

MINISTERSTWO OBRONY NARODOWEJ
INSPEKTORAT SYSTEMÓW INFORMACYJNYCH

ISI/2015



INSTRUKCJA
O GOSPODAROWANIU SPRZĘTEM
INFORMATYKI I OPROGRAMOWANIEM
W RESORCIE OBRONY NARODOWEJ
DU-4.22.3.1

Warszawa
2015



MINISTER OBRONY NARODOWEJ

**DECYZJA Nr 36 /Log./P4
MINISTRA OBRONY NARODOWEJ
z dnia 25 maja 2015 r.**

w sprawie wprowadzenia do użytku „Instrukcji o gospodarowaniu sprzętem informatyki i oprogramowaniem w resorcie obrony narodowej” DU-4.22.3.1

Na podstawie § 1 pkt 8 lit. a, c, d i § 2 pkt 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. Nr 94, poz. 426 i z 2014 r., poz. 933) i § 2 ust. 1 pkt 11 decyzji Nr 435/MON Ministra Obrony Narodowej z dnia 24 grudnia 2013 r. w sprawie określenia funkcji gestorów i centralnych organów logistycznych sprzętu wojskowego w resorcie obrony narodowej (Dz. Urz. MON z 2013 r., poz. 390) oraz decyzji Nr 42/Log./P4 Ministra Obrony Narodowej z dnia 02 lipca 2014 r. w sprawie wprowadzenia w resorcie obrony narodowej „Zasad opracowywania dokumentów logistycznych w resorcie obrony narodowej, DA-04” ustala się, co następuje:

1. Wprowadza się do użytku „Instrukcję o gospodarowaniu sprzętem informatyki i oprogramowaniem w resorcie obrony narodowej” DU-4.22.3.1, stanowiącą załącznik do niniejszej decyzji¹.
2. Decyzja nie dotyczy Służby Wywiadu Wojskowego.
3. Traci moc decyzja Nr 97/MON Ministra Obrony Narodowej z dnia 27 marca 2009 r. (Dz. Urz. MON Nr 6, poz. 74) w sprawie wprowadzenia do użytku „Instrukcji prowadzenia gospodarki materiałowo – technicznej sprzętem informatyki i oprogramowaniem w resorcie obrony narodowej” (sygn. Dep. liT. 1/2009).
4. Decyzja wchodzi w życie po upływie 14 dni od dnia podpisania.

z upoważnienia Ministra Obrony Narodowej



SZEF SZTABU GENERALNEGO WP

Generał Mieczysław GOCUŁ

¹ „Instrukcja o gospodarowaniu sprzętem informatyki i oprogramowaniem w resorcie obrony narodowej” zostanie opublikowana w formie wydawnictwa wojskowego – sygn. ISI/2015.

SPIS TREŚCI

ROZDZIAŁ 1 – WPROWADZENIE

0101. Postanowienia ogólne 7 (1-1)

ROZDZIAŁ 2 – PLANOWANIE I ORGANIZACJA ZAOPATRYWANIA

0201. Określanie potrzeb rzeczowych..... 11 (2-1)

0202. Realizowanie zakupów sprzętu informatyki i oprogramowania..... 16 (2-6)

0203. Zasady dystrybucji sprzętu informatyki i oprogramowania 19 (2-9)

0204. Zasady identyfikacji oprogramowania 23 (2-13)

0205. Zasady zarządzania oprogramowaniem..... 26 (2-16)

0206. Użytkowanie oprogramowania 31 (2-21)

ROZDZIAŁ 3 – EWIDENCJA ILOŚCIOWO-WARTOŚCIOWA ORAZ ILOŚCIOWO-JAKOŚCIOWA SPRZĘTU INFORMATYKI I OPROGRAMOWANIA

0301. Zasady prowadzenia ewidencji ilościowo-wartościowej oraz
ilościowo-jakościowej..... 33 (3-1)

ROZDZIAŁ 4 – EKSPLOATACJA SPRZĘTU INFORMATYKI

0401. Przegląd i naprawa sprzętu informatyki..... 39 (4-1)

ROZDZIAŁ 5 – PRZEKLASYFIKOWANIE I WYBRAKOWANIE

0501. Kategorie klasyfikacyjne sprzętu informatyki i oprogramowania 43 (5-1)

0502. Klasyfikacja..... 44 (5-2)

0503. Wybrakowanie 47 (5-5)

ROZDZIAŁ 6 – INWENTARYZACJA (SPIS Z NATURY)

0601. Inwentaryzacja sprzętu informatyki i oprogramowania 53 (6-1)

ROZDZIAŁ 7 – NADZÓR SŁUŻBOWY

0701. Nadzór służbowy w obszarze gospodarowania sprzętem
informatyki i oprogramowaniem 59 (7-1)

ROZDZIAŁ 8 – SPRAWOZDAWCZOŚĆ

0801. Sprawozdawczość w procesie gospodarowania sprzętem
informatyki i oprogramowaniem 61 (8-1)

ROZDZIAŁ 9 – GOSPODAROWANIE SPRZĘTEM INFORMATYKI I OPROGRAMOWANIEM SYSTEMÓW TELEINFORMATYCZNYCH PRZETWARZAJĄCYCH INFORMACJE NIEJAWNE

0901. Postanowienia ogólne 63 (9-1)

0902. Ewidencja i przekazywanie niejawnych informatycznych
nośników danych 63 (9-1)

0903. Naprawa sprzętu informatyki eksploatowanego w systemach teleinformatycznych przetwarzających informacje niejawne	64 (9-2)
0904. Przechowywanie sprzętu informatyki wykorzystywanego w systemach teleinformatycznych przetwarzających informacje niejawne	66 (9-4)
0905. Wycofywanie sprzętu informatyki eksploatowanego w systemach teleinformatycznych przetwarzających informacje niejawne	66 (9-4)
0906. Deklasyfikacja i wymazywanie danych z informatycznych nośników danych eksploatowanych w systemach teleinformatycznych przetwarzających informacje niejawne	69 (9-7)
0907. Niszczanie informatycznych nośników danych eksploatowanych w systemach teleinformatycznych przetwarzających informacje niejawne	71 (9-9)
0908. Kontrola systemów teleinformatycznych przetwarzających informacje niejawne	74 (9-12)
ROZDZIAŁ 10 – ZAKOŃCZENIE	
1001. Postanowienia końcowe.....	75 (10-1)
ZAŁĄCZNIK A PROTOKÓŁ PRZYJĘCIA-PRZEKAZANIA	77 (A-1)
ZAŁĄCZNIK B ZESTAWIENIE ZBIORCZE O ZREALIZOWANYCH ZAKUPACH SPRZĘTU INFORMATYKI I OPROGRAMOWANIA	79 (B-1)
ZAŁĄCZNIK C PLAN ROZDYSPONOWANIA SPRZĘTU INFORMATYKI I OPROGRAMOWANIA NA ZABEZPIECZENIE POTRZEB WOJSKOWYCH ODDZIAŁÓW GOSPODARCZYCH (W TYM KOMÓREK/JEDNOSTEK ORGANIZACYJNYCH RON POZOSTAJĄCYCH NA ICH ZAOPATRZENIU LOGISTYCZNO-FINANSOWYM	80 (C-1)
ZAŁĄCZNIK D ROZDZIELNIK NA WYDANIE SPRZĘTU INFORMATYKI I OPROGRAMOWANIA	81 (D-1)
ZAŁĄCZNIK E POLECENIE WYDANIA/PRZEKAZANIA SPRZĘTU INFORMATYKI I OPROGRAMOWANIA DLA WOJSKOWEGO ODDZIAŁU GOSPODARCZEGO.....	82 (E-1)
ZAŁĄCZNIK F KARTA SPRZĘTU	83 (F-1)
ZAŁĄCZNIK G WNIOSEK NA OPROGRAMOWANIE	87 (G-1)
ZAŁĄCZNIK H UPOWAŻNIENIE	88 (H-1)
ZAŁĄCZNIK I ARKUSZ ZGŁOSZENIA AWARII.....	89 (I-1)

ZAŁĄCZNIK J CZĘSTOTLIWOŚĆ REALIZACJI PRZEDSIĘWZIĘĆ NADZORCZYCH W ZAKRESIE GOSPODARKI SPRZĘTEM INFORMATYKI I OPROGRAMOWANIEM.....	90 (J-1)
ZAŁĄCZNIK K PROTOKÓŁ WYMAZANIA DANYCH	92 (K-1)
ZAŁĄCZNIK L PROTOKÓŁ ZNISZCZENIA WSTĘPNEGO INFORMATYCZNYCH NOŚNIKÓW DANYCH	93 (L-1)
ZAŁĄCZNIK M PROTOKÓŁ ZNISZCZENIA OSTATECZNEGO INFORMATYCZNYCH NOŚNIKÓW DANYCH NIENISZCZONYCH WSTĘPNIE	94 (M-1)
ZAŁĄCZNIK N PROTOKÓŁ ZNISZCZENIA OSTATECZNEGO INFORMATYCZNYCH NOŚNIKÓW DANYCH ZNISZCZONYCH WSTĘPNIE	95 (N-1)
SŁOWNIK TERMINÓW I DEFINICJI	96 (Słownik-1)
LISTA AKRONIMÓW I SKRÓTÓW	110 (LAIS-1)
WYKAZ DOKUMENTÓW ŹRÓDŁOWYCH	113 (SU-1)
ARKUSZ ZMIAN	116 (SU-4)

„STRONA PUSTA”

ROZDZIAŁ 1 WPROWADZENIE

0101. Postanowienia ogólne

1. Postanowienia niniejszej instrukcji określają zasady prowadzenia gospodarki sprzętem informatyki i oprogramowaniem w resorcie obrony narodowej, a w szczególności planowania i realizacji zakupów, dystrybucji, ewidencji, użytkowania, naprawy sprzętu, przeklasyfikowania i wybrakowania, dla których gestorem sprzętu wojskowego (gestor SpW) jest Inspektorat Systemów Informacyjnych, a centralnym organem logistycznym sprzętu wojskowego (COL SpW) – Szefostwo Eksploatacji Sprzętu Łączności, Informatyki i WE Inspektoratu Wsparcia SZ.
2. Instrukcja stanowi podstawę do działalności organizacyjno-logistycznej w zakresie sprzętu informatyki i oprogramowania dla organów logistycznych, finansowo-księgowych oraz formułowania uregulowań (zasad) w zakresie pozyskiwania, ewidencji, dystrybucji, przeklasyfikowania, użytkowania i wycofywania sprzętu informatyki oraz oprogramowania i stosuje się do:
 - a. gestora SpW;
 - b. COL SpW;
 - c. Organizatorów Systemów Funkcjonalnych (OSF);
 - d. organów planujących oraz dysponentów środków budżetowych odpowiedzialnych za planowanie i gospodarkę sprzętem informatyki i oprogramowaniem;
 - e. komórek organizacyjnych Ministerstwa Obrony Narodowej oraz jednostek organizacyjnych resortu obrony narodowej na rzecz, których są planowane i realizowane zakupy sprzętu informatyki i oprogramowania;
 - f. jednostek organizacyjnych resortu obrony narodowej sprawujących funkcję organów kontrolujących, nadzorujących i koordynujących w odniesieniu do całokształtu przedsięwzięć bezpieczeństwa informatycznego w resorcie obrony narodowej;

- g. organów zaopatrujących w sprzęt informatyki i oprogramowanie – organów wykonawczych terytorialnego systemu zabezpieczenia;
 - h. organów realizujących zakup (pozyskanie) sprzętu informatyki i oprogramowania;
 - i. użytkowników, posiadających na swoim wyposażeniu i ewidencji grupy sprzętu informatyki i oprogramowania wymienione w pkt. 3, sekcji 0101;
 - j. uprawnionych pododdziałów obsługi i naprawy oraz punktów napraw sprzętu informatyki poza potencjałem SZ RP;
 - k. osób funkcyjnych odpowiedzialnych za gospodarowanie sprzętem informatyki i oprogramowaniem.
3. Sprzęt informatyki (w tym sprzęt klasy TEMPEST) i oprogramowanie, o których mowa w pkt. 1, sekcji 0101 ujmuje się w następujące grupy (zakres przedmiotowy):
- a. sprzęt i wyposażenie informatyki:
 - urządzenia komputerowe, w szczególności stacje robocze, serwery, terminale, monitory, notebooki, ultrabooki, tablety,
 - urządzenia peryferyjne, w szczególności drukarki, skanery, plotery, projektory multimedialne, itp.;
 - b. sprzęt i urządzenia sieci komputerowych;
 - c. stacjonarny i mobilny sprzęt i urządzenia wideokonferencji;
 - d. sprzęt i urządzenia ekranujące;
 - e. sprzęt, urządzenia i wyposażenie serwisów kontrolno-pomiarowych dla sprzętu informatyki;
 - f. systemy zasilania bezprzerwowego (UPS) oraz chemiczne źródła zasilania dla sprzętu informatyki;
 - g. kontenery specjalistyczne;
 - h. oprogramowanie (produkty programowe):

- systemy operacyjne,
 - systemy baz danych,
 - pakiety biurowe,
 - środowiska programistyczne i inżynierii oprogramowania,
 - oprogramowanie serwerów usług (np. WWW),
 - zintegrowane systemy informatyczne,
 - oprogramowanie z zakresu bezpieczeństwa informatycznego (np. antywirusowe, firewall, IDS, IPS, itp.),
 - specjalistyczne oprogramowanie dziedzinowe (w tym wspomagające zarządzanie i kierowanie resortem obrony narodowej).
4. Gospodarka sprzętem informatyki i oprogramowaniem w komórkach i jednostkach organizacyjnych resortu obrony narodowej ma na celu:
- a. tworzyć materialne i organizacyjne warunki niezbędne do zapewnienia prawidłowego przebiegu działalności operacyjno-szkoleniowej, logistyczno-finansowej oraz innych form działalności służbowej;
 - b. zapewnić racjonalne wykorzystywanie przydzielonego sprzętu informatyki i oprogramowania;
 - c. odzwierciedlać stan zmian ilościowych, jakościowych i wartościowych sprzętu informatyki i oprogramowania wojskowego oddziału gospodarczego (w tym również jednostki organizacyjnej resortu obrony narodowej pełniącej funkcję wojskowego oddziału gospodarczego), zwanego dalej WOG.
5. Podstawowym zadaniem gospodarki materiałowo-technicznej jest zapewnienie:
- a. właściwego wyposażenia struktur organizacyjno-etatowych resortu obrony narodowej w sprzęt informatyki i oprogramowanie;
 - b. prawidłowego użytkowania, przechowywania i ochrony, prowadzenia kontroli oraz ewidencji sprzętu informatyki i oprogramowania w resorcie obrony narodowej.

6. W celu zapewnienia odpowiedniej jakości oraz kompatybilności nabywanego sprzętu informatyki i oprogramowania, jak też zgodności z realiami rynkowymi, należy przestrzegać zasad określonych w decyzji w sprawie opracowania, wprowadzania i aktualizacji „Wykazu obowiązujących standardów sprzętu informatyki i oprogramowania do stosowania w resorcie obrony narodowej”.
7. W instrukcji określono podstawowe wymagania dotyczące przebiegu procesów cyklu życia sprzętu informatyki i oprogramowania. Instrukcja ustala miejsce i rolę wszystkich uczestników procesów cyklu życia sprzętu informatyki i oprogramowania. Jest przeznaczona do stosowania od chwili identyfikacji potrzeby, aż do wycofania sprzętu informatyki i oprogramowania z eksploatacji w resorcie obrony narodowej.
8. Podstawowe procesy cyklu życia sprzętu informatyki i oprogramowania to: identyfikacja potrzeb, projektowanie i rozwój, produkcja i zakup, wprowadzanie, eksploatacja, wycofanie (w tym dalsze ich zagospodarowanie).

ROZDZIAŁ 2

PLANOWANIE I ORGANIZACJA ZAOPATRYWANIA

0201. Określanie potrzeb rzeczowych

1. Ustalenia zawarte w niniejszym rozdziale normują zasady, organizację, tryb i metody w zakresie planowania i organizowania zaopatrywania w sprzęt informatyki i oprogramowanie w resorcie obrony narodowej, stanowiącymi zasoby określone, jako dział zaopatrzenia 07, poddział 06 planu przydziałów gospodarczych resortu obrony narodowej¹. Planowanie ma na celu sprawne, właściwe pod względem ilościowo-jakościowym oraz terminowe zaspokojenie potrzeb komórek i jednostek organizacyjnych resortu obrony narodowej w sprzęt informatyki i oprogramowanie. Proces ten odbywa się w ramach systemu planowania zasobów, usług i robót budowlanych w resorcie obrony narodowej.
2. Sprzęt informatyki i oprogramowanie na potrzeby komórek i jednostek organizacyjnych resortu obrony narodowej, ze względu na charakterystykę, w tym w szczególności przedmiot zamówienia i przewidywany sposób finansowania, zalicza się do sprzętu powszechnego użytku pozyskiwanego poprzez dostawy realizowane w systemie zakupów scentralizowanych, w ramach realizacji centralnych planów rzeczowych (z wyjątkiem technicznych środków materiałowych oraz materiałów eksploatacyjnych do sprzętu i urządzeń, które są planowane i pozyskiwane przez właściwe WOG w systemie zakupów decentralnych w ramach przydzielonego limitu finansowego).
3. W szczególnie uzasadnionych przypadkach podyktowanych pilną potrzebą organizacyjno-etatową SZ RP, operacyjno-szkoleniową lub logistyczno-finansową, przy braku możliwości zabezpieczenia potrzeby z dostaw realizowanych w systemie scentralizowanym, która z przyczyn obiektywnych nie została zidentyfikowana w procesie planistycznym, gestor SpW może wyrazić zgodę na zakup decentralny przez WOG, pod warunkiem posiadania

¹ Decyzja Nr 57/Log./P4 Ministra Obrony Narodowej z dnia 27 grudnia 2013 roku w sprawie zasad funkcjonowania przydziałów gospodarczych w resorcie obrony narodowej (niepublikowana w Dz. Urz. MON).

przez podmiot wnioskujący limitu środków finansowych oraz przestrzegania zasad określonych w decyzji w sprawie opracowania, wprowadzania i aktualizacji „Wykazu obowiązujących standardów sprzętu informatyki i oprogramowania do stosowania w resorcie obrony narodowej”.

4. Zakupy sprzętu informatyki i oprogramowania na potrzeby Polskich Kontyngentów Wojskowych (PKW), misji pokojowych wydzielonych do realizacji zadań poza granicami kraju oraz polskich przedstawicielstw wojskowych i zespołów łącznikowych przy organizacjach międzynarodowych lub międzynarodowych dowództwach wojskowych i ataszatów obrony przy przedstawicielstwach dyplomatycznych RP poza granicami kraju, **zwanych dalej JW poza granicami kraju**, mogą być realizowane w sposób decentralny, z zachowaniem wymagań określonych przez gestora SpW w „Wykazie obowiązujących standardów sprzętu informatyki i oprogramowania do stosowania w resorcie obrony narodowej”, o których mowa w pkt. 6, sekcji 0101. Ujęcie w planie modernizacji technicznej SZ zadań rzeczowych dotyczących zakupu sprzętu informatyki i oprogramowania odbywa się na zasadach i w trybie określonym w decyzji w sprawie opracowywania i realizacji centralnych planów rzeczowych.
5. Potrzeby w zakresie sprzętu informatyki i oprogramowania określa się w drodze planowania rocznego i wieloletniego przez właściwe organy planujące, biorąc za podstawę potrzeby komórek i jednostek organizacyjnych ustalone zgodnie z pkt. 11, sekcji 0201, aktualny stan posiadania oraz prognozę wybrakowania przed rokiem planistycznym.
6. Potrzeby rzeczowe oraz utrzymywanie ciągłości zaopatrywania komórek i jednostek organizacyjnych resortu obrony narodowej w sprzęt informatyki i oprogramowanie, zabezpiecza się:
 - a. w drodze dostaw planowych – scentralizowanych zakupów dokonywanych przez właściwą jednostkę wsparcia teleinformatycznego resortu obrony narodowej (dysponenta środków budżetu państwa trzeciego stopnia), jak też instytucję centralnie realizującą zadania rzeczowe, w ramach planów modernizacji technicznej SZ, zgodnie z podziałem kompetencji

- określonym w decyzji w sprawie systemu planowania zasobów, usług i robót budowlanych w resorcie obrony narodowej;
- b. z funduszu dyspozycyjnego – naliczanego i utrzymywanego centralnie w organach wykonawczych terytorialnego systemu zabezpieczenia, podporządkowanych IWsp SZ (składach materiałowych RBLog), w wysokości do 1% należności sprzętu informatyki i oprogramowania resortu obrony narodowej, według asortymentu określonego w pkt. 3, sekcji 0101;
 - c. w drodze zakupu doraźnego – dokonywanych przez właściwych dysponentów środków budżetu państwa trzeciego stopnia, na zasadach określonych w pkt. 3 i 4, sekcji 0201.
7. Zasadniczym ogniwem procesu zabezpieczenia potrzeb sprzętu informatyki i oprogramowania jest WOG, uwzględniający potrzeby własne (pododdziałów organicznych) oraz komórek/jednostek organizacyjnych resortu obrony narodowej (pododdziałów gospodarczych) będących na jego zaopatrzeniu logistyczno-finansowym.
 8. Podstawą do przyjęcia jednostek wojskowych nieprowadzących samodzielnej gospodarki materiałowo-finansowej na zaopatrzenie WOG jest plan przydziałów gospodarczych resortu obrony narodowej.
 9. Jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane działające na zasadach własnego rozrachunku gospodarczego, zaopatrują się w sprzęt informatyki i oprogramowanie, o których mowa w pkt. 3, sekcji 0101, we własnym zakresie.
 10. Jednostki organizacyjne resortu obrony narodowej w przypadku przejścia na własny rozrachunek gospodarczy mogą otrzymać będący w ich wyposażeniu sprzęt informatyki i oprogramowanie, jako pierwsze wyposażenie, na zasadach określonych w ustawie o finansach publicznych.
 11. Podstawę do planowania potrzeb sprzętu informatyki i oprogramowania stanowią:
 - a. obowiązujące etaty;

- b. normy (tabele) należności naliczeniowego sprzętu informatyki;
 - c. minimalne normy efektywności wykorzystania;
 - d. programy rozwoju SZ RP wraz z planami pochodnymi (zasadniczymi i uzupełniającymi), zatwierdzone programy operacyjne, programy uzbrojenia, wnioski w sprawie pozyskania nowego SpW (dokumentacji technicznej) dla Sił Zbrojnych RP oraz dokumentacja techniczna;
 - e. dokumenty wynikające z procesu planowania i rozliczania działalności resortu obrony narodowej na rok planistyczny;
 - f. potrzeby związane z zabezpieczeniem:
 - funkcjonujących i wdrażanych systemów informatycznych wspomagających działalność resortu obrony narodowej,
 - działalności operacyjno-szkoleniowo oraz logistyczno-finansowej,
 - automatyzacji prac biurowych,
 - udziału w międzynarodowych misjach pokojowych.
12. Sprzęt i wyposażenie informatyki wymienione w pkt. 3, sekcji 0101 eksploatowane jest według stanu technicznego.
13. Minimalna norma efektywności wykorzystania, stosowana dla celów planowania sukcesywnej wymiany (rotacji) sprzętu informatyki w danej konfiguracji sprzętu oraz oprogramowania systemowego wynosi dla:
- a. stacji roboczych 5 lat;
 - b. urządzeń peryferyjnych 5 lat;
 - c. sprzęt i urządzenia wideokonferencji 5 lat;
 - d. serwerów i terminali 8 lat;
 - e. aktywnych urządzeń sieciowych 10 lat.
14. Dla sprzętu informatyki wymienionego w pkt. 13, sekcji 0201 nie określa się norm eksploatacji sprzętu. Z racji cech techniczno-eksploatacyjnych, w toku bieżącej eksploatacji podlega on tylko obsłudgom (serwisowaniu) oraz

naprawom stosownie do powstałych (niemożliwych do przewidzenia) uszkodzeń i awarii określonych modułów sprzętu lub oprogramowania.

15. Proces planowania potrzeb sprzętu informatyki i oprogramowania rozpoczyna się po wydaniu na wszystkich poziomach kierowania i dowodzenia dokumentów dotyczących planowania działalności na rok planistyczny, co najmniej 18 miesięcy (do 30 czerwca) przed rozpoczęciem roku planistycznego.
16. Planowanie potrzeb sprzętu informatyki i oprogramowania realizowane jest przez wszystkie komórki i jednostki organizacyjne resortu obrony narodowej, z uwzględnieniem zasad i kompetencji określonych w decyzjach Ministra Obrony Narodowej: w sprawie systemu planowania zasobów, usług i robót budowlanych w resorcie obrony narodowej oraz w sprawie zasad opracowywania i realizacji centralnych planów rzeczowych.
17. Szczegółowe zasady definiowania potrzeb sprzętu informatyki i oprogramowania określają wytyczne Szefa Inspektoratu Wsparcia SZ w zakresie szczegółowych zasad definiowania potrzeb w poszczególnych działach zaopatrzenia.
18. Do czasu wdrożenia systemu informatycznego, kierownicy komórek/jednostek organizacyjnych resortu obrony narodowej pełniący funkcję organów planujących drugiego i trzeciego stopnia bezpośrednio podległych organowi planującemu pierwszego stopnia (z wyłączeniem zarządu właściwego w zakresie planowania rzeczowego), określą zakres informacyjny oraz szczegółowe procedury procesu planowania potrzeb, dotyczące właściwych kompetencyjnie obszarów zabezpieczenia, w tym sprzętu informatyki i oprogramowania.
19. W procesie planowania i organizacji zaopatrywania, w pierwszej kolejności należy uwzględnić priorytety określone w dokumentach, o których mowa w pkt. 15, sekcji 0201.

20. Zaopatrywanie w sprzęt informatyki i oprogramowanie dla JW poza granicami kraju realizują w oparciu o ustalone normy należności, stosownie do potrzeb wynikających z ich zadań i przeznaczenia operacyjnego:
- a. właściwe WOG – dla Polskich Kontyngentów Wojskowych (PKW), misji pokojowych wydzielonych do realizacji zadań poza granicami kraju;
 - b. komórka (jednostka) organizacyjna resortu obrony narodowej finansująca pełnienie służby poza granicami państwa – dla polskich przedstawicielstw wojskowych i zespołów łącznikowych przy organizacjach międzynarodowych lub międzynarodowych dowództwach wojskowych i ataszatów obrony przy przedstawicielstwach dyplomatycznych RP poza granicami kraju.

0202. Realizowanie zakupów sprzętu informatyki i oprogramowania

1. Zakupy sprzętu informatyki i oprogramowania, o których mowa w pkt. 3 sekcji 0101, odbywają się w sposób określony w decyzji w sprawie opracowywania i realizacji centralnych planów rzeczowych, przy czym:
 - a. podstawę do realizacji zakupów sprzętu informatyki i oprogramowania stanowi plan modernizacji technicznej SZ zatwierdzony przez Ministra Obrony Narodowej;
 - b. zadania rzeczowe zakwalifikowane do zakupów scentralizowanych realizuje się zgodnie ze szczegółowymi zasadami i kompetencjami określonymi w decyzji w sprawie systemu planowania zasobów, usług i robót budowlanych w resorcie obrony narodowej przez:
 - instytucję centralnie realizującą zadania rzeczowe, określoną przez Ministra Obrony Narodowej w decyzji w sprawie zasad opracowywania i realizacji centralnych planów rzeczowych – plan centralny,
 - jednostkę wsparcia teleinformatycznego resortu obrony narodowej (dysponenta środków budżetu państwa trzeciego stopnia) – plan decentralny (wydatki objęte planem modernizacji technicznej SZ w kwotach zbiorczych).

2. Dostawy sprzętu informatyki i oprogramowania pochodzące z zakupu scentralizowanego dostarczane są do wskazanych RBLog lub kierowane są do bezpośredniego odbioru przez WOG.
3. Zakupiony sprzęt informatyki i oprogramowania w zależności od warunków umowy lub specyfikacji istotnych warunków zamówienia na dostawę mogą być dostarczane:
 - a. jednorazowo, obejmując całość planowanych dostaw;
 - b. etapowo, obejmując określone części planowanych dostaw, w ciągu danego roku budżetowego;
 - c. w cyklu wieloletnim (w ramach umów wieloletnich), rozłożonym na kilkuletnie dostawy sprzętu informatyki i oprogramowania.
4. Proces odbioru sprzętu informatyki i oprogramowania do składów materiałowych RBLog (lub do magazynów WOG oraz JW poza granicami kraju – w przypadku realizacji zakupów w trybie decentralnym) odbywa się na podstawie dowodu dostawy (WZ, faktura, itp.) identyfikującego dostawcę oraz ilość, jakość i wartość sprzętu informatyki i oprogramowania będącego przedmiotem dostawy wraz z załączoną umową, specyfikacją lub specyfikacją istotnych warunków zamówienia.
5. Za wnioskowanie o nadanie JIM dla nowo zakupionego w systemie scentralizowanym sprzętu informatyki i oprogramowania odpowiada gestor SpW (lub WOG oraz komórki/jednostki organizacyjne MON finansujące JW poza granicami kraju – w przypadku zakupów decentralnych, realizowanych na zasadach określonych w pkt. 3 i 4, sekcji 0201).
6. W przypadku sprzętu klasy TEMPEST, wymagane są stosowne certyfikaty ochrony elektromagnetycznej wydane przez ABW lub SKW.
7. Odbioru dostawy sprzętu informatyki i oprogramowania dokonują wyznaczone w tym celu komisje wytypowanych RBLog (lub WOG oraz JW poza granicami kraju – w przypadku realizacji zakupów w trybie decentralnym), składające się minimum z 3 osób (z wyjątkiem JW poza granicami kraju, gdzie skład komisji, – a w szczególności jej ilość – wynika z możliwości osobowych). Członkami

komisji nie mogą być osoby znajdujące się w konflikcie interesów. Odbiór ma na celu ustalenie czy dostarczony sprzęt informatyki i oprogramowanie spełniają warunki umowy, specyfikacji lub specyfikacji istotnych warunków zamówienia oraz opisów zawartym w dowodach dostaw, poprzez:

- a. odbiór ilościowy polegający na sprawdzeniu ilości dostarczonego (odbieranego) sprzętu informatyki i oprogramowania przez ich przeliczenie, w określonych jednostkach miary oraz porównanie z dowodem dostawy lub specyfikacją dostawcy;
 - b. odbiór jakościowy (techniczny) polegający na stwierdzeniu jakości sprzętu informatyki i nośników oprogramowania oraz zgodności wszystkich istotnych ich właściwości z wymaganiami technicznymi podanymi w specyfikacji, specyfikacji istotnych warunków zamówienia, bądź w umowie, a także (jeżeli jest to konieczne) z innymi wymogami i normami.
8. O zrealizowaniu przedmiotu zamówienia przez dostawcę odbiorca informuje organ realizujący nabycie (realizatora zakupu), w sposób oraz w terminie i na zasadach określonych w umowie.
 9. W przypadku stwierdzenia (wykrycia) niedoborów i wad w sprzęcie informatyki i oprogramowaniu, odbiorca odmawia przyjęcia dostawy. Jeśli niedobory i wady zostały ustalone (ujawnione) po rozładunku przedmiotu dostawy, odbiorca może pozostawić sprzęt informatyki i oprogramowanie do dyspozycji dostawcy traktując, jako towar w depozycie. O zaistniałym fakcie niezwłocznie powiadamia pisemnie organ realizujący nabycie oraz gestora SpW i COL SpW. Odbiór sprzętu informatyki i oprogramowania pozostawionego do dyspozycji przez dostawcę powinien nastąpić w
 10. ciągu 7 dni od daty zgłoszenia tego faktu przez realizatora zakupu, pod rygorem obciążenia dostawcy kosztami składowania i przeładunków. Wydanie towaru może nastąpić po pokryciu przez dostawcę ww. kosztów, na podstawie wystawionej przez organ realizujący nabycie faktury VAT.

11. W przypadku braku dostawy sprzętu informatyki i oprogramowania w wymaganym w umowie terminie, odbiorca niezwłocznie powiadamia pisemnie organ realizujący nabycie, który odpowiednio do zapisów umowy nalicza dostawcy należne kary umowne.
12. W sprawach nieuregulowanych umowami w zakresie trybu odbioru sprzętu informatyki i oprogramowania oraz reklamacji z tytułu stwierdzonych wad i braków dostawy, mają zastosowanie przepisy Kodeksu cywilnego oraz innych obowiązujących aktów prawnych dotyczących ogólnych warunków umów sprzedaży oraz dostawy w obrocie pomiędzy podmiotami gospodarczymi.
13. Podstawą do dokonania zaprzychodowania w składzie materiałowym RBLog (lub w magazynie WOG oraz w JW poza granicami kraju – w przypadku realizacji zakupów w trybie decentralnym) jest protokół przyjęcia-przekazania sprzętu informatyki i oprogramowania sporządzony przez wyznaczoną w tym celu komisję.
14. Wzór protokołu przyjęcia-przekazania sprzętu informatyki i oprogramowania przedstawia załącznik A.

0203. Zasady dystrybucji sprzętu informatyki i oprogramowania

1. Protokoły przyjęcia-przekazania sprzętu informatyki i oprogramowania, RBLog (lub WOG) wytypowane do odbioru sprzętu informatyki i oprogramowania, przesyłają do COL SpW i właściwego organu realizującego scentralizowany zakup (nabycie) sprzętu informatyki i oprogramowania, o którym mowa w ppkt. b, pkt. 1, sekcji 0202.
2. Na podstawie informacji zawartej w protokołach przyjęcia-przekazania, COL SpW sporządza zestawienie zbiorcze o zrealizowanych zakupach sprzętu informatyki i oprogramowania w ujęciu ilościowym, które przesyła do gestora SpW celem podjęcia decyzji dotyczącej rozdysponowania zakupionego sprzętu informatyki i oprogramowania. Wzór zestawienia zbiorczego o zrealizowanych zakupach sprzętu informatyki i oprogramowania przedstawia załącznik B.

3. W oparciu o przedstawione przez COL SpW zestawienie o zrealizowanych zakupach, gestor SpW dokonuje analizy oraz podziału sprzętu informatyki i oprogramowania na zabezpieczenie potrzeb zgłoszonych przez jednostki organizacyjne resortu obrony narodowej, wymienione w pkt. 18, sekcji 0201 i opracowuje plan rozdysponowania.
4. Opracowany plan rozdysponowania sprzętu informatyki i oprogramowania gestor SpW przesyła do właściwych jednostek organizacyjnych resortu obrony narodowej, wymienionych w pkt. 18, sekcji 0201, z jednoczesnym poinformowaniem COL SpW. Wzór planu rozdysponowania sprzętu informatyki i oprogramowania przedstawia załącznik C.
5. Na podstawie otrzymanego planu rozdysponowania sprzętu informatyki i oprogramowania, jednostki organizacyjne resortu obrony narodowej, wymienione w pkt. 18, sekcji 0201, wg właściwości i ustalonym w planie rozdysponowania zakresie rzeczowo-ilościowym, przesyłają COL SpW – poprzez gestora SpW – rozdzielniki na wydanie sprzętu informatyki i oprogramowania dla WOG. Wzór rozdzielnika na wydanie sprzętu informatyki i oprogramowania przedstawia załącznik D.
6. W oparciu o przesłane rozdzielniki, COL SpW sporządza i przekazuje do RBLog polecenie wydania/przekazania sprzętu informatyki i oprogramowania dla WOG. Wzór polecenia wydania/przekazania sprzętu informatyki i oprogramowania dla WOG przedstawia załącznik E.
7. Podstawę do wydania sprzętu informatyki i oprogramowania z RBLog stanowi sporządzone przez COL SpW polecenie wydania/przekazania sprzętu i oprogramowania dla WOG.
8. RBLog opracowuje plan zaopatrywania jednostek terytorialnego systemu zabezpieczenia, z jednoczesnym poinformowaniem zainteresowanych WOG o terminie i sposobie odbioru sprzętu informatyki i oprogramowania.
9. Wydawanie sprzętu informatyki i oprogramowania ze składu materiałowego (magazynu) RBLog odbywa się na podstawie dokumentów materiałowo-finansowych uprawniających do wydania sprzętu i oprogramowania oraz

dokonania stosownych zmian w ewidencji ilościowo-wartościowej i ilościowo-jakościowej pionu głównego księgowego i logistyki. Są to dokument WZ (wydanie na zewnątrz) oraz zlecenie-asygnata.

10. Do odbioru sprzętu informatyki i oprogramowania wyznacza się upoważnione osoby przez WOG. Odbierający muszą posiadać pisemne upoważnienie do odbioru sprzętu i oprogramowania, podpisane przez kierownika WOG lub zastępcę kierownika WOG. Podpis musi być potwierdzony odciskiem pieczęci urzędowej WOG.
11. Kierownik magazynu lub osoba wydająca, przed przystąpieniem do wydania sprzętu informatyki i oprogramowania musi sprawdzić:
 - a. tożsamość odbiorcy – na podstawie legitymacji służbowej lub dowodu osobistego;
 - b. upoważnienie do odbioru sprzętu i oprogramowania;
 - c. dostosowanie środka transportowego do przewozu urządzeń komputerowych pod kątem ochrony przed uszkodzeniem, utratą i wpływami warunków atmosferycznych.
12. Urządzenia komputerowe, takie jak: stacje robocze, monitory, notebooki, serwery należy transportować w opakowaniach fabrycznych, zabezpieczających przed zniszczeniem lub stosując w tym celu amortyzację wykonaną z filcu, gumy gąbczastej, itp. Sprzęt informatyki wrażliwy na ładunki elektrostatyczne (w szczególności dyski twarde) powinien być transportowany w przeznaczonych do tego kieszeniach lub opakowaniach antystatycznych.
13. Przekazywanie sprzętu informatyki i oprogramowania powinno odbywać się tylko w miejscu wyznaczonym (np. oddzielne pomieszczenie lub wyznaczona powierzchnia), znajdującym się w kompleksie pomieszczeń magazynowych. W trakcie czynności wydawczo-odbiorczych należy sprawdzić, w obecności wydającego i przyjmującego, ilość i jakość wydawanego (odbieranego) sprzętu i oprogramowania. Szczegółowe zasady przyjmowania, magazynowania i wydawania sprzętu informatyki i oprogramowania, określa w wewnętrznych przepisach lub wytycznych właściwy organ logistyczny.

14. Jeżeli w skład urządzenia wchodzi podzespoły o innej numeracji niż urządzenie zasadnicze, to w dokumencie rozchodowo-przychodowym należy wykazać również numery tych podzespołów.
15. Jeden egzemplarz dokumentu rozchodowo-przychodowego wręcza się odbiorcy wraz z dowodem urządzenia. Pozostałe egzemplarze dokumentu rozsyła się zgodnie z rozdzielnikiem występującym w poleceniu wydania/przekazania sprzętu informatyki i oprogramowania dla WOG. Dowód urządzenia – na sprzęt informatyki podlegający obsłudze (serwisowaniu) oraz naprawom, o którym mowa w ppkt. od a do g, pkt. 3, sekcji 0101 – wytwarzany jest w RBLog lub WOG (w przypadku dostaw bezpośrednich do WOG).
16. Dopuszcza się możliwość stosowania dla sprzętu informatyki zamiast dowodów urządzeń – o których mowa w pkt. 15, sekcji 0203 – kart sprzętu. Wzór „karty sprzętu” oraz zasady dokonywania wpisów, przedstawia załącznik F.
17. Na podstawie wcześniej zgłoszonych potrzeb rzeczowych, WOG dokonuje rozdziału sprzętu informatyki i oprogramowania dla pododdziałów własnych oraz pododdziałów gospodarczych pozostających na jego zaopatrzeniu logistyczno-finansowym, zgodnie z planem przydziałów gospodarczych resortu obrony narodowej, z uwzględnieniem ilości przydzielonego sprzętu informatyki i oprogramowania.
18. Przyjęcie sprzętu informatyki i oprogramowania w pododdziale gospodarczym dokonuje się na podstawie rozkazu (decyzji) kierownika komórki/jednostki organizacyjnej i dokumentu obrotu materiałowo-finansowego WOG.
19. Za organizację odbioru sprzętu informatyki i oprogramowania z WOG oraz sposób jego przydziału dla użytkowników indywidualnych oraz zbiorowych odpowiada kierownik komórki/jednostki organizacyjnej realizującej zadania pododdziału gospodarczego.
20. Odbioru sprzętu informatyki i oprogramowania z WOG przez pododdziały własne oraz pododdziały gospodarcze pozostające na jego zaopatrzeniu

logistyczno-finansowym dokonuje się na zasadach określonych w pkt. 9-14, sekcji 0203.

21. Zasady prowadzenia ewidencji ilościowo-wartościowej i ilościowo-jakościowej sprzętu informatyki i oprogramowania przez WOG określa rozdział 3.

0204. Zasady identyfikacji oprogramowania

1. Oprogramowanie zalicza się do wartości niematerialnych i prawnych. Przez wartości niematerialne i prawne rozumie się, zgodnie z ustawą o rachunkowości, nabyte przez komórkę/jednostkę organizacyjną resortu obrony narodowej prawa majątkowe, zaliczane do aktywów trwałych, nadające się do gospodarczego wykorzystania, o przewidywanym okresie ekonomicznej użyteczności dłuższym niż rok, przeznaczone do używania na potrzeby komórki/jednostki, a w szczególności: autorskie prawa majątkowe, prawa pokrewne, licencje, koncesje.
2. Licencja jest umową uprawniającą do korzystania z oprogramowania przez czas i w sposób określony w umowie licencyjnej, natomiast nie przenosi na nabywcę praw autorskich do programu.
3. Licencja nabyta na okres krótszy niż 12 miesięcy, nie spełnia warunków zakwalifikowania do wartości niematerialnych i prawnych. Jej wartość ujmuje się jednorazowo w kosztach oraz w ewidencji pozabilansowej.
4. Bezpłatne oprogramowanie (licencja), za które nie uiszcza się opłaty na rzecz konkretnego producenta, ogólnie dostępne, może być użytkowane w komórkach/jednostkach organizacyjnych resortu obrony narodowej tylko za zgodą organizatora systemu teleinformatycznego.
5. W resorcie obrony narodowej ze względu na specyfikę działalności i różnorodność zapotrzebowań informacyjnych, oprogramowanie wytwarza się także we własnym zakresie, zgodnie z obowiązującymi przepisami.
6. Prawo majątkowe do oprogramowania wytworzonego przez pracowników/kadrę komórki/jednostki organizacyjnej resortu obrony narodowej w ramach obowiązków służbowych, wynikających ze stosunku pracy/służby należy do komórki/jednostki organizacyjnej, o ile umowa o pracę

nie stanowi inaczej. Komórka/jednostka organizacyjna resortu obrony narodowej nie może go wykazywać w wartościach niematerialnych i prawnych, a wydatki poniesione na jego wytworzenie obciążają koszty okresu, w którym zostały poniesione. Oprogramowanie ujmuje się w ewidencji pozabilansowej (z wyłączeniem oprogramowania wytworzonego na potrzeby administrowania systemami teleinformatycznymi w celu automatyzacji czynności administracyjnych, tj. skryptów administracyjnych).

7. Komórka/jednostka organizacyjna resortu obrony narodowej staje się właścicielem prawa majątkowego wytworzonego przez pracowników wojska/żołnierzy zawodowych oprogramowania na podstawie dodatkowego zlecenia, umowy darowizny, umowy o pracę, tylko wtedy, gdy zgodnie z umową zawartą między pracownikami, a pracodawcą prawo to będzie przeniesione na pracodawcę. W takim przypadku oprogramowanie uznaje się za nabyte i zalicza się do wartości niematerialnych i prawnych komórki/jednostki organizacyjnej.
8. Umowa o przeniesienie praw autorskich majątkowych przenosi na nabywcę prawo do wyłącznego korzystania z danego oprogramowania.
9. Każde eksploatowane oprogramowanie może być doskonalone poprzez modyfikacje (aktualizacje) lub przeprojektowanie, przy czym:
 - a. przeprojektowanie oprogramowania wymaga opracowania założeń projektowych (zadania projektowego) i zrealizowania pełnego lub skróconego cyklu projektowo-wdrożeniowego;
 - b. modyfikacja (aktualizacja) oprogramowania polega na jego dostosowaniu do nowych potrzeb lub zwiększeniu efektów użytkowych, technologicznych, funkcjonalnych, sprawności i niezawodności, jak również uzyskaniu wyższego poziomu bezpieczeństwa informatycznego.
10. Zgodnie z ustawą o rachunkowości wydatki poniesione na modyfikacje (aktualizacje), przeprojektowanie lub zakup prawa do rozwiązywania problemów technicznych z funkcjonowaniem oprogramowania:

- a. nie zwiększają wartości początkowej oprogramowania (wydatki na modyfikację uwzględniane są bezpośrednio w kosztach, w dacie ich poniesienia), jeśli nie została nabyta nowa licencja, baza programu pozostaje ta sama;
 - b. zwiększają wartość oprogramowania (lub sprzętu w przypadku oprogramowania OEM lub oprogramowania typu firmware), jeśli została zawarta nowa umowa licencyjna, a przewidywany okres korzystania z nabytego prawa przekroczy 12 miesięcy – oznacza nabycie nowych składników wartości niematerialnych i prawnych.
11. Do wartości niematerialnych i prawnych nie zalicza się zmodyfikowanego oprogramowania, którego przewidywany okres ekonomicznej użyteczności jest krótszy niż 12 miesięcy.
12. Jednostką organizacyjną resortu obrony narodowej właściwą w zakresie gromadzenia, przechowywania i udostępniania oprogramowania w resorcie obrony narodowej – z wyłączeniem oprogramowania, o którym mowa w pkt. 4, sekcji 0205 – jest komórka wewnętrzna Resortowego Centrum Zarządzania Projektami Informatycznymi (RCZPI) – Biblioteka Teleinformatyczna Resortu Obrony Narodowej zwana dalej Biblioteką.
13. Wszystkie wersje źródłowe oprogramowania (o którym mowa w pkt. 12, sekcji 0204) wraz z dokumentacją użytkową i technologiczną, do których autorskie prawa majątkowe posiada resort obrony narodowej należy przekazywać do Biblioteki.
14. Do podstawowych zadań Biblioteki należy:
- a. gromadzenie, ewidencja i przechowywanie dokumentacji oraz kodów źródłowych oprogramowania, do których autorskie prawa majątkowe przysługują Ministrowi Obrony Narodowej, jako reprezentantowi Skarbu Państwa;
 - b. gromadzenie, ewidencja i przechowywanie oprogramowania deweloperskiego wykorzystywanego do budowy systemów

informatycznych, do którego autorskie prawa majątkowe przysługują Ministrowi Obrony Narodowej, jako reprezentantowi Skarbu Państwa;

- c. gromadzenie oprogramowania komercyjnego zakupionego (centralnie i decentralnie) na potrzeby resortu obrony narodowej;
- d. dystrybucja (użyczenie lub przekazanie) zgromadzonych zasobów oprogramowania komórkom i jednostkom organizacyjnym resortu obrony narodowej, jak też innym podmiotom (organizacjom) spoza resortu ON;
- e. prowadzenie systemu bibliotecznego zasobów oprogramowania i dokumentacji systemów informatycznych resortu obrony narodowej;
- f. bieżąca analiza stanu zasobów Biblioteki oraz przedstawienie do ISI wniosków dotyczących usprawnienia sposobu zarządzania oprogramowaniem;
- g. gromadzenie, ewidencja, klasyfikacja i udostępnianie umów licencyjnych na oprogramowanie zgromadzone w zasobach Biblioteki.

0205. Zasady zarządzania oprogramowaniem

1. Po odebraniu z WOG oprogramowania zakupionego w systemie scentralizowanym, RCZPI wprowadza je do własnej bazy danych ewidencyjnych (pododdziału gospodarczego) i przekazuje do Biblioteki.
2. Biblioteka wprowadza oprogramowanie do systemu bibliotecznego, ujmując niezbędne dane ewidencyjne identyfikujące pozyskany produkt programowy, w tym w szczególności:
 - a. dane dotyczące umowy (m.in. numer umowy, strony umowy, data zawarcia umowy, data realizacji umowy);
 - b. dane dotyczące oprogramowania (m.in. pełna nazwa oprogramowania, oznaczenie wersji, rok produkcji, nazwa producenta, JIM, cena jednostkowa/wartość brutto, liczba licencji, nośników oraz informacja o usłudze);
 - c. dane dotyczące okresu posiadanego wsparcia technicznego na oprogramowanie oraz rejestruje oprogramowanie w serwisie

producenta oprogramowania (o ile producent oprogramowania przewidział taką możliwość).

3. W przypadku realizacji zakupu decentralnego, o którym mowa w pkt. 3, sekcji 0201, WOG realizujący zakup oprogramowania przekazuje pozyskany produkt programowy do właściwego WOG, na którego zaopatrzeniu logistyczno-finansowym znajduje się RCZPI. Po wprowadzeniu oprogramowania do systemu bibliotecznego jest ono użyczane przez Bibliotekę dla użytkownika (komórki/jednostki organizacyjnej) na potrzeby, którego realizowany był zakup.
4. Zasada przekazywania do Biblioteki nie dotyczy oprogramowania:
 - a. zakupionego w ramach licencji OEM (Original Equipment Manufacturer – Producent Oryginalnego Wyposażenia), które jest nierozdzielnie połączone z konkretnym komputerem (lub jego częścią składową), na którym jest ono zainstalowane;
 - b. oprogramowania wbudowanego w sprzęt;
 - c. zabezpieczonego kluczem sprzętowym (lub innym sposobem zabezpieczenia przed kopiowaniem);
 - d. oprogramowania wytworzonego na potrzeby administrowania systemami teleinformatycznymi w celu automatyzacji zadań administracyjnych (skrypty administracyjne).
5. Zabezpieczenie potrzeb komórki/jednostki organizacyjnej resortu obrony narodowej w oprogramowanie przez Bibliotekę może odbywać się poprzez jego użyczenie lub przekazanie.
6. Użyczenie oprogramowania jest zdarzeniem polegającym na jego wydaniu z Biblioteki, do czasowego użytkowania przez:
 - a. komórkę/jednostkę organizacyjną resortu obrony narodowej – użyczenie wewnętrzne;
 - b. inny podmiot (organizację) spoza resortu ON – użyczenie zewnętrzne, zgodnie z odrębnymi przepisami.

7. Użyczenie nie powoduje zmiany w ewidencji ilościowo-wartościowej w WOG, na którego zaopatrzeniu logistyczno-finansowym pozostaje Biblioteka.
8. Przekazanie oprogramowania jest zdarzeniem polegającym na jego wydaniu z Biblioteki do:
 - a. komórki/jednostki organizacyjnej resortu obrony narodowej – przekazanie wewnętrzne;
 - b. innego podmiotu (organizacji) spoza resortu ON – przekazanie zewnętrzne, zgodnie z odrębnymi przepisami.
9. Przekazanie oprogramowania powoduje zmiany w ewidencji ilościowo-wartościowej w WOG, na którego zaopatrzeniu logistyczno-finansowym pozostaje Biblioteka i w WOG właściwym dla danej komórki/jednostki organizacyjnej resortu obrony narodowej.
10. Podstawę przekazania oprogramowania stanowi dokument przychodowo-rozchodowy wystawiony przez WOG, na którego zaopatrzeniu logistyczno-finansowym pozostaje Biblioteka.
11. Proces użyczenia lub przekazania oprogramowania przez Bibliotekę zostaje uruchomiony w wyniku złożenia wniosku przez komórkę/jednostkę organizacyjną resortu obrony narodowej, w uzgodnieniu z właściwym WOG.
12. Wnioski na użyczenie lub przekazanie oprogramowania składane są przez osoby funkcyjne wyznaczone w rozkazie (decyzji) kierownika komórki/jednostki organizacyjnej, jako odpowiedzialne w komórce/jednostce organizacyjnej resortu obrony narodowej za gospodarkę materiałowo-techniczną oprogramowaniem.
13. Zasadniczym sposobem składania wniosku jest właściwie wypełniony formularz elektroniczny Biblioteki. Dopuszcza się złożenie wniosku metodą tradycyjną (papierową) w przypadku braku dostępu do systemu wspierającego funkcjonowanie Biblioteki w sieci teleinformatycznej resortu obrony narodowej (wzór wniosku przedstawia załącznik G).

14. Instytucją właściwą do rozpatrzenia złożonych wniosków, o których mowa w pkt. od 11 do 13, sekcji 0205 jest ISI, który uwzględniając zasoby Biblioteki oraz zasadność zgłoszonej potrzeby, przedstawioną w uzasadnieniu do wniosku, podejmuje decyzję o użyczeniu lub przekazaniu oprogramowania wnioskodawcy.
15. Biblioteka, realizując decyzję ISI, o której mowa w pkt. 14, sekcji 0205:
 - a. użycza oprogramowanie komórce/jednostce organizacyjnej resortu obrony narodowej, udostępniając je drogą elektroniczną lub metodą tradycyjną (przesyłając poprzez kancelarię RCZPI) wraz z dodatkowymi informacjami, w tym o ilości przydzielonych licencji i czasie użytkowania. Informację w tym zakresie przesyła również do WOG, na którego zaopatrzeniu logistyczno-finansowym znajduje się dana komórka/jednostka organizacyjna resortu obrony narodowej;
 - b. przekazuje oprogramowanie na nośniku (np. płyta CD/DVD) poprzez WOG, który jednocześnie dokonuje stosownych zmian w ewidencji ilościowo-wartościowej.
16. Potwierdzeniem dla komórki/jednostki organizacyjnej resortu obrony narodowej prawa do użytkowania oprogramowania uzyskanego w drodze użyczenia jest ewidencja w Systemie Bibliotecznym lub w przypadku użyczenia metodą tradycyjną upoważnienie do eksploatacji oprogramowania wydane przez Komendanta RCZPI (wzór upoważnienia przedstawia załącznik H) zwane dalej upoważnieniem.
17. Ewidencja w Systemie Bibliotecznym lub upoważnienie jest potwierdzeniem legalności oprogramowania.
18. Rezygnacja komórki/jednostki organizacyjnej resortu obrony narodowej z użyczonego oprogramowania odbywa się w drodze wniosku w sposób, o którym mowa w pkt. 13, sekcji 0205. Fakt jego złożenia skutkuje zdjęciem oprogramowania z konta komórki/jednostki organizacyjnej resortu obrony narodowej w Bibliotece i wygaśnięciem upoważnienia.

19. Biblioteka dokonuje bieżącej aktualizacji prowadzonej ewidencji o informacje związane z użyczeniem (lub rezygnacją, zwrotem) lub przekazaniem oprogramowania.
20. W przypadku likwidacji komórki/jednostki organizacyjnej resortu obrony narodowej, WOG, na którego zaopatrzeniu logistyczno-finansowym pozostaje likwidowana komórka/jednostka organizacyjna resortu obrony narodowej, oprogramowanie pozostające na jego ewidencji ilościowo-wartościowej zagospodarowuje na zabezpieczenie potrzeb własnych i zaopatrywanych pododdziałów gospodarczych, zgodnie z planem przydziałów gospodarczych resortu obrony narodowej. Informację o niezagospodarowanym oprogramowaniu przekazuje do Biblioteki.
21. Biblioteka analizuje możliwość wykorzystania niezagospodarowanego oprogramowania w WOG, o którym mowa w pkt. 20, sekcji 0205, w resorcie obrony narodowej. Wynik analizy przedstawia do WOG, wskazując oprogramowanie zakwalifikowane, jako przydatne w resorcie obrony narodowej, które należy przekazać do Biblioteki oraz pozostałe, które należy zagospodarować zgodnie z obowiązującymi przepisami w sprawie gospodarowania niektórymi składnikami mienia Skarbu Państwa będącego we władaniu komórek organizacyjnych Ministerstwa Obrony Narodowej i jednostek podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych.
22. W przypadku likwidacji komórki/jednostki organizacyjnej resortu obrony narodowej, rezygnacja z użyczonego dotychczas oprogramowania następuje na podstawie informacji o jej likwidacji, przekazanej do RCZPI przez właściwego kierownika komórki/jednostki organizacyjnej. Rezygnacja z użyczenia skutkuje ponownym skierowaniem oprogramowania do zasobów pozostających w dyspozycji Biblioteki, które może być wykorzystane do zabezpieczenia potrzeb zgłaszanych przez innych użytkowników (komórki/jednostki organizacyjne resortu obrony narodowej).
23. Szczegółowe zasady funkcjonowania Biblioteki określa jej regulamin.

0206. Użytkowanie oprogramowania

1. W rozległych systemach teleinformatycznych resortu obrony narodowej dozwolone jest użytkowanie oprogramowania wdrożonego przez organizatora systemu teleinformatycznego, którego składniki instalowane są w sposób zautomatyzowany.
2. Oprogramowania instalowanego w sposób zautomatyzowany nie ujmuje się w ewidencji ilościowo-wartościowej i ilościowo-jakościowej komórki/jednostki organizacyjnej resortu obrony narodowej, na rzecz której oprogramowanie zostało zainstalowane. Oprogramowanie pozostaje na ewidencji WOG właściwego dla Biblioteki, odpowiedzialnego za zachowanie warunków licencjonowania, w szczególności ilości zainstalowanych lub użytkowanych kopii oprogramowania.
3. Organizator systemu teleinformatycznego publikuje z wykorzystaniem mechanizmów zaimplementowanych w systemie teleinformatycznym, wykaz oprogramowania zainstalowanego w sposób zautomatyzowany.
4. W każdej komórce/jednostce organizacyjnej resortu obrony narodowej zabronione jest użytkowanie oprogramowania nabytego poza dozwolonym obrotem prawnym. Zabronione jest również użytkowanie oprogramowania w sposób niezgodny z warunkami licencjonowania.
5. Instalowanie kolejnych wersji oprogramowania, w zależności od jego złożoności musi odbywać się pod kontrolą formalnych procedur opracowanych przez gestora SpW, w tym: przygotowania do dystrybucji, testów, przekazywania do właściwego miejsca eksploatacji oraz szkolenia.
6. W przypadku udostępnienia przez producenta nowej wersji oprogramowania, osoba wskazana przez gestora SpW (administrator SI eksploatującego oprogramowanie) przeprowadza i przekazuje do gestora analizę zasadności migracji do nowej wersji z uwzględnieniem:
 - a. konieczności wyeliminowania błędów lub usterek oprogramowania;
 - b. nowych funkcjonalności;

- c. zmian w systemie licencjonowania;
 - d. szacowanego kosztu migracji;
 - e. innych czynników wpływających na eksploatację oprogramowania.
7. Komórki i jednostki organizacyjne resortu obrony narodowej, korzystające z oprogramowania, powinny posiadać potwierdzenie prawa do eksploatacji każdego oprogramowania (w postaci licencji lub potwierdzenia z Biblioteki oprogramowania). Za przechowywanie licencji odpowiada osoba odpowiedzialna za gospodarkę materiałowo-techniczną sprzętem informatyki i oprogramowaniem lub inna osoba wyznaczona przez kierownika komórki/jednostki organizacyjnej. Oryginały licencji oprogramowania użyczanego z Biblioteki pozostają w RCZPI.
8. Nielegalne oprogramowanie, to także piractwo komputerowe związane z nielegalnym posiadaniem, kopiowaniem oraz korzystaniem z kopii programów komputerowych.

ROZDZIAŁ 3

EWIDENCJA ILOŚCIOWO-WARTOŚCIOWA ORAZ ILOŚCIOWO-JAKOŚCIOWA SPRZĘTU INFORMATYKI I OPROGRAMOWANIA

0301. Zasady prowadzenia ewidencji ilościowo-wartościowej oraz ilościowo-jakościowej

1. Przedmiotem ewidencji ilościowo-wartościowej oraz ilościowo-jakościowej opisanej w instrukcji jest sprzęt informatyki i oprogramowanie znajdujące się na wyposażeniu komórek/jednostek organizacyjnych resortu obrony narodowej, ujmowane w urządzeniach ewidencyjno-księgowych WOG, w sposób pozwalający na ustalenie ich ilości, wartości i jakości.
2. Ewidencję sprzętu informatyki i oprogramowania prowadzi się w:
 - a. WOG – w zakresie ilościowo-wartościowym i ilościowo-jakościowym. Prowadzą ją wyznaczone osoby funkcyjne pionu głównego księgowego oraz pionu logistyki, za pododdziały własne (organiczne) oraz zaopatrywane pododdziały gospodarcze. Ewidencją główną jest ewidencja ilościowo-wartościowa pionu głównego księgowego. Prowadzi się ją w oparciu o dokumenty ewidencyjne, zawierające cechy wymagane przez ustawę o rachunkowości, a w szczególności takie jak: ilość i wartość (protokół przyjęcia-przekazania, raport wytwórczości, dowód dostawy, faktura, umowa licencyjna, protokół przeklasyfikowania-wybrakowania, itp.). Ewidencja ilościowo-jakościowa prowadzona w pionie logistyki jest ewidencją pomocniczą. Ewidencja ilościowo-jakościowa powinna odzwierciedlać wszystkie zdarzenia gospodarcze od chwili pozyskania sprzętu do jego wycofania z eksploatacji oraz umożliwiać organom planistycznym, zaopatrującym oraz eksploatującym sprzęt informatyki i oprogramowanie prowadzenie racjonalnych zakupów (dostaw), dystrybucję, przechowywanie oraz serwisowanie (w tym naprawy gwarancyjne, pogwarancyjne, modernizację, modyfikację);

- b. komórce (jednostce) organizacyjnej resortu obrony narodowej finansującej pełnienie służby poza granicami państwa – na zasadach, jak w ppkt. a, pkt. 2, sekcji 0301;
 - c. pododdziałach gospodarczych – bazę danych dotyczącą ewidencji sprzętu informatyki i oprogramowania prowadzą wyznaczone osoby funkcyjne, w zakresie ilościowo-jakościowym, zgodnie z ustaleniami WOG.
3. Ewidencję ilościowo-wartościową oraz ilościowo-jakościową prowadzi się w celu:
- a. ewidencjonowania stanów ilościowych i jakościowych sprzętu informatyki i oprogramowania użytkowanego w resorcie obrony narodowej;
 - b. wyceny zgromadzonych zasobów;
 - c. odzwierciedlenia zmian w zapasach;
 - d. odzwierciedlenia przepływu majątku pomiędzy poszczególnymi elementami struktur organizacyjnych;
 - e. optymalizacji stanu zapasów;
 - f. planowania i racjonalizacji zakupów.
4. Prowadzenie ewidencji sprzętu informatyki i oprogramowania polega na prawnym udokumentowaniu dowodami obrotu materiałowo-finansowego prawidłowości i terminowości zapisów w księgach i kartach ewidencyjnych lub systemach informatycznych wszystkich operacji dotyczących ich wartości, przemieszczenia oraz stanu ilościowego i jakościowego.
5. Zdarzenia gospodarcze w obrocie sprzętem informatyki i oprogramowaniem dzielą się na dwie podstawowe grupy:
- a. zdarzenia zewnętrzne;
 - b. zdarzenia wewnętrzne.
6. Zdarzenia gospodarcze zewnętrzne – obejmują realizację procesów związanych z:

- a. pozyskiwaniem sprzętu informatyki i oprogramowania z otoczenia zewnętrznego WOG (np. z RBLog, z innych WOG, z gospodarki narodowej, z importu) – przyjęcia zewnętrzne;
 - b. dystrybucją sprzętu informatyki i oprogramowania poza WOG (np. do innych WOG) – wydania zewnętrzne.
7. Zdarzenia gospodarcze wewnętrzne – obejmują realizację procesów związanych z przechowywaniem i eksploatacją sprzętu informatyki i oprogramowania oraz zabezpieczeniem procesów operacyjno-szkoleniowych i finansowo-gospodarczych WOG. Są to:
- a. rozchód wewnętrzny;
 - b. przychód wewnętrzny;
 - c. przesunięcie międzymagazynowe;
 - d. przecena;
 - e. przeklasyfikowanie;
 - f. wybrakowanie;
 - g. wytworzenie;
 - h. rozkompletowanie;
 - i. bilans otwarcia;
 - j. rozliczenie inwentaryzacji.
8. Zdarzenia w obrocie sprzętem informatyki i oprogramowaniem podejmowane są na podstawie wcześniej przygotowanych i zaakceptowanych przez właściwych przełożonych dokumentów, do których w szczególności zalicza się:
- a. plan zaopatrywania WOG;
 - b. polecenie wydania/przekazania sprzętu i oprogramowania dla WOG;
 - c. roczny plan zakupów;
 - d. roczny plan zamierzeń;

- e. plan obsługi technicznych.
9. Ewidencja ilościowo-wartościowa oraz ilościowo-jakościowa sprzętu informatyki i oprogramowania w WOG, a także komórki/jednostki organizacyjnej MON finansującej pełnienie służby poza granicami państwa obejmuje: nazwę sprzętu, indeks materiałowy, jednostkę miary, kategorię, ilość egzemplarzy oraz ich numery fabryczne (tylko dla sprzętu informatyki, na który wydano dowód urządzenia/kartę sprzętu), miejsce użytkowania (składowania), wartość początkową sprzętu/oprogramowania oraz wartość dotychczasowego umorzenia.
 10. Sprzęt informatyki stanowiący samodzielny wyrób (produkt) handlowy, np. jednostka centralna, monitor, szafa montażowa, zasilacz UPS, akumulator, itp. ewidencjonuje się, jako oddzielne pozycje.
 11. Sprzęt informatyki, który stanowi samodzielny wyrób (produkt) handlowy, lecz jest integralną częścią SpW (np. aparatowni) ewidencjonuje się, jako cały zestaw (komplet), zgodnie z dokumentem dostawy (zakupu) pod jedną pozycją. Elementy składowe zestawu (kompletu) wyszczególnia się w dowodzie urządzenia/karcie sprzętu. Aktualizacji dowodów urządzeń/kart sprzętu – w zakresie zmian ewidencyjnych, na podstawie dokumentów obrotu materiałowo-finansowego WOG – dokonuje kierownik komórki/jednostki organizacyjnej resortu obrony narodowej lub wyznaczona osoba funkcyjna odpowiedzialna za pododdziałową gospodarkę materiałowo-techniczną sprzętem informatyki. Dokonaną zmianę odnotowuje się w dowodzie urządzenia/karcie sprzętu i potwierdza własnoręcznym, czytelnym podpisem w tej dokumentacji oraz na dokumencie obrotu materiałowo-finansowego fakt wykonania tej czynności.
 12. Wykorzystanie informatycznych nośników danych (IND) do przetwarzania informacji niejawnych, musi być poprzedzone oznakowaniem i ewidencją w kancelarii przez użytkownika, na zasadach określonych w rozdziale 9.
 13. Do prowadzenia ewidencji ilościowo-wartościowej można wykorzystać systemy informatyczne, które spełniają wymogi określone w ustawie

o rachunkowości. Dla ewidencji ilościowo-jakościowej takie systemy informatyczne określa i wprowadza organizator logistycznych systemów informatycznych – IWsp SZ. Systemy oprócz ewidencjonowania sprzętu informatyki i oprogramowania umożliwiają redagowanie dokumentów stanowiących podstawę przyjęcia lub rozchodu składników majątku w ujęciu ilościowo-wartościowym i ilościowo-jakościowym.

14. Zasady prowadzenia ewidencji rzeczowych składników majątkowych, o których mowa w pkt. 3, sekcji 0101 oraz obiegu wszystkich dokumentów wewnętrznych i zewnętrznych mających wpływ na ilość, jakość i wartość sprzętu informatyki i oprogramowania w WOG, regulują szczegółowo:
 - a. w zakresie ilościowo-wartościowym – wewnętrzna „Instrukcja obiegu i kontroli dowodów księgowych WOG”;
 - b. w zakresie ilościowo-jakościowym – wytyczne COL SpW.

„STRONA PUSTA”

ROZDZIAŁ 4

EKSPLOATACJA SPRZĘTU INFORMATYKI

0401. Przegląd i naprawa sprzętu informatyki

1. Instytucją właściwą do określania w resorcie obrony narodowej zasad eksploatacji sprzętu informatyki – na podstawie odrębnych przepisów – jest COL SpW, przy współudziale gestora SpW.
2. Za właściwą organizację procesu eksploatacji sprzętu informatyki odpowiada kierownik komórki/jednostki organizacyjnej resortu obrony narodowej. W tym celu może wyznaczyć osobę funkcyjną do bezpośredniego nadzoru nad prawidłową eksploatacją, prowadzonymi przeglądami i naprawami. Bezpośrednią odpowiedzialność za stan ukończenia, sprawność techniczną, terminową realizację czynności konserwacyjnych i właściwą eksploatację ponosi użytkownik.
3. Przeglądom i konserwacji należy poddawać sprzęt zgodnie z zasadami przewidzianymi w instrukcjach producenta lub warunkami określonymi w gwarancji, które dostawca jest zobowiązany załączyć do każdego egzemplarza wyrobu.
4. Czynności, o których mowa w pkt. 3, sekcji 0401, planuje i realizuje się na szczeblu komórki/jednostki organizacyjnej resortu obrony narodowej, odpowiedzialnej za eksploatację sprzętu informatyki w ramach dni technicznych oraz obsługiwanego rocznego.
5. Decyzję o ujęciu sprzętu informatyki w planach eksploatacji i ewidencji pracy SpW podejmuje kierownik właściwego WOG. Fakt przeprowadzenia czynności w ramach obsługiwanego rocznego i dni technicznych należy odnotować w dokumentacji eksploatacyjnej (dowodzie urządzenia/karcie sprzętu). Zakres i terminy przeprowadzenia tych czynności powinny być zawarte w dokumentacji obsługiwanego rocznego oraz dni technicznych.
6. Nie poddaje się czynnościom obsługiwanego rocznego i dni technicznych sprzętu informatyki pracującego w trybie ciągłym, np. serwery, macierze, jednostki sterujące, itp.

7. Sprzęt informatyki eksploatowany jest według stanu technicznego. Z racji techniczno-eksploatacyjnych cech sprzęt informatyki podlega naprawom (serwisowaniu) stosownie do powstałych (niemożliwych do przewidzenia) uszkodzeń i awarii określonych modułów sprzętu, powstałych w toku bieżącej eksploatacji.
8. Utrzymanie sprawności sprzętu informatyki w resorcie obrony narodowej oparte jest głównie o etatowe warsztaty obsługowo-naprawcze, funkcjonujące w ramach terytorialnego systemu zabezpieczenia.
9. Uzupełniająco, w rejonach obsługowo-naprawczych, w których nie działają wojskowe warsztaty obsługowo-naprawcze, a dowóz do nich jest daleki, niecelowy i nieopłacalny, sprzęt informatyki (z wyjątkiem sprzętu wykorzystywanego do przetwarzania informacji niejawnych, którego naprawa jest określona rozdziale 9) bez lub z wymontowanymi IND, może być przekazywany do cywilnych punktów napraw na ogólnie przyjętych zasadach. Do specjalistycznych warsztatów i punktów napraw poza resortem obrony narodowej przekazywany jest również sprzęt, którego nie można naprawić w warsztatach wojskowych.
10. Sprzęt, urządzenia i wyposażenie informatyki pracujące w jawnych systemach lub sieciach teleinformatycznych podlegają naprawie w okresie gwarancyjnym w zakładzie (warsztacie, serwisie) gwaranta lub upoważnionym przez gwaranta. Po wygaśnięciu gwarancji, napraw dokonuje się w wojskowych warsztatach obsługowo-naprawczych lub w innych zakładach specjalizujących się w dokonywaniu tego typu napraw, wyłonionych zgodnie z ustawą - Prawo zamówień publicznych.
11. Zabrania się użytkownikom rozplombowywania sprzętu informatyki w celu dokonywania samowolnych napraw lub demontowania podzespołów tych urządzeń.
12. Sprzęt informatyki kwalifikuje się do naprawy na podstawie protokołu stanu technicznego (sporządzonego przez komisję wyznaczoną rozkazem/decyzją

kierownika komórki/jednostki organizacyjnej resortu obrony narodowej) lub arkusza zgłoszenia awarii (sporządzonego przez użytkownika – załącznik I).

13. Sprzęt informatyki zakwalifikowany do naprawy przekazuje się do wyspecjalizowanego warsztatu, wskazanego przez WOG.
14. Sprzęt informatyki kierowany do naprawy powinien być w pełni ukompletowany oraz jakości i wartości odpowiadającej rzeczywistemu stanowi technicznemu, opisanemu w protokole stanu technicznego/arkuszu zgłoszenia awarii (z wyjątkiem IND) i posiadać dowód urządzenia/kartę sprzętu oraz inne dokumenty (jeśli takie występują), w zależności od rodzaju sprzętu. Informacje o wymienionych w trakcie naprawy częściach i podzespołach wpisuje kierownik wojskowego warsztatu obsługowo-naprawczego do dowodu urządzenia/karty sprzętu.
15. Sprzęt informatyki kierowany do naprawy pozostaje na ewidencji ilościowo-wartościowej i ilościowo-jakościowej WOG.
16. W przypadku braku możliwości wykonania naprawy sprzętu informatyki przez wojskowy warsztat obsługowo-naprawczy, do protokołu stanu technicznego lub arkusza zgłoszenia awarii należy załączyć dokładną opinię (ekspertyzę) specjalisty wykonującego naprawę, wskazującą na niesprawne elementy (moduły, części, itp.), przyczynę braku możliwości wykonania naprawy oraz propozycję skierowania sprzętu do naprawy w specjalistycznych warsztatach i punktach napraw poza resortem obrony narodowej lub przeklasyfikowania do kategorii V.
17. Dopuszcza się naprawę sprzętu informatyki przez serwis u użytkownika z wykorzystaniem specjalistycznych, ruchomych grup zabezpieczenia technicznego lub serwisowych.
18. Naprawę sprzętu informatyki, z którego niemożliwe jest wymontowanie IND wykonuje się wyłącznie w pomieszczeniach warsztatowych etatowych warsztatów obsługowo-naprawczych, funkcjonujących w ramach terytorialnego systemu zabezpieczenia lub przez firmy spoza resortu obrony

narodowej w miejscu eksploatacji zainstalowanego sprzętu, pod nadzorem użytkownika.

19. Naprawy sprzętu informatyki w serwisie zewnętrznym (poza resortem obrony narodowej) – wyłonionym zgodnie z ustawą Prawo zamówień publicznych – realizuje się zgodnie z procedurą wynikającą z zawartej umowy.

ROZDZIAŁ 5

PRZEKLASYFIKOWANIE I WYBRAKOWANIE

0501. Kategorie klasyfikacyjne sprzętu informatyki i oprogramowania

1. Sprzęt informatyki dzieli się na następujące kategorie klasyfikacyjne:
 - a. kategoria I (100% wartości użytkowych) – sprzęt nowy, nieużywany, bez braków i uszkodzeń, znajdujący się w magazynie;
 - b. kategoria II (od 99% - 50% wartości użytkowych) – sprzęt znajdujący się w użytku lub zwrócony przez użytkownika do magazynu, sprawny technicznie, bez braków i uszkodzeń. Do tej kategorii zalicza się również sprzęt naprawiany oraz sprzęt o przekroczonej normie efektywności wykorzystania, sprawny technicznie;
 - c. kategoria III (od 49% - 25% wartości użytkowych) – sprzęt znajdujący się w magazynie, niesprawny technicznie, przeznaczony do naprawy;
 - d. kategoria V (poniżej 25% wartości użytkowych) sprzęt znajdujący się w magazynie, po upływie normy efektywności wykorzystania, zużyty i niesprawny technicznie, którego naprawa, modyfikacja lub modernizacja jest niecelowa i ekonomicznie niezasadniona. Do tej kategorii zalicza się również sprzęt nieprzydatny w resorcie obrony narodowej zgodnie z jego przeznaczeniem (w tym również przed przekroczeniem normy efektywności wykorzystania), planowany do wybrakowania.
2. Oprogramowanie dzieli się na następujące kategorie klasyfikacyjne:
 - a. kategoria I - nowe oprogramowanie (komercyjne lub wytworzone w resorcie obrony narodowej przy wykorzystaniu oprogramowania narzędziowego), nieużywane, bez braków i uszkodzeń, znajdujące się w magazynie;
 - b. kategoria II - oprogramowanie obecnie eksploatowane lub zastąpione poprawionymi lub nowszymi wersjami, którego przechowywanie (magazynowanie) jest przydatne i celowe;

- c. kategoria V - oprogramowanie, któremu wygasły prawa licencyjne do użytkowania lub oprogramowanie nieprzydatne w resorcie obrony narodowej, przeznaczone do wybrakowania.

0502. Klasyfikacja

1. Klasyfikację sprzętu informatyki i oprogramowania przeprowadza się w celu potwierdzenia lub określenia aktualnej ich wartości użytkowej, stanu technicznego z uwzględnieniem dotychczasowego zużycia oraz w celu określenia dalszej ich przydatności dla potrzeb wojska. Dla poszczególnych kategorii sprzętu, a w szczególności przy ustalaniu szkód w mieniu wojskowym, stosuje się procentową wartość w stosunku do rynkowej ceny detalicznej obowiązującej w momencie ujawnienia szkody.
2. Klasyfikację sprzętu informatyki i oprogramowania przeprowadza się w przypadku:
 - a. dokonywania inwentaryzacji;
 - b. obrotu materiałowo-finansowego zachodzącego w trakcie realizacji zdarzeń gospodarczych w WOG polegających na:
 - przyjmowaniu (odbioru) sprzętu informatyki i oprogramowania pochodzącego z zakupu (scentralizowanego, decentralnego),
 - przekazywaniu sprzętu informatyki i oprogramowania pomiędzy WOG oraz do RBLog,
 - zaopatrywaniu użytkowników w sprzęt informatyki i oprogramowanie,
 - przekazaniu sprzętu przez użytkownika do magazynu;
 - c. przekazywania do (z) naprawy;
 - d. stwierdzenia uszkodzenia lub zużycia sprzętu informatyki i oprogramowania;
 - e. kwalifikowania sprzętu informatyki i oprogramowania do wybrakowania;
 - f. na polecenie (zarządzenie) kierownika WOG lub nadrzędnych organów zaopatrujących.

3. Przeklasyfikowanie sprzętu informatyki i oprogramowania z kategorii I do II następuje z chwilą wydania z magazynu i zaksięgowania dokumentu materiałowo-finansowego wystawionego na ich wydanie.
4. Na sprzęt informatyki zdawany do magazynu sporządza się w pododdziale gospodarczym protokół stanu technicznego. Przyjęcie sprzętu informatyki od użytkowników do magazynu dokonuje magazynier, w kategorii zgodnej z zapisami dokumentu materiałowo-finansowego wystawionego na jego zwrot. Może to być:
 - a. kategoria II, jeżeli sprzęt jest sprawny technicznie, bez braków i uszkodzeń;
 - b. kategoria III, jeżeli przyjmowany od użytkownika sprzęt jest niesprawny technicznie, lecz kwalifikuje się wstępnie do naprawy. W takim przypadku sprzęt ten kierowany jest do warsztatu obsługowo-naprawczego, który dokonuje oceny opłacalności jego naprawy lub proponuje przeklasyfikowanie do kat. V (przeznaczony do wybrakowania). Opinia warsztatu obsługowo-naprawczego powinna być zamieszczona lub załączona do „Protokołu przeklasyfikowania-wybrakowania”;
 - c. kategoria V, jeżeli przyjmowany od użytkownika sprzęt jest zużyty i niesprawny technicznie, a naprawa, modyfikacja lub modernizacja jest niecelowa i ekonomicznie nieuzasadniona.
5. Sprzęt informatyki przyjmowany od użytkowników do magazynu oraz zakwalifikowany na podstawie opinii warsztatu obsługowo-naprawczego do kat. V podlega weryfikacji przez komisję wyznaczoną do przeprowadzenia czynności przeklasyfikowania, która jest uprawniona do wnioskowania o podwyższenie lub obniżenie kategorii sprzętu informatyki.
6. Komisyjnego przeklasyfikowania sprzętu informatyki i oprogramowania dokonuje komisja w składzie, co najmniej trzech osób wyznaczonych rozkazem kierownika WOG, które posiadają odpowiednie kompetencje, wiedzę

- i znajomość w zakresie problematyki związanej ze sprzętem informatyki i oprogramowaniem, zastrzeżeniem pkt. 7, sekcji 0502.
7. Przeklasyfikowania sprzętu informatyki i oprogramowania w JW poza granicami kraju dokonuje komisja powołana przez kierownika komórki/jednostki organizacyjnej MON finansującej pełnienie służby poza granicami państwa. Skład komisji (w tym jej ilość) i kwalifikacje jej członków wynikają z możliwości osobowych JW poza granicami kraju. Dopuszcza się powoływanie do składu komisji pracowników ambasad posiadających wiedzę i znajomość w zakresie problematyki związanej ze sprzętem informatyki i oprogramowaniem. Przeklasyfikowanie sprzętu informatyki i oprogramowania jest realizowane w miejscu funkcjonowania (stacjonowania) JW poza granicami kraju.
 8. Klasyfikację przeprowadza się komisyjnie:
 - a. w okresie inwentaryzacji;
 - b. w okresie bezpośrednio poprzedzającym planowane wybrakowanie sprzętu informatyki i oprogramowania;
 - c. z innych uzasadnionych przyczyn – na polecenie kierownika WOG lub nadrzędnych organów zaopatrujących.
 9. Z przeprowadzonych czynności komisja sporządza protokół przeklasyfikowania i przedstawia go kierownikowi WOG do zatwierdzenia. Zatwierdzony protokół przeklasyfikowania stanowi podstawę dokonania zmian w prowadzonej ewidencji ilościowo-wartościowej i ilościowo-jakościowej WOG.
 10. Protokół przeklasyfikowania sprzętu informatyki i oprogramowania JW poza granicami kraju zatwierdza kierownik komórki (jednostki) organizacyjnej MON finansującej pełnienie służby poza granicami państwa.
 11. Sprzęt nowy (uprzednio nieeksploatowany) podlega przeklasyfikowaniu w przypadku, jeżeli jego stan techniczny uległ obniżeniu wskutek wadliwego lub długotrwałego składowania. Każdy przypadek nieuzasadnionego zużycia bądź obniżenia wartości użytkowych zobowiązuje komisję do wnioskowania

o przeprowadzenie postępowania wyjaśniającego w sprawie szkód w mieniu wojskowym, zgodnie z obowiązującymi przepisami.

12. Przeklasyfikowania sprzętu informatyki wykorzystywanego w niejawnych systemach teleinformatycznych, z którego wymontowano niejawny IND dokonuje się zgodnie z zasadami opisanymi w niniejszym rozdziale instrukcji.

0503. Wybrakowanie

1. Wybrakowanie jest zdarzeniem gospodarczym związanym z wycofaniem z użytkowania (likwidacją) określonych grup sprzętu informatyki i oprogramowania, wymienionych w pkt. 3, sekcji 0101, które utraciły swoje wartości użytkowe, a ich naprawa, modyfikacja lub modernizacja jest niecelowa i ekonomicznie nieuzasadniona.
2. Sprzęt informatyki i oprogramowanie przeznaczone do wybrakowania muszą być uprzednio przeklasyfikowane do kategorii V oraz zdeponowane w oddzielnym pomieszczeniu wraz z niezbędną dokumentacją ewidencyjną.
3. Sprzęt informatyki (z wyłączeniem sprzętu klasy TEMPEST, który wycofuje się z eksploatacji w resorcie obrony narodowej na zasadach określonych w pkt. 4 – 8 sekcji 0905) i oprogramowanie zakwalifikowane do kategorii V może być spisane z ewidencji WOG:
 - a. po przekazaniu do Agencji Mienia Wojskowego (zwanej dalej Agencją), gospodarującej mieniem Skarbu Państwa będącym w trwałym zarządzie jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, a także innym mieniem będącym we władaniu tych jednostek, niewykorzystywanym do realizacji ich zadań;
 - b. po przekazaniu, o którym mowa w pkt. 8, sekcji 0503;
 - c. po wybrakowaniu i przekazaniu do Agencji w formie surowców wtórnych (np. złom użytkowy, odpady elektroniczne i elektryczne);
 - d. po wybrakowaniu i przekazaniu w formie surowców wtórnych (np. złom użytkowy, odpady elektroniczne i elektryczne) do punktów zbiórki (skupów) zgodnie z przepisami kraju urzędowania – tylko w przypadku

mienia Skarbu Państwa wykorzystywanego w polskich przedstawicielstwach wojskowych i polskich zespołach łącznikowych przez żołnierzy pełniących służbę w strukturach NATO i UE oraz ataszatach obrony przy przedstawicielstwach dyplomatycznych RP poza granicami kraju;

4. Przekazaniu poza resort obrony narodowej, w tym do Agencji nie podlegają IND, które należy bezwzględnie wymontować ze sprzętu informatyki.
5. Sprawne IND, które nie były wykorzystywane do przetwarzania informacji niejawnych należy zagospodarować w komórkach/jednostkach organizacyjnych resortu obrony narodowej lub w wojskowych warsztatach obsługowo-naprawczych (RWT, WT), natomiast zbędne i niesprawne podlegają wybrakowaniu na zasadach określonych w niniejszym rozdziale.
6. IND wykorzystywane do przetwarzania informacji niejawnych wycofuje się z eksploatacji w resorcie obrony narodowej na zasadach określonych w rozdziale 9.
7. W uzasadnionych ekonomicznie przypadkach wybrakowanie sprzętu informatyki i oprogramowania może odbywać się w JW poza granicami kraju. Zdemontowane dyski twarde podlegają przekazaniu do kraju, niszczeniu przez komisję powołaną decyzją kierownika komórki (jednostki) organizacyjnej MON finansującej pełnienie służby poza granicami państwa.
8. Dopuszcza się nieodpłatne przekazanie zbędnego sprzętu informatyki (z zachowaniem wyłączeń określonych w pkt. 4, sekcji 0503) i oprogramowania:
 - a. muzeom, państwowym i samorządowym instytucjom kultury, państwowym i samorządowym szkołom publicznym, państwowym szkołom wyższym oraz państwowym wyższym szkołom zawodowym – na cele muzealne, wystawiennicze, kulturalne lub szkoleniowe;
 - b. państwowym jednostkom organizacyjnym, jednostkom samorządu terytorialnego, stowarzyszeniom i fundacjom prowadzącym działalność związaną z obronnością lub bezpieczeństwem państwa – na cele ich działalności statutowej;

- c. organizacjom humanitarnymi instytucjom administracji rządowej poza granicami kraju, zgodnie z obowiązującymi w tym zakresie przepisami.
9. Przy dokonywaniu analiz, dotyczących zagospodarowania zbędnego sprzętu informatyki i oprogramowania, należy kierować się nadrzędną zasadą zagospodarowania tego mienia w innych komórkach/jednostkach organizacyjnych resortu obrony narodowej, na działalność bieżącą lub ukompletowanie zapasów.
10. Wybrakowaniu i spisaniu z ewidencji WOG podlega sprzęt informatyki:
 - a. zdjęty z wyposażenia, przestarzały technicznie i niemający zastosowania w resorcie obrony narodowej;
 - b. wyeksploatowany (zużyty fizycznie), który wypracował ustaloną dla niego minimalną normę efektywności wykorzystania, a jego naprawa, modyfikacja lub modernizacja jest technicznie i ekonomicznie nieopłacalna;
 - c. uszkodzony w następstwie awarii (wypadku), a jego naprawa jest nieopłacalna lub niemożliwa ze względów technicznych.
11. Wybrakowaniu i spisaniu z ewidencji WOG podlega oprogramowanie spełniające jeden z poniższych warunków:
 - a. wygasło prawo licencyjne;
 - b. jest nieprzydatne z uwagi na zmiany technologiczne sprzętu informatyki;
 - c. producent zakończył wsparcie techniczne (nie ma możliwości aktualizacji), co powoduje obniżenie bezpieczeństwa przetwarzanych danych. Fakt obniżenia bezpieczeństwa stwierdza protokolarnie powołana do tego celu komisja.
12. Organizatorem procesu wybrakowania sprzętu informatyki i oprogramowania jest kierownik WOG oraz kierownik komórki (jednostki) organizacyjnej MON finansującej pełnienie służby poza granicami państwa, który powołuje komisję i określa tryb, zakres, miejsce oraz czas rozpoczęcia i zakończenia jej pracy.

13. Wybrakowanie sprzętu informatyki i oprogramowania przeprowadza się raz w roku – w trzecim lub czwartym kwartale roku kalendarzowego – na szczeblu WOG oraz w JW poza granicami kraju, w odniesieniu do sprzętu i oprogramowania będącego na ich ewidencji (z uwzględnieniem komórek i jednostek organizacyjnych resortu obrony narodowej pozostających na zaopatrzeniu logistyczno-finansowym).
14. Wybrakowanie sprzętu informatyki i oprogramowania można prowadzić w trybie doraźnym, jeżeli zaistniały ku temu ważne powody, a w szczególności klęska żywiołowa lub inne zdarzenia losowe (np. rozformowanie komórki/jednostki organizacyjnej, wycofanie z eksploatacji całej grupy sprzętu lub oprogramowania).
15. Wybrakowanie sprzętu informatyki i oprogramowania przeprowadza komisja powołana rozkazem kierownika WOG w składzie co najmniej trzech osób. Do składu komisji nie powołuje się osób bezpośrednio odpowiedzialnych materialnie za sprzęt informatyki i oprogramowanie w WOG.
16. Wybrakowanie sprzętu informatyki i oprogramowania w JW poza granicami kraju dokonuje komisja powołana przez kierownika komórki (jednostki) organizacyjnej MON finansującej pełnienie służby poza granicami państwa. Skład komisji (w tym jej ilość) i kwalifikacje jej członków wynikają z możliwości osobowych tych jednostek. Dopuszcza się powoływanie do składu komisji pracowników ambasad posiadających wiedzę i znajomość w zakresie w zakresie problematyki związanej ze sprzętem informatyki i oprogramowaniem. Wybrakowanie sprzętu i oprogramowania jest realizowane w miejscu funkcjonowania (stacjonowania) JW poza granicami kraju.
17. Nadzór nad prawidłowością pracy komisji sprawuje kierownik WOG oraz kierownik komórki (jednostki) organizacyjnej MON finansującej pełnienie służby poza granicami państwa.
18. Sprzęt informatyki i oprogramowanie zakwalifikowane do wybrakowania przedstawia osoba funkcyjna WOG, odpowiedzialna materialnie za powierzone mienie.

19. Komisja dokonująca wybrakowania sprzętu informatyki i oprogramowania jest zobowiązana:
- a. sprawdzić zgodność przedstawionego sprzętu i oprogramowania z ewidencją WOG, jak również stan wyposażenia i ukończenia sprzętu wyszczególnionego w dokumencie ewidencyjnym;
 - b. dokonać szczegółowego przeglądu sprzętu i oprogramowania, zgodnie z aktualną oceną stanu technicznego i właściwościami eksploatacyjno-użytkowymi;
 - c. zbadać przyczyny wybrakowania sprzętu i oprogramowania. Każdy przypadek przedwczesnego zużycia lub niewłaściwego użytkowania, zobowiązuje komisję do wnioskowania o przeprowadzenie postępowania wyjaśniającego;
 - d. dokonać wybrakowania sprzętu i oprogramowania, poprzez pozbawienie ich cech używalności w sposób uniemożliwiający ich powtórne wykorzystanie, np. poprzez przewiercenie, potłuczenie, zmiżdżenie, pocięcie, połamanie, itp. – z uwzględnieniem postanowień pkt. 20, sekcji 0503.
20. Pozbawienia cech używalności sprzętu informatyki należy dokonywać w taki sposób, aby nie uszkodzić i nie zniszczyć wartości użytkowych tych części lub podzespołów (ukończenia), które mogą być wykorzystane do zabezpieczenia działalności obsługowo-naprawczej. Pozbawiony cech używalności sprzęt informatyki, po przeprowadzonym demontażu sprawnych podzespołów lub części zamiennych, kwalifikuje się jako odpad elektryczny i elektryczny. Uzyskane podzespoły, części zamienne i odpady należy zaewidencjonować. Niezależnie od powyższego w zakresie składników niebezpiecznych należy przestrzegać postanowień ustawy o zużytych sprzęcie elektrycznym i elektronicznym.
21. Z przeprowadzonych czynności komisja sporządza protokół przeklasyfikowania-wybrakowania, który przedstawia kierownikowi WOG oraz kierownikowi komórki (jednostki) organizacyjnej MON finansującej pełnienie

służby poza granicami państwa do zatwierdzenia wraz z wnioskami komisji w sprawie zagospodarowania lub likwidacji wybrakowanego sprzętu informatyki i oprogramowania. Zatwierdzony protokół przeklasyfikowania-wybrakowania stanowi podstawę dokonania zmian w prowadzonej ewidencji ilościowo-wartościowej i ilościowo-jakościowej WOG i określa sposób dalszego postępowania (zagospodarowania) z podzespołami, częściami zamiennymi i odpadami uzyskanymi z wybrakowania.

22. W przypadku braku możliwości zagospodarowania materiałów (urządzeń, podzespołów, złomu użytkowego, odpadów elektronicznych i elektrycznych) uzyskanych z wybrakowanego sprzętu informatyki i oprogramowania w komórkach/jednostkach organizacyjnych resortu obrony narodowej, należy je przechowywać i utrzymywać wraz ze sprzętem zużytym do czasu opracowania przez IWsp SZ planu przekazywania trwale zbędnych rzeczy ruchomych oraz przekazania ich do Agencji, zgodnie z obowiązującymi w tym zakresie przepisami.

ROZDZIAŁ 6

INWENTARYZACJA (SPIS Z NATURY)

0601. Inwentaryzacja sprzętu informatyki i oprogramowania

1. **Inwentaryzacja** jest procesem ustalenia rzeczywistego stanu (spisem z natury) składników majątkowych i źródeł ich pochodzenia. Podstawowym celem inwentaryzacji jest:
 - a. ustalenie rzeczywistego stanu składników majątkowych;
 - b. porównanie stanów ewidencyjnych ze stanem rzeczywistym;
 - c. ustalenie, wyjaśnienie i rozliczenie różnic inwentaryzacyjnych;
 - d. rozliczenie osób materialnie odpowiedzialnych za powierzone mienie (składniki majątkowe);
 - e. doprowadzenie danych ewidencyjnych ksiąg rachunkowych (ewidencji księgowej) do zgodności ze stanem faktycznym, wynikającym ze spisu z natury.
2. Rodzaje, terminy i częstotliwość inwentaryzacji regulują przepisy ustawowe.
3. Zakres prowadzonej inwentaryzacji w WOG, komórce/jednostce organizacyjnej MON finansującej pełnienie służby poza granicami państwa obejmuje pododdziały własne oraz pododdziały gospodarcze (komórki i jednostki organizacyjne) będące na zaopatrzeniu logistyczno-finansowym. Za przygotowanie i przeprowadzenie inwentaryzacji odpowiada kierownik WOG oraz kierownik komórki (jednostki) organizacyjnej MON finansującej pełnienie służby poza granicami państwa.
4. Do przeprowadzenia inwentaryzacji kierownik WOG, kierownik komórki (jednostki) organizacyjnej MON finansującej pełnienie służby poza granicami państwa wyznacza komisję inwentaryzacyjną w składzie zapewniającym terminowe i sprawne jej przeprowadzenie. Przy powoływaniu komisji do przeprowadzenia inwentaryzacji sprzętu i oprogramowania systemów niejawnych obowiązuje wymóg posiadania przez jej członków uprawnień do dostępu do informacji niejawnych zgodnie z wymaganiami zawartymi

w dokumentacji bezpieczeństwa teleinformatycznego danego systemu niejawnego.

5. Powołując komisję inwentaryzacyjną kierownik WOG, kierownik komórki (jednostki) organizacyjnej MON finansującej pełnienie służby poza granicami państwa określa zadania, skład osobowy oraz czas jej działania. Do komisji inwentaryzacyjnej i zespołów spisowych powołuje się osoby posiadające kwalifikacje zawodowe, kompetencje i odpowiednią wiedzę w zakresie problematyki związanej ze sprzętem informatyki i oprogramowania. Jednocześnie do składu komisji nie wyznacza się osób odpowiedzialnych za stan (ilość i jakość) sprzętu i oprogramowania podlegającego spisowi lub osób prowadzących ich ewidencję finansową i materiałową, które nie zapewniają bezstronności dokonania spisu. Przewodniczącym komisji inwentaryzacyjnej powinien być pracownik na stanowisku kierowniczym, jednak nie powinien to być główny księgowy, ani pracownik pionu finansowo-księgowego.
6. Do uprawnień i obowiązków przewodniczącego komisji inwentaryzacyjnej należy:
 - a. wnioskowanie w sprawie zmian i uzupełnień w składzie komisji inwentaryzacyjnej i zespołów spisowych;
 - b. ustalenie zakresu czynności dla członków komisji oraz wyznaczenie zastępcy przewodniczącego spośród członków komisji;
 - c. przeprowadzenie szkolenia członków komisji inwentaryzacyjnej oraz zespołów spisowych;
 - d. organizowanie prac przygotowawczych do inwentaryzacji;
 - e. prowadzenie rozliczenia zespołów spisowych (m.in. z wydanych im druków ścisłego zarachowania);
 - f. stawianie – w uzasadnionych przypadkach – wniosków w sprawie:
 - zmiany terminu inwentaryzacji,
 - przeprowadzenie inwentaryzacji w sposób uproszczony,

- przeprowadzenie spisów uzupełniających lub powtórnych;
 - g. kontrolowanie przygotowań do spisów oraz przebiegu spisów z natury;
 - h. kontrolowanie pod względem formalnym i rachunkowym wypełnionych przez zespoły spisowe arkuszy spisów z natury i innych dokumentów inwentaryzacyjnych;
 - i. zarządzanie – w uzasadnionych przypadkach – przyjęcia lub wydania składników majątku w czasie trwania spisu;
 - j. dopilnowanie terminowego złożenia wyjaśnień w sprawie ewentualnych różnic inwentaryzacyjnych przez osoby odpowiedzialne za ich powstanie;
 - k. ustalenie przyczyn powstania różnic inwentaryzacyjnych i postawienie wniosków w sprawie ich rozliczenia;
 - l. przygotowanie wniosków o wszczęcie postępowania wyjaśniającego w przypadku ujawnienia niedoborów i szkód;
 - m. wnioskowanie w sprawie sposobu zagospodarowania ujawnionych w czasie inwentaryzacji zapasów niepełnowartościowych, zbędnych lub nadmiernych oraz w sprawie usprawnienia gospodarki sprzętem informatyki i oprogramowaniem (w tym gospodarki finansowej składnikami majątku).
7. Do zasadniczych zadań komisji inwentaryzacyjnej należy:
- a. organizacyjne i personalne przygotowanie procesu inwentaryzacji;
 - b. przeprowadzenie i nadzorowanie spisu z natury;
 - c. ostateczne ustalenie, weryfikacja i rozliczenie ewentualnych różnic inwentaryzacyjnych;
 - d. sporządzenie sprawozdania i podsumowanie wyników inwentaryzacji;
 - e. ostateczne skompletowanie dokumentacji inwentaryzacyjnej i przekazanie jej do archiwizacji.
8. Przebieg inwentaryzacji:
- a. wydanie instrukcji inwentaryzacyjnej;

- b. opracowanie planu i harmonogramu inwentaryzacji oraz przeprowadzenie szkolenia z członkami komisji inwentaryzacyjnej, zespołów spisowych oraz osobami sprawującymi nadzór nad gospodarką sprzętem i oprogramowaniem;
- c. pobranie przez członków zespołów spisowych za pokwitowaniem odpowiedniej ilości ponumerowanych i ostemplowanych arkuszy spisowych (druków ścisłego zarachowania);
- d. sprawdzenie, czy sprzęt informatyki i oprogramowanie posiadają oznaczenie umożliwiające ich identyfikację (oznaczenia muszą być zgodne z Jednolitym Indekssem Materiałowym);
- e. sprawdzenie, czy pomieszczenia, w których znajdują się składniki majątku podlegające spisowi z natury są należycie zabezpieczone;
- f. sprawdzenie, czy wyroby o tej samej nazwie, numerze indeksowym i cenie zgromadzone są w jednym miejscu;
- g. sprawdzenie, czy ewidencja prowadzona przez osoby materialnie odpowiedzialne została uzgodniona w urządzeniach ewidencyjno-księgowych na dzień inwentaryzacji lub na koniec ostatniego miesiąca;
- h. sprawdzenie, czy ewidencja inwentaryzowanego sprzętu i oprogramowania została zabezpieczona w sposób uniemożliwiający korzystanie z niej w czasie spisu;
- i. pobranie, przed rozpoczęciem procedur liczenia inwentaryzowanych składników majątkowych, oświadczenia od osoby materialnie odpowiedzialnej, z którego treści wynika, że znajdujące się w rejonie spisowym wyroby zostały prawidłowo udokumentowane, a dokumenty potwierdzające operację przychodu i rozchodu sprzętu i oprogramowania zostały przekazane do właściwych komórek organizacyjnych przed rozpoczęciem spisu;
- j. przeprowadzenie spisu według najlepszej metody i techniki, stosownie do przedmiotu inwentaryzacji, rodzaju i formy – ustalenie ilości i ocena

jakości spisywanych składników, przy czym na oddzielnych arkuszach dokonuje się spisu:

- środków trwałych,
 - rzeczowego majątku obrotowego,
 - składników majątkowych obcych,
 - składników majątkowych niepełnowartościowych, uszkodzonych,
 - środków trwałych niskocennych (ewidencja pozabilansowa);
- k. sporządzenie zestawień inwentaryzacyjnych;
- l. rozliczenie wstępne inwentaryzacji;
- m. weryfikacja i kontrola spisu oraz wycena;
- n. rozliczenie końcowe inwentaryzacji;
- o. skompletowanie dokumentacji, podsumowanie i sprecyzowanie wniosków poinwentaryzacyjnych.
9. Szczegółowe zasady prowadzenia inwentaryzacji reguluje wewnętrzna „Instrukcja inwentaryzacji mienia wojskowego WOG”, uwzględniająca przepisy ustawowe oraz specyfikę funkcjonowania WOG.

„STRONA PUSTA”

ROZDZIAŁ 7 NADZÓR SŁUŻBOWY

0701. Nadzór służbowy w obszarze gospodarowania sprzętem informatyki i oprogramowaniem

1. Nadzór służbowy jest zasadniczą formą działalności kontrolnej w zakresie prowadzenia gospodarki materiałowo-technicznej sprzętem informatyki i oprogramowaniem w WOG oraz w pododdziałach gospodarczych będących na zaopatrzeniu logistyczno-finansowym WOG. Celem nadzoru jest wyeliminowanie nieprawidłowości oraz odstępstw od regulacji prawnych i uregulowań, a w szczególności sprawdzenie:
 - a. zasadności i poprawności zgłaszanych potrzeb rzeczowo-finansowych na sprzęt informatyki i oprogramowanie;
 - b. prawidłowości powierzenia mienia osobom odpowiedzialnym materialnie oraz posiadania wymaganych kwalifikacji specjalistycznych przez te osoby;
 - c. ważności (legalności) dokumentów przychodowo-rozchodowych;
 - d. zgodności zapisów ewidencyjnych z dowodami obrotu materiałowo-finansowego;
 - e. zgodności stanu rzeczywistego sprzętu informatyki i oprogramowania ze stanem ewidencyjnym;
 - f. przestrzeganie zasad magazynowania, konserwacji i wymiany sprzętu;
 - g. stanu magazynów pod względem wyposażenia, przydatności, wykorzystania, zabezpieczenia przeciwpożarowego, przestrzegania przepisów bezpieczeństwa i higieny pracy oraz zabezpieczenia przed włamaniem i kradzieżą;
 - h. zasadności zużycia i rozliczania zużycia materiałów eksploatacyjnych, remontowych i konserwacyjnych;
 - i. celowości i rzeczowości wydawania środków finansowych przeznaczonych na utrzymanie sprzętu informatyki;

- j. zasadności, celowości i racjonalności zlecenia podmiotom zewnętrznym czynności obsługowych, naprawczych i konserwacyjnych.
2. Nadzór służbowy w zakresie prowadzenia gospodarki materiałowo-technicznej sprzętem informatyki i oprogramowaniem w WOG oraz w pododdziałach gospodarczych będących na zaopatrzeniu logistyczno-finansowym WOG przeprowadzają osoby funkcyjne WOG i pododdziału gospodarczego zgodnie z załącznikiem J.
 3. Nadzór służbowy powinien być wykonywany w dniach i godzinach służbowych, w miarę możliwości w sposób, który nie zakłóci normalnego toku pracy jednostki/komórki organizacyjnej resortu obrony narodowej, zgodnie z planem nadzorów.
 4. Wyniki nadzoru służbowego powinny być dokumentowane w protokołach i dokumentach ewidencyjnych wyszczególnionych w załączniku J.
 5. Nadzór służbowy w zakresie gospodarki materiałowo-technicznej sprzętem informatyki i oprogramowaniem w zależności od celu i rodzaju przeprowadzonych czynności oraz kontrolowanego szczebla, powinien mieć odpowiedni stopień szczegółowości, umożliwiający przeprowadzenie właściwej analizy, wyciągnięcie obiektywnych wniosków oraz podanie rzeczowych zaleceń pokontrolnych.
 6. Przełożeni wszystkich szczebli kierowania i dowodzenia SZ RP – osobiście lub poprzez wyznaczone osoby funkcyjne (komisje) – mogą w sposób planowy oraz doraźnie (wg potrzeb) prowadzić nadzór służbowy (kontrolę) gospodarki materiałowo-technicznej sprzętem informatyki i oprogramowania w odniesieniu do podległych/podporządkowanych im komórek/jednostek organizacyjnych resortu obrony narodowej.
 7. Zasady prowadzenia kontroli regulują odrębne przepisy.

ROZDZIAŁ 8 SPRAWOZDAWCZOŚĆ

0801. Sprawozdawczość w procesie gospodarowania sprzętem informatyki i oprogramowaniem

1. Prowadzenie sprawozdawczości procesu gospodarowania sprzętem informatyki i oprogramowaniem ma na celu dostarczenie administratorowi branżowemu systemu sprawozdawczego w dziedzinie informatyki i telekomunikacji informacji o stanie ilościowo-jakościowym zasobów sprzętowo-programowych.
2. System sprawozdawczości obejmuje zespół czynności związanych z opracowywaniem, przekazywaniem, przetwarzaniem i wykorzystywaniem informacji zawartych w dokumentach i urządzeniach ewidencyjno-księgowych w celach planistycznych, rozliczeniowych lub kontrolnych.
3. Sprawozdawczość z gospodarowania sprzętem informatyki i oprogramowaniem realizowana jest na:
 - a. podstawowym szczeblu sprawozdawczym, obejmującym wszystkie komórki i jednostki organizacyjne resortu obrony narodowej użytkujące sprzęt informatyki i oprogramowanie, wykonujące sprawozdania na podstawie własnych materiałów źródłowych (dokumenty i urządzenia ewidencyjno-księgowe), dotyczących wyłącznie danej komórki/jednostki organizacyjnej resortu obrony narodowej;
 - b. resortowym szczeblu sprawozdawczym, obejmującym Inspektorat Systemów Informacyjnych, jako właściwego administratora branżowego systemu sprawozdawczego w dziedzinie informatyki i telekomunikacji.
4. Kierownicy komórek i jednostek organizacyjnych resortu obrony narodowej podstawowego szczebla sprawozdawczego są odpowiedzialni za:
 - a. przestrzeganie zasad funkcjonowania systemu sprawozdawczego;
 - b. realizację sprawozdawczości w ustalonych terminach;

- c. zgłaszanie do właściwego administratora branżowego systemu sprawozdawczego w dziedzinie informatyki i telekomunikacji propozycji zmierzających do racjonalizacji sprawozdawczości.
5. Komórki i jednostki organizacyjne resortu obrony narodowej, o których mowa w ppkt. a, pkt. 3, sekcji 0801, opracowują w terminie do 31 marca roku posprawozdawczego – wg stanu na dzień 31 grudnia roku sprawozdawczego – sprawozdanie w dziedzinie informatyki i telekomunikacji, zgodnie z wzorami sprawozdań określonymi w „Zestawieniu sprawozdań obowiązujących na poszczególnych szczeblach dowodzenia i zarządzania resortu obrony narodowej”.
 6. Informacje sprawozdawcze opracowuje się i przedstawia w formie zapewniającej ich informatyczne przetwarzanie, a także umożliwiającą budowę oraz aktualizowanie komputerowej bazy danych branżowych.
 7. W przypadkach uzasadnionych koniecznością jednorazowego lub doraźnego uzyskania informacji sprawozdawczych, które nie zostały wyszczególnione w „Zestawieniu sprawozdań obowiązujących na poszczególnych szczeblach dowodzenia i zarządzania resortu obrony narodowej”, decyzję o sposobie, zakresie i terminie przesłania informacji sprawozdawczej podejmuje administrator branżowy systemu sprawozdawczego w dziedzinie informatyki i telekomunikacji.
 8. Podstawowym źródłem danych na potrzeby sprawozdawczości jest prowadzona w WOG oraz komórce (jednostce) organizacyjnej MON finansującej pełnienie służby poza granicami państwa, ewidencja ilościowo-wartościowa oraz ilościowo-jakościowa sprzętu informatyki i oprogramowania, która powinna umożliwiać identyfikowanie sprzętu według typu, rodzaju, producenta, kategorii, wartości i miejsca użytkowania.

ROZDZIAŁ 9

GOSPODAROWANIE SPRZĘTEM INFORMATYKI I OPROGRAMOWANIEM SYSTEMÓW TELEINFORMATYCZNYCH PRZETWARZAJĄCYCH INFORMACJE NIEJAWNE

0901. Postanowienia ogólne

1. Sprzęt informatyki oraz oprogramowanie wykorzystywane w systemach teleinformatycznych, w których są przetwarzane informacje niejawne podlegają ogólnym zasadom gospodarki materiałowo-finansowej, w tym ewidencji ilościowo-wartościowej oraz ilościowo-jakościowej.
2. Ilekroć w instrukcji mówi się o niejawnych IND należy przez to rozumieć także IND zawierające informacje niejawne międzynarodowe, NATO lub Unii Europejskiej o odpowiedniej klauzuli tajności.
3. Niejawne IND podlegają dodatkowym procedurom w zakresie ewidencji, przechowywania, wycofywania z eksploatacji, opisanym w kolejnych sekcjach niniejszego rozdziału oraz dodatkowo określone są w dokumentacji bezpieczeństwa systemu teleinformatycznego.
4. IND wycofane z eksploatacji w resorcie obrony narodowej nie podlegają przekazaniu poza resort obrony narodowej, bez względu na ich kategorię klasyfikacyjną, wartość finansową czy klauzulę tajności.
5. Zasady prowadzenia gospodarki sprzętem informatyki i oprogramowaniem stanowiącym urządzenia lub narzędzia kryptograficzne regulują odrębne przepisy.

0902. Ewidencja i przekazywanie niejawnych informatycznych nośników danych

1. IND przeznaczone do przetwarzania informacji niejawnych traktuje się jak materiały niejawne. Podlegają one ewidencji w kancelarii poprzez wpisanie w kolumnie 5 Rejestru Wydanych Przedmiotów (RWP) rodzaju, nazwy producenta, modelu, pojemności oraz jeśli jest to możliwe numeru fabrycznego IND.

2. Oznaczanie niejawnych IND następuje zgodnie z obowiązującymi przepisami. W przypadku, gdy niemożliwe jest oznakowanie IND zamontowanego w zestawie lub urządzeniu, to ewidencji i oznakowaniu podlega cały zestaw (np. jednostka centralna, urządzenie).
3. Podwyższenie klauzuli tajności IND może nastąpić na każdym etapie jego użytkowania.
4. Przekazywanie niejawnych IND odbywa się na takich samych zasadach jak innych materiałów niejawnych.

0903. Naprawa, modyfikacja lub modernizacja sprzętu informatyki eksploatowanego systemach teleinformatycznych przetwarzających informacje niejawne

1. Naprawę, modyfikację lub modernizację sprzętu informatyki eksploatowanego w systemach teleinformatycznych przetwarzających informacje niejawne (z zastrzeżeniem pkt 3, sekcji 0903) organizuje się według postanowień określonych w niniejszym rozdziale, jeżeli dokumentacja bezpieczeństwa systemu teleinformatycznego nie stanowi inaczej.
2. Sprzęt informatyki przekazywany jest do naprawy, modyfikacji lub modernizacji po wymontowaniu IND oraz po wymazaniu danych z układów pamięciowych urządzenia, realizowanym zgodnie z dokumentacją bezpieczeństwa systemu teleinformatycznego.
3. Naprawę, modyfikację lub modernizację sprzętu informatyki, z którego wymontowanie niejawnych IND jest niemożliwe, wykonuje się wyłącznie w miejscu zainstalowania/użytkowania urządzenia, zgodnie z dokumentacją bezpieczeństwa systemu teleinformatycznego.
W szczególnie uzasadnionych przypadkach, w uzgodnieniu z SKW, naprawa sprzętu może być wykonana w wojskowych warsztatach lub firmach spoza resortu obrony narodowej, po weryfikacji zdolności warsztatów/firm oraz ich procedur w zakresie ochrony informacji niejawnych.
4. Naprawa, modyfikacja lub modernizacja sprzętu informatyki klasy TEPMEST może być realizowana przez podmioty zewnętrzne posiadające stosowną

koncesję na wytwarzanie i obrót wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym, określonymi w WT XI Załącznika nr 2 Rozporządzenia Rady Ministrów z dnia 3 grudnia 2001 r. w sprawie rodzajów broni i amunicji oraz wykazu wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym, na których wytwarzanie lub obrót jest wymagana koncesja (Dz. U. Nr 145, poz. 1625 z późn. zm.). Wybór podmiotu serwisującego nie może naruszać zapisów umów z producentem lub jego krajowym przedstawicielem.

5. Sprzęt informatyki klasy TEMPEST, po przeprowadzonej naprawie, modyfikacji lub modernizacji podlega ponownej certyfikacji lub specjalistycznym badaniom potwierdzającym utrzymanie właściwych parametrów ochrony elektromagnetycznej, zgodnie z zapisami zawartymi w warunkach ważności certyfikatów ochrony elektromagnetycznej wydanych dla tego sprzętu.
6. Informacja o skierowaniu sprzętu informatyki klasy TEMPEST do naprawy pogwarancyjnej, modyfikacji lub modernizacji wraz z wnioskiem o przeprowadzenie badań potwierdzających utrzymanie ważności certyfikatu ochrony elektromagnetycznej przesyłana jest do organu sprawującego nadzór nad tym certyfikatem.
7. Po naprawie pogwarancyjnej, modyfikacji lub modernizacji sprzętu klasy TEMPEST posiadającego certyfikat ochrony elektromagnetycznej wydany przez SKW, kopia Protokołu z Usługi Serwisowej powinna być przesłana do właściwej jednostki organizacyjnej SKW, sprawującej nadzór nad tym certyfikatem, celem określenia potrzeby i zakresu badań kontrolnych. W przypadku sprzętu klasy TEMPEST posiadającego certyfikat ochrony elektromagnetycznej wydany przez ABW ważność certyfikatu należy potwierdzić we właściwej jednostce organizacyjnej ABW sprawującej nadzór nad tym certyfikatem.
8. Sprzęt klasy TEMPEST po przeprowadzonej naprawie pogwarancyjnej, modyfikacji lub modernizacji odbierany jest po potwierdzeniu ważności

certyfikatu ochrony elektromagnetycznej wydanym przez organ sprawujący nadzór nad tym certyfikatem.

9. Sprzęt klasy TEMPEST naprawiany w ramach gwarancji producenta, należy odbierać z potwierdzeniem utrzymania ważności certyfikatu ochrony elektromagnetycznej wydanego dla danego sprzętu. W przypadku konieczności wykonania badań kontrolnych po takiej naprawie, odbywają się one na wniosek gwaranta.
10. Po przeprowadzonej naprawie, modyfikacji lub modernizacji sprzętu informatyki, dla którego SKW określiła „klasę urządzenia”, kopia Protokołu z Usługi Serwisowej powinna być przesłana do właściwej jednostki organizacyjnej SKW, która wydała potwierdzenie spełnienia określonej klasy urządzenia, celem ustalenia potrzeby i zakresu badań kontrolnych.

0904. Przechowywanie sprzętu informatyki wykorzystywanego w systemach teleinformatycznych przetwarzających informacje niejawne

1. Sposób przechowywania sprzętu informatyki wykorzystywanego w systemach teleinformatycznych przetwarzających informacje niejawne opisany jest w dokumentacji bezpieczeństwa danego systemu teleinformatycznego.
2. Sprzęt informatyki (w tym m.in. klasy TEMPEST) posiadający certyfikat ochrony elektromagnetycznej wydany przez ABW lub SKW, podlega ochronie do momentu jego zniszczenia.

0905. Wycofywanie sprzętu informatyki eksploatowanego w systemach teleinformatycznych przetwarzających informacje niejawne

1. Decyzję o zaprzestaniu eksploatacji sprzętu informatyki w systemie teleinformatycznym przetwarzającym informacje niejawne (w tym sprzętu klasy TEMPEST) podejmuje kierownik komórki/jednostki organizacyjnej resortu obrony narodowej, w której sprzęt jest eksploatowany. Wycofanie sprzętu z eksploatacji w systemie teleinformatycznym przetwarzającym informacje niejawne odbywa się zgodnie z zapisami dokumentacji bezpieczeństwa systemu teleinformatycznego.

2. Sprzęt informatyki wycofany z eksploatacji w systemie teleinformatycznym przetwarzającym informacje niejawne może być przeznaczony do ponownego użycia w komórce/jednostce organizacyjnej, w której był eksploatowany. W przypadku braku potrzeby zagospodarowania w ramach komórki/jednostki organizacyjnej należy go przekazać do właściwego WOG na ogólnych zasadach przewidzianych dla sprzętu informatyki, z wyłączeniem sprzętu klasy TEMPEST, który wycofuje się z użycia na zasadach określonych w pkt. od 4 do 8, sekcji 0905.
3. Sposób postępowania z IND ze sprzętu informatyki wycofywanego z eksploatacji w systemie teleinformatycznym przetwarzającym informacje niejawne określa dokumentacja bezpieczeństwa tego systemu. W przeciwnym przypadku, IND ze sprzętu informatyki wycofywanego z eksploatacji w systemie teleinformatycznym przetwarzającym informacje niejawne podlegają procesowi niszczenia. Dopuszcza się wymazywanie IND, z zachowaniem klauzuli tajności, w przypadku przeznaczenia ich do ponownego użycia, zgodnie z zaleceniami SKW.
4. Sprzęt klasy TEMPEST, niezagospodarowany lub nieplanowany do zagospodarowania w ramach komórki/jednostki organizacyjnej resortu obrony narodowej należy przekazać do właściwego WOG na zasadach przewidzianych dla sprzętu informatyki, pod warunkiem spełnienia wymagań określonych w pkt. 3, sekcji 0905.
5. W celu wycofania z eksploatacji w Siłach Zbrojnych RP sprzętu klasy TEMPEST kierownik WOG wyznacza komisję, która dokonuje oceny stanu technicznego sprzętu. Z przeprowadzonych czynności komisja sporządza protokół stanu technicznego na podstawie, którego COL SpW podejmuje decyzję o jego dalszej eksploatacji (w tym o przeklasyfikowaniu do kat. V).
6. Decyzję o wycofaniu z eksploatacji w Siłach Zbrojnych RP pojedynczych egzemplarzy sprzętu klasy TEMPEST podejmuje gestor