMU TELEINFORMATYCZNEGO**

    Zalecane jest tworzenie dokumentacji w oparciu o Zalecenia ZIBT – 818 A - Zalecenia w zakresie zawartości dokumentacji bezpieczeństwa systemów teleinformatycznych przetwarzających informacje niejawne SWB oraz Zalecenia ZIBT – 818 B - Zalecenia w zakresie zawartości dokumentacji bezpieczeństwa systemów teleinformatycznych przetwarzających informacje niejawne PBE. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. 159, poz. 948) jest dokumentem normatywnym alternatywnym, wykorzystywanym do systemów rozległych lub nietypowych, ale przede wszystkim do wykorzystania w sferze cywilnej.

* **UKŁAD SWB NA PODSTAWIE ZALECEŃ SKW ZIBT-818 A**

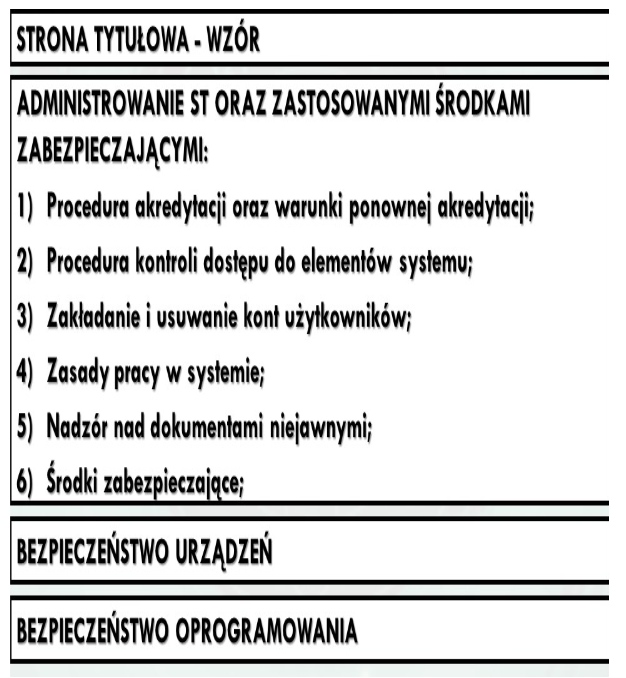


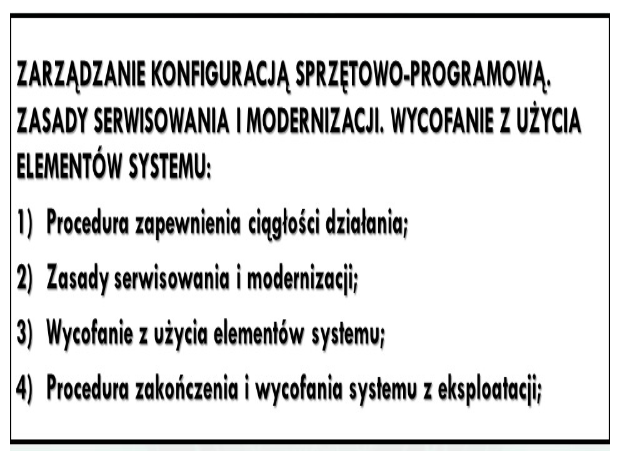




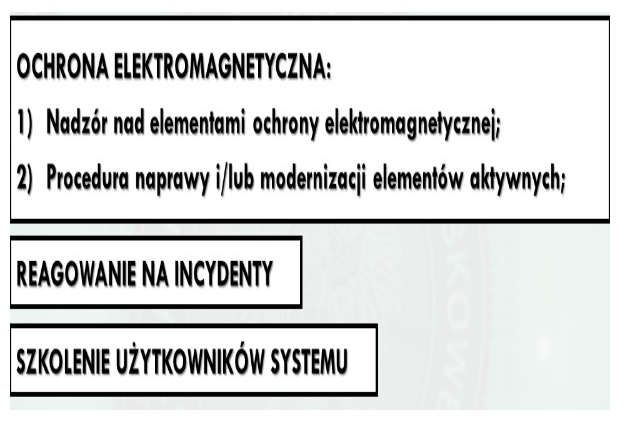


* **UKŁAD PBE NA PODSTAWIE ZALECEŃ SKW ZIBT-818 B**









**Uwaga!**

W przypadku potrzeby wymieniania informacji niejawnych przez system teleinformatyczny posiadający akredytację bezpieczeństwa teleinformatycznego z rozwiązaniami informatycznymi dopuszczonymi na podstawie art. 51 ust. 3 ustawy niezbędne jest uwzględnienie wymagań i procedur w przedmiotowym zakresie w dokumentacji szczególnych wymagań bezpieczeństwa oraz procedur bezpiecznej eksploatacji systemu z zastosowaniem procedur określonych w dokumencie „Wymagania ochrony informacji niejawnych” które opracowane zostały na podstawie Rozporządzenia Ministra Obrony Narodowej z dnia 29 września 2022 r. w sprawie trybu oceny i sposobu dopuszczania rozwiązań informatycznych, w których mają być przetwarzane informacje niejawne (Dz. U. 14 października 2022, poz. 2098).

**UWAGI ODNOŚNIE SZACOWANIA RYZYKA WYNIKAJĄCE Z ZALECEŃ ZIBT – 818 A I DBBT – 811**

- brak możliwości przedstawienia całości dokumentacji szacowania ryzyka w SWB;

- dokumentacja szacowania ryzyka stanowi oddzielny dokument, na który należy się powołać w SWB;

- brak możliwości obiektywnej oceny dokumentacji bezpieczeństwa bez przesłania dokumentacji szacowania ryzyka lub wyciągu dotyczącego szacowania ryzyka danego systemu teleinformatycznego (w przypadku gdy dokumentacja szacowania ryzyka dotyczy więcej niż jednego systemu teleinformatycznego);

- konieczność określenia częstotliwości przeprowadzania okresowego przeglądu ryzyka oraz ponownego szacowania ryzyka;

- konieczność wskazania metodyki użytej w procesie szacowania ryzyka;

- metodyka szacowania ryzyka wskazana w SWB powinna być zbieżna z zapisami właściwego dokumentu szacowania ryzyka;

- konieczność identyfikacji ryzyka szczątkowego i jego przedstawienia;

- ryzyko szczątkowe wskazane w SWB powinno być zbieżne z zapisami właściwego dokumentu szacowania ryzyka;

- dobór zabezpieczeń przeprowadza się na podstawie analizy wyników procesu szacowania ryzyka;

- wszelkie odstępstwa od wymagań normatywnych powinny zostać uwzględnione w procesie szacowania ryzyka;

- konieczność zastosowania dodatkowych zabezpieczeń powinna wynikać z wyników szacowania ryzyka;

* **NAJCZĘSTSZE BŁĘDY W OPRACOWANEJ DOKUMENTACJI BEZPIECZEŃSTWA SYSTEMU, POD WZGLĘDEM DOBORU AKTÓW NORMATYWNYCH**

- oparcie się na niewłaściwych aktach normatywnych dotyczących np. innych rodzajów informacji niejawnych (narodowych, UE, NATO), materiałów kryptograficznych, itp.;

- wskazanie wykluczających się aktów normatywnych, na podstawie których opracowano dokumentację bezpieczeństwa;

- odwoływanie się do aktów prawnych, które nie mają faktycznego zastosowania dla systemu teleinformatycznego;

* **NAJCZĘSTSZE BŁĘDY W OPRACOWANEJ DOKUMENTACJI BEZPIECZEŃSTWA SYSTEMU**

- niejednoznaczna nazwa systemu;

- brak wskazania przyjętej metody szacowania ryzyka;

- brak ryzyka szczątkowego oraz jego zatwierdzenia przez kierownika jednostki organizacyjnej;

- zamieszczanie informacji niedotyczących bezpieczeństwa systemu teleinformatycznego;

- brak określenia terminu akredytacji w systemach teleinformatycznych przetwarzających informacje niejawne „ZASTRZEŻONE”;

- nie wskazanie miejsca przekazania informatycznych nośników danych (dysków twardych) w momencie zakończenia pracy systemu;

- niekonsekwencje i rozbieżności (np. tryb pracy systemu, wykorzystywanych IND);

- opisy nie odnoszą się do przedmiotowego systemu;

- w przypadku zastosowania urządzeń typu: skaner, urządzenie wielofunkcyjne, należy określić zakres wykorzystania, rodzaj pamięci, minimalną konfigurację (z uwzględnieniem wyłączonych interface-ów), procedury jego użytkowania;

- brak informacji o określonym poziomie zabezpieczenia miejsca PZM (wraz z nr pisma) oraz ewentualnych zmianach mających wpływ na jego ważności;

- dokonywanie samodzielnych zmian w układzie dokumentacji bezpieczeństwa bez wyrażenia zgody Zarządu VI SKW;

- wskazanie niewłaściwego podmiotu przewidzianego do informowania w przypadku problemów ze sprzętem (awariami) posiadającym przyznany certyfikat ochrony elektromagnetycznej (ABW lub SKW);

- zbyt niskie poświadczenie bezpieczeństwa osobowego administratora systemu teleinformatycznego;

- brak informacji o postępowaniu w przypadku przekazania do naprawy lub wycofania elementów systemu (zwłaszcza drukarki) oraz pominięcie problemu wymazywania pamięci ulotnych;

- niewłaściwe postępowanie z nośnikami cyfrowymi wielokrotnego zapisu (typu RW) - brak określenia warunków użycia ww. IND;

- nieprawidłowo określone parametry haseł użytkowników i administratora, niezapewniające właściwy poziomu ochrony (niezgodność z DBBT 803);

- niekompletny spis rodzajów wykorzystywanych IND;

- brak określenia klauzuli tajności nośnika (IND), na którym wykonane będą kopie zapasowe systemu operacyjnego;

- niewłaściwe postępowanie z pamięciami ulotnymi w momencie ich wycofania (brak stosowania specjalistycznego oprogramowania, brak wskazania metody wymazywania);

- niewłaściwe adresowanie pism przewodnich lub odniesienia w treści dokumentacji bezpieczeństwa do nieistniejących instytucji (ZBIN, BBC) zamiast Zarządu VI SKW;

- brak wymaganych załączników: pomocniczej listy kontrolnej, zobrazowania cyfrowego z sumą kontrolną;

- brak uszczegółowienia sposobu przeprowadzenia audytu wewnętrznego (w oparciu np. o wykaz sprzętu i oprogramowania);

- brak zatwierdzenia dokumentacji przez wszystkie osoby funkcyjne (m.in. oficera bezpieczeństwa łączności i informatyki w systemach kryptograficznych);

- brak zbroszurowania lub oprawienia dokumentacji bezpieczeństwa;

* **NAJCZĘSTSZE BŁĘDY W EKSPLOATACJI SYSTEMÓW TELEINFORMATYCZNYCH**

- niewłaściwe postępowanie w przypadku wystąpienia incydentów komputerowych (DEC. 62/DK WOC/MON) oraz informowanie SKW poprzez pełnomocnika w przypadku ujawnienia informacji niejawnych od klauzuli poufne wzwyż);

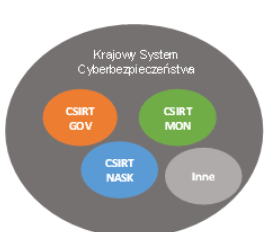
- przetwarzanie informacji niejawnych narodowych w systemach teleinformatycznych międzynarodowych (i odwrotnie), w przypadku, gdy dokumentacja bezpieczeństwa tego nie przewiduje;

- brak podziału na dyski lub partycje dedykowane dla informacji niejawnych międzynarodowych i narodowych;

- brak zarządzania dodatkowym oprogramowaniem, np. SI ETAT (brak hasła aplikacji, ewidencji użytkowników, wyznaczenia dodatkowego administratora itp.).

### Krajowy System Cyberbezpieczeństwa

W tej lekcji przedstawiona zostanie ogólna architektura Krajowego Systemu Cyberbezpieczeństwa. Dowiesz się jakie instytucje biorą udział w obsłudze incydentów oraz jaki jest ich zakres działania.



Ogólne zasady działania oraz architekturę KSC określa „ustawa dnia 5 lipca 2018r.o krajowym systemie cyberbezpieczeństwa” (Dz. U. 2018 poz. 1560). Definicja KSC znajduje się w ww. ustawie w artykule 3:

***Krajowy System Cyberbezpieczeństwa****ma  na  celu  zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów.*

Definicja jest bardzo ogólna, przez co może być niezrozumiała lub źle interpretowana. Wyjaśniając, głównym zadaniem ustawy o KSC jest wskazanie podmiotów wiodących w obszarach cyberprzestrzeni oraz zakresu ich działania i współpracy z pozostałymi podmiotami.

Ustawa określa jakie podmioty wchodzą w skład KSC w artykule 4:

W *skład Krajowego Systemu Cyberbezpieczeństwa wchodzą:*

*1.     operatorzy usług kluczowych,*

*2.     dostawcy usług cyfrowych,*

***3.     CSIRT MON,***

*4.     CSIRT NASK,*

*5.     CSIRT GOV,*

*6.     sektorowe zespoły cyberbezpieczeństwa,*

*7.     jednostki sektora finansów publicznych, o których mowa wart.9 pkt 1–6, 8, 9, 11 i 12 ustawy   
z dnia 27 sierpnia 2009r. o finansach publicznych (Dz.U. z2017r. poz.2077 oraz z 2018r. poz.62, 1000 i 1366),*

*8.     instytuty badawcze,*

*9.     Narodowy Bank Polski,*

*10.  Bank Gospodarstwa Krajowego,*

*11.  Urząd Dozoru Technicznego,*

*12.  Polską Agencję Żeglugi Powietrznej,*

*13.  Polskie Centrum Akredytacji,*

*14.  Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej,*

*15.  spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej  
w rozumieniu art.1ust.2 ustawy z dnia 20grudnia 1996r. o gospodarce komunalnej (Dz.U. z 2017r. poz.827 oraz z 2018 r. poz. 1496),*

*16.  podmioty świadczące usługi z zakresu cyberbezpieczeństwa,*

*17.  organy właściwe do spraw cyberbezpieczeństwa,*

*18.  Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa, zwany dalej „Pojedynczym Punktem Kontaktowym”,*

*19.  Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, zwanego dalej „Pełnomocnikiem,*

*20.  Kolegium do Spraw Cyberbezpieczeństwa, zwane dalej „Kolegium”.*

Najistotniejszymi elementami z punktu widzenia administratora Jednostki Organizacyjnej  
w Ministerstwie Obrony Narodowej są trzy zespoły CSIRT:

1.     CSIRT MON

2.     CSIRT NASK

3.     CSIRT GOV

**Rolę CSIRT MON pełni Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni i dla administratora JO RON jest to najważniejszy element Systemu Cyberbezpieczeństwa RON.**

### System Cyberbezpieczeństwa Resortu Obrony Narodowej

W tej lekcji przedstawiony zostanie System Cyberbezpieczeństwa Resortu Obrony Narodowej. Dowiesz się, jakie elementy(Jednostki Organizacyjne)  wchodzą w jego skład oraz skład poszczególnych zespołów.

Ustawa o Krajowym Systemie Cyberbezpieczeństwa powołała do istnienia CSIRT MON, który współpracując na szczeblu krajowym z pozostałymi podmiotami zapewnia obsługę incydentów.  Kierownictwo Resortu Obrony Narodowej, bazując na ustawie o KSC uwarzyło System Cyberbezpieczeńśtwa Resortu Obrony Narodowej – kory ma zagwarantować wysoki poziom bezpieczeństwa systemów teleinformatycznych, obsługę incydentów oraz budować świadomość  
o istniejących zagrożeniach wśród kadry resortu.

**System Cyberbezpieczeństwa Resortu Obrony Narodowej opisany został w Decyzji 396/NCBC Ministra Obrony Narodowej.**

W skład Systemu Cyberbezpieczeństwa Resortu Obrony Narodowej wchodzą:

1.     CSIRT MON;

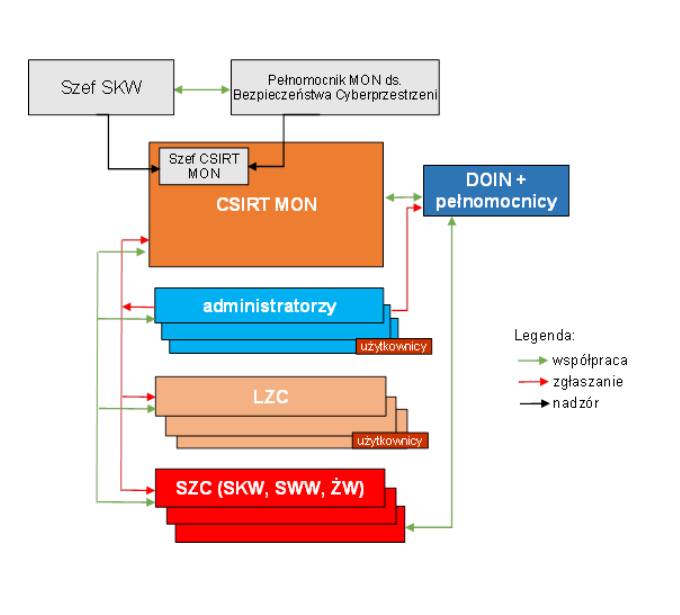
2.     LZC (Lokalne Zespoły Cyberbezpieczeńśtwa) ;

3.     SZC (Samodzielne Zespoły Cyberbezpieczeństwa);

**4.     administratorzy systemów IT RON;**

5.     DOIN (Departament Ochrony Informacji Niejawnych MON) oraz pełnomocnicy ochrony wraz  
z podległymi pionami ochrony;

6.     SKW, SWW, ŻW, OUK (Operator Usługi Kluczowej) oraz jednostki i komórki organizacyjne realizujące zadania z zakresu projektowania, wdrażania, eksploatacji oraz wycofywania systemów IT – w zakresie niezbędnym do zapewnienia bezpieczeństwa systemów IT RON.



LZC tworzone są przez:

a)     organizatorów systemów rozległych oraz funkcjonujących w więcej niż jednej lokalizacji systemów lokalnych, w tym systemów mobilnych (polowych),

b)    organizatorów rozległych systemów wsparcia dowodzenia SZ RP,

c)     jednostki organizacyjne RON świadczące usługi lub realizujące zadania na rzecz organizatorów systemów IT RON,

LZC mogą składać się z oddziałów (zespołów), wydziałów, sekcji lub pojedynczych stanowisk, zwanych dalej „komórkami”:

a)     w zależności od możliwości i potrzeb organizatora systemu,

b)    stosownie do potrzeb wynikających z realizowanych zadań,

c)     z uwzględnieniem liczby systemów IT monitorowanych przez dany LZC, ich złożoności i rozległości,

d)    z uwzględnieniem liczby i złożoności obsługiwanych incydentów.

SZC tworzone są przez SKW, SWW i ŻW, odpowiedzialne za  monitorowanie zagrożeń cyberbezpieczeństwa w organizowanych przez te służby systemach IT oraz za reagowanie na występujące w nich incydenty.

Szef Służby Kontrwywiadu Wojskowego w odniesieniu do Systemu Cyberbezpieczeństwa RON jest właściwy do:

a)     monitorowania zagrożeń w systemach teleinformatycznych wynikających z ustawy o SKW  
i SWW (w szczególności szpiegostwo i przestępstwa przeciwko bezpieczeństwu informacji)

b)    monitorowania zagrożeń w systemach teleinformatycznych związanych ze zdarzeniami  
o charakterze terrorystycznym ( w tym koordynowanie lub obsługa tego typu incydentów)

c)     wspiera działania SC na terytorium Polski

**d)    przedstawia kandydatów na szefa CSIRT**

e)     budowania świadomości w zakresie zagrożeń

Z zapisów tych (Dec. 396/NCBC §8) wynika, że administratorzy systemów zobowiązani są do przekazywania informacji dla przedstawicieli SKW i ściśle z nimi współpracować w odniesieniu do wykrytych incydentów bezpieczeństwa dotyczących zagrożeń terrorystycznych, szpiegostwa czy związanych z systemami niejawnymi, gdyż to SKW jest właściwą komórką (na podstawie ustawy  
o SKW i SWW - Dz.U. 2006 nr 104 poz. 709 [1]) do obsługi incydentów o charakterze szpiegostwa, terrorystycznym czy też związanych z ochroną informacji niejawnych.

Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni jest właściwy do:

a)     określania kierunków rozwoju Systemu Cyberbezpieczeństwa RON

b)    nadzorowania prawidłowego funkcjonowania Systemu Cyberbezpieczeństwa RON

c)     określenia zakresu i obszaru działania Systemu Cyberbezpieczeństwa RON

d)    wskazywania osoby do objęcia stanowiska Szefa CSIRT MON spośród kandydatów przedstawionych przez Szefa SKW

Pełnomocnik zatwierdza więc standardowe procedury operacyjne wykorzystywane w SC RON, współpracuje z Szefem SKW oraz zapewnia odpowiednie warunki funkcjonowania całego Systemu Cyberbrezpieczeństwa RON.

### Zadania CSIRT MON

W tej lekcji przedstawione zostaną główne zadania oraz obszary odpowiedzialności CSIRT MON.  Dowiesz się z kim współpracuje CSIR MON, za co odpowiada i jakie są możliwości działania.

CSIRT MON jako jeden z podmiotów Systemu Cyberbezpieczeństwa Resortu Obrony Narodowej odpowiada za koordynację i obsługę incydentów bezpieczeństwa, szkolenie personelu i budowanie świadomości. Rolę CSIRT MON pełni Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni. Zadania CSIRT MON określone zostały w ustawie o Krajowym Systemie Cyberbezpieczeństwa (omówionym  
w lekcji 1).

W celu zapewnienia właściwego obiegu informacji i zapewnienia odpowiedniego poziomu wiedzy na temat aktualnych zagrożeń CSIRT MON, współpracuje z wieloma podmiotami i instytucjami (również spoza RON). Pozyskana wiedza, informacje są następnie dystrybuowane w RON.

Do głównych zadań CSIRT MON (zgodnie z zapisami ustawy o KSC Dz. U. 2018 poz. 1560, art. 26 pkt. 3) należą:

1.     monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym;

2.     szacowanie ryzyka związanego z ujawnionym zagrożeniem cyberbezpieczeństwa oraz zaistniałymi incydentami, w tym prowadzenie dynamicznej analizy ryzyka;

3.     przekazywanie informacji dotyczących incydentów i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa;

4.     wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa;

5.     reagowanie na zgłoszone incydenty;

6.     klasyfikowanie incydentów, w tym incydentów poważnych oraz incydentów istotnych, jako incydenty krytyczne oraz koordynowanie obsługi incydentów krytycznych;

7.     zmiana klasyfikacji incydentów poważnych i incydentów istotnych;

8.     przekazywanie do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV informacji technicznych dotyczących incydentu, którego koordynacja obsługi wymaga współpracy CSIRT

9.     przeprowadzanie w uzasadnionych przypadkach badania urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić  
w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, oraz składanie wniosków w sprawie rekomendacji dla podmiotów krajowego systemu cyberbezpieczeństwa dotyczących stosowania urządzeń informatycznych lub oprogramowania, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, zwanych dalej „re-komendacjami dotyczącymi stosowania urządzeń informatycznych lub oprogramowania”;

10.  współpraca z sektorowymi zespołami cyberbezpieczeństwa w zakresie koordynowania obsługi incydentów poważnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej, i incydentów krytycznych oraz w zakresie wymiany informacji pozwalających przeciwdziałać zagrożeniom cyberbezpieczeństwa;

11.  przekazywanie do innych państw, w tym państw członkowskich Unii Europejskiej,  
i przyjmowanie z tych państw in-formacji o incydentach poważnych i incydentach istotnych dotyczących dwóch lub większej liczby państw członkowskich, a także przekazywanie do Pojedynczego Punktu Kontaktowego zgłoszenia incydentu poważnego i istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej;

12.  przekazywanie, w terminie do dnia 30 maja każdego roku, do Pojedynczego Punktu Kontaktowego zestawienia zgłoszonych w poprzednim roku kalendarzowym przez operatorów usług kluczowych incydentów poważnych mających wpływ na ciągłość świadczenia przez nich usług kluczowych w Rzeczypospolitej Polskiej oraz ciągłość świadczenia przez nich usług kluczowych w państwach członkowskich Unii Europejskiej, a także zestawienia zgłoszonych  
w poprzednim roku kalendarzowym przez dostawców usług cyfrowych incydentów istotnych,  
 w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej;

13.  wspólne opracowywanie i przekazywanie ministrowi właściwemu do spraw informatyzacji części Raportu o zagrożeniach bezpieczeństwa narodowego, o którym mowa w art.5a ust.1 ustawy z dnia 26 kwietnia 2007r. o zarządzaniu kryzysowym, dotyczącej cyberbezpieczeństwa;

14.  zapewnienie zaplecza analitycznego oraz badawczo-rozwojowego, które w szczególności:

a)     prowadzi zaawansowane analizy złośliwego oprogramowania oraz analizy podatności,

b)    monitoruje wskaźniki zagrożeń cyberbezpieczeństwa,

c)     rozwija narzędzia i metody do wykrywania i zwalczania zagrożeń cyberbezpieczeństwa,

d)    prowadzi analizy i opracowuje standardy, rekomendacje i dobre praktyki w zakresie cyberbezpieczeństwa,

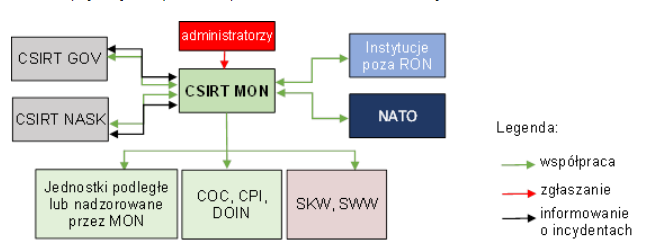
e)     wspiera podmioty krajowego systemu cyberbezpieczeństwa wbudowaniu potencjału  
i zdolności w obszarze cyberbezpieczeństwa,

f)     prowadzi działania z zakresu budowania świadomości w obszarze cyberbezpieczeństwa,

g)    współpracuje w zakresie rozwiązań edukacyjnych w obszarze cyberbezpieczeństwa;

15.  zapewnienie możliwości dokonywania zgłoszeń i przekazywania informacji, o których mowa  
w art.11 ust.1 pkt 4, art.13 ust.1, art.18 ust.1 pkt 4, art.20, art. 22 ust.1 pkt 2, art.24 i art.30 ust.1, oraz udostępnienie i obsługa środków komunikacji pozwalających na dokonywanie tych zgłoszeń;

16.  udział w Sieci CSIRT składającej się z przedstawicieli CSIRT państw członkowskich Unii Europejskiej, CSIRT właściwego dla instytucji Unii Europejskiej, Komisji Europejskiej oraz Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA).



Administratorzy jako jeden z elementów Systemu Cyberbezpieczeństwa RON zgłaszają wykryte incydenty bezpieczeństwa teleinformatycznego do CSIRT MON oraz mogą zwrócić się do Szefa CSIRT o pomoc techniczną w procesie obsługi incydentu.

CSIRT MON odpowiedzialny jest za klasyfikację incydentu, przeprowadzenie analizy kodu oprogramowania złośliwego, budowanie, opracowanie i wdrażanie rozwiązań i narzędzi bezpieczeństwa. Raporty z badań, analiz, wdrożone rozwiązania bezpieczeństwa **są dostępne dla administratorów** systemów, w celach szkoleniowych i poprawy stanu bezpieczeństwa zarządzanych przez nich systemach.

Jako element budowania świadomości, CSIRT MON wydaje biuletyny i komunikaty traktujące o zaobserwowanych zagrożeniach bezpieczeństwa RON, przeprowadza - we współpracy  
z administratorem – testy bezpieczeństwa całych lub wybranych elementów systemów teleinformatycznych.

**Sprawne działanie Systemu Cyberbezpieczeństwa RON, a więc i zapewnienie bezpieczeństwa dla użytkowników i systemów teleinformatycznych w dużej mierze zależy od sprawnego działania administratorów, wdrożeniu przez nich zaleceń i poprawek uczestnictwa  
w dedykowanych szkoleniach.**

### Zadania administratorów w Systemie Cyberbezpieczeństwa RON

W tej lekcji przedstawione zostaną główne zadania administratorów systemów teleinformatycznych i ich rola w Systemie Cyebrbezpieczeństwa Resortu Obrony Narodowej.

Wiedza, umiejętności i doświadczenie administratorów systemów teleinformatycznych jest niezwykle ważne dla zapewnienia bezpieczeństwa w zarządzanych przez nich systemach a także  
w procesie budowania świadomości użytkowników o zagrożeniach dla bezpieczeństwa tych systemów. **Administrator jest jednym z najważniejszych elementów Systemu Cyberbezpieczeństwa RON.**

**Rolą administratora** systemu teleinformatycznego RON oprócz zarządzania systemem jest również **szkolenie użytkowników** odnośnie znanych zagrożeń, właściwego użytkowania systemu teleinformatycznego a także **wdrażanie procedur** mających za zadanie poprawę bezpieczeństwa  
a w przypadku wystąpienia incydentu, ścisła **współpraca** z LZC, IBT lub CSIR MON.

Administratorzy systemów IT w jednostkach organizacyjnych i komórkach organizacyjnych są zobowiązani (**zgodnie z §14 Decyzji nr 396/NCBC MON**) do:

1)   realizacji procedur SC RON w zakresie bezpośredniej i technicznej obsługi incydentów oraz wykonywania doraźnych zaleceń odpowiednio: Dyrektora NCBC (przekazywanych poprzez Szefa CSIRT MON), Szefa CSIRT MON, Szefa LZC lub Szefa SZC w zakresie przeciwdziałania naruszeniom polityk bezpieczeństwa oraz reagowania na incydenty;

2)   wdrożenia, w uzgodnieniu z kierownikiem jednostki (komórki) organizacyjnej, oraz stosowania „Lokalnych Procedur Operacyjnych SC RON” oraz, jeśli to właściwe, procedur ujętych  
w dokumentacji bezpieczeństwa systemów niejawnych;

3)   nadzorowania użytkowników administrowanych systemów IT w zakresie przestrzegania ustalonych procedur bezpieczeństwa;

4)   występowania odpowiednio do Szefa CSIRT MON, Szefa LZC lub Szefa SZC o udzielenie wsparcia technicznego w zakresie obsługi incydentów;

5)   współpracy odpowiednio: z CSIRT MON, LZC lub SZC w zakresie zabezpieczenia śladów  
i ustalenia przyczyn wystąpienia incydentu, w tym zabezpieczania i przekazywania próbek kodu lub innych materiałów umożliwiających przeprowadzenie analiz technicznych,  
z zastrzeżeniem, że w przypadku systemów niejawnych, czynności te realizowane są na zasadach opisanych w dokumentacji bezpieczeństwa danego systemu;

**6)   zgłaszania odpowiednio: do CSIRT MON, LZC lub SZC, a w przypadku systemów niejawnych dodatkowo do IBT, wykrytych incydentów oraz wszelkich zdarzeń mogących wpłynąć na naruszenie polityki bezpieczeństwa w administrowanych przez nich systemach IT.**

Administrator systemów teleinformatycznych monitoruje stan bezpieczeństwa w swoich systemach, informuje użytkowników o wszelkich niepożądanych zdarzeniach mogących obniżyć poziom bezpieczeństwa, uczestniczy w szkoleniach.

**Koordynacja CSIR MON**

W tej lekcji omówiona zostanie koordynacja incydentów bezpieczeństwa przez CSIRT MON. Dowiesz się jakie instytucje, przedsiębiorstwa i jednostki organizacyjne są bezpośrednio podległe  
i nadzorowane przez Ministra Obrony Narodowej.

CSIR MON koordynuje obsługę incydentów zgłaszanych przez(art. 26 pkt. 5 ustawy o KSC):

1.     podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej

2.     przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, w stosunku do których organem organizującym i nadzorującym wykonywanie zadań na rzecz obronności państwa jest Minister Obrony Narodowe

Minister obrony Narodowej, oprócz kierowania jednostkami wojskowymi (za pośrednictwem Szefa Sztabu Generalnego, Dowództw Generalnego, Operacyjnego, Obrony Terytorialnej), nadzoruje również inne podmioty związane z obronnością państwa. Zaliczyć do nich możemy:

1.     Uczelnie wojskowe (WAT, AWL, AL, AMW, ASzW), Liceum Lotnicze w Dęblinie

2.     Agencja Mienia Wojskowego

3.     Wojskowe Instytuty Badawcze (WIŁ, WITPiS, WITU, WICiR, WIML, itp.)

4.     Szpitale wojskowe i przychodnie lekarskie (w tym pracownie psychologiczne)

5.     Wojskowe ordynariaty polowe

6.     Muzea wojskowe, biblioteki wojskowe

"Z uwagi na szczególne znaczenie gospodarczo-obronne niektórych przedsiębiorstw Minister Obrony Narodowej, sprawuje również nadzór nad spółką Exatell S.A. oraz spółkami wchodzącymi w skład Polskiej Grupy Zbrojeniowej, do której należą [m.in](http://m.in/).:

1. Rosmoak S.A
2. Huta Stalowa Wola S.A
3. GZ Stocznia Wojenna sp. z o.o.
4. Polski Holding Obronny sp. z o.o
5. Wojskowe Zakłady Lotnicze Nr 1 S.A. w Łodzi.
6. Wojskowe Zakłady Lotnicze Nr 2 S.A. w Bydgoszczy.
7. Wojskowe Centralne Biuro Konstrukcyjno-Technologiczne S.A. w Warszawie.
8. Wojskowe Zakłady Elektroniczne S.A. w Zielonce.
9. Wojskowe Zakłady Inżynieryjne S.A. w Dęblinie.
10. Wojskowe Biuro Projektów Budowlanych sp. z o.o. w Poznaniu.
11. Ośrodek Badawczo-Rozwojowy Przemysłu Oponiarskiego „STOMIL” sp. z o.o. w Poznaniu.
12. Polski Holding Obronny sp. z o.o. w Warszawie.
13. Stocznia Marynarki Wojennej S.A. w upadłości likwidacyjnej w Gdyni.
14. Wojskowe Zakłady Kartograficzne sp. z o.o. w Warszawie.
15. Zakład Przemysłu Odzieżowego „CORA-TEX” w Krasnymstawie S.A.

CSIRT MON koordynuje proces obsługi zgłaszanych incydentów bezpieczeństwa we wszystkich podległych Ministrowi ON jednostkach organizacyjnych i instytucjach a także przez niego nadzorowanych. Aktualny wykaz podległych Ministrowi ON instytucji i nadzorowanych przez niego znajduje się w Decyzji Ministra Obrony Narodowej Nr 35/MON z dnia 13 kwietnia 2018 r. w sprawie wykazu jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych wraz z ich podporządkowaniem[1].

### Incydent bezpieczeństwa teleinformatycznego

W tej lekcji przedstawione zostanie co to jest incydent bezpieczeństwa teleinformatycznego, co może być uznane za incydent oraz gdzie powinno się zgłaszać incydenty.

**Incydent bezpieczeństwa teleinformatycznego** jest to pojedyncze zdarzenie lub seria zdarzeń, związanych z bezpieczeństwem informacji, które zagrażają ich poufności, dostępności lub integralności. Nie tylko ujawnienie informacji jest incydentem, ale z definicji wynika, że może to być także modyfikacja informacji oraz brak dostępności informacji (zwłaszcza w systemach niejawnych). Brak dostępności informacji może wynikać np. z celowego ale nieuprawnionego ich usunięcia, działania złośliwego oprogramowania, awarii systemu. Incydent dotyczy nie tylko informacji, ale szeroko rozumianych zasobów systemu teleinformatycznego, takich jak: osoby, usługi, oprogramowanie, dane, sprzęt i inne elementy mające wpływ na bezpieczeństwo informacji, a więc dostępności systemu teleinformatycznego również jest incydentem.

Za incydent uznaje się każde niepożądane wydarzenie w systemie teleinformatycznym, którego wynikiem może być:

a)     utrata poufności danych,

b)    uszkodzenie lub utrata danych,

c)     zakłócenie integralności systemu komputerowego,

d)    nieautoryzowane użycie konta innego użytkownika,

e)     nieautoryzowane użycie praw dostępu,

f)     wprowadzenie złośliwych kodów, które niszczą informacje (np. malware[[1]](https://elearning.wp.mil.pl/mod/lesson/view.php?id=19950" \l "_ftn1" \o ")).

Działania jakie powinny zostać podjęte przez administratora w przypadku wykrycia incydentu bezpieczeństwa teleinformatycznego opisuje „Podręcznik reagowania na incydenty komputerowe  
w Resorcie Obrony Narodowej” dostępny w ST MILNET-Z. Do podstawowych działań zaliczyć możemy m.in.:

1.     zarejestrowanie i weryfikacja,

2.     dokonanie wstępnej oceny,

3.     zgłoszenie incydentu do LZC, SBC lub CSIRT MON a w przypadku systemów niejawnych IBT,

4.     przystąpić do działań mających na celu usunięcie skutków incydentu. Administrator może zwrócić się o pomoc techniczną w zakresie obsługi incydentu do Szefa CSIRT MON, Szefa LZC lub Szefa SZC,

5.     współpraca i informowanie LZC, SBC lub CSIRT MON a w przypadku systemów niejawnych IBT.

Szczegółowe informacje na temat koniecznych do podjęcia działań przez administratora zawarte są w „Standardowych Procedurach Operacyjnych Systemu Reagowania na Incydenty Komputerowe  
w Resorcie Obrony Narodowej” dostępne w ST MILNET-Z na stronie CSIRT MON (sbt.ron.int).

**Dokumenty te są aktualizowane i nazwy ich mogą ulec zmianie. Aktualne i obowiązujące wersję tych dokumentów (podręcznik, procedury) dostępne są w ST MILNET-Z na stronie CSIRT MON (sbt.ron.int).**

Kategorie incydentów:

**1. Złośliwe oprogramowanie**

1.1 Oprogramowanie złośliwe w poczcie elektronicznej

1.2 Oprogramowanie złośliwe na stronie WWW

1.3 Oprogramowanie złośliwe na zewnętrznym nośniku danych

1.4 Infekcja systemu operacyjnego

1.5 Klient bootnetu

**2 Przełamywanie zabezpieczeń**

2.1 Próba włamania

2.1.1 Próba nieuprawnionego logowania / włamania na konto

2.1.2 Próba wykorzystania luk w oprogramowaniu

2.1.3 Próba obejścia zabezpieczeń / wykorzystania podatności w urządzeniu

2.2 Włamanie

2.2.1 Nieuprawnione logowanie / włamanie na konto

2.2.2 Włamanie do aplikacji

2.2.3 Obejście zabezpieczeń / wykorzystanie podatności w urządzeniu

2.2.4 Nieuprawnione wykorzystanie zasobów

**3 Niepożądane treści**

3.1 Treści obraźliwe

3.2 Spam

**4 Gromadzenie informacji**

4.1 Skanowanie

4.2 Podsłuch

4.3 Inżynieria społeczna

**5 Dostępność zasobów**

5.1 Atak blokujący (DoS)

5.2 Rozproszony atak blokujący (DDoS)

5.3 Inny sposób ataku / sabotaż

**6 Bezpieczeństwo informacji**

6.1 Nieuprawniony dostęp / wykorzystanie informacji

6.2 Nieuprawniona zmiana informacji

6.3 Naruszenie procedur (świadome, zaniedbanie, brak wiedzy)

6.3.1 Eksploatowanie oprogramowania spoza wykazu programów dopuszczonych do użytkowania

6.3.2 Użytkowanie oprogramowania w wersji posiadającej znane podatności / brak aktualizacji

6.3.3 Błędna konfiguracja urządzenia

**7 Naruszenie przepisów prawa**

7.1 Kopiowanie / rozpowszechnianie plików niezgodnie z przepisami prawa

7.2 Naruszenie praw autorskich

7.3 Pornografia dziecięca

7.4 Przemoc, rasizm, nienawiść

7.5 Cyberterrozryzm

7.6 Cyberszpiegostwo

**8 Inne**

8.1 Awarie (zasilania, łączy, sprzętowe, oprogramowania)

8.2 Pozostałe incydenty komputerowe

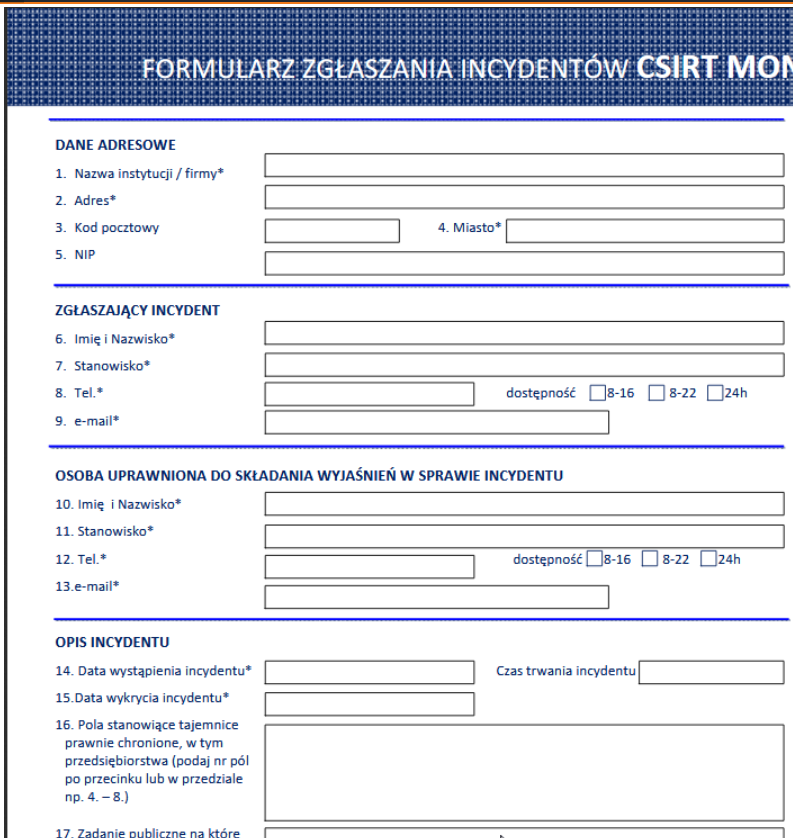
Formularz zgłaszania incydentów bezpieczeństwa teleinformatycznego CSIR MON dostępny jest na stronie www. csirt-mon.wp.mil.pl

**Dane kontaktowe CSIRT MON**

Tel.: +48 261 87 16 41

Email: csirt-mon@ron.mil.pl

www: csirt-mon.wp.mil.pl



[[1]](https://elearning.wp.mil.pl/mod/lesson/view.php?id=19950#_ftnref1) Malware – ogół szkodliwego oprogramowania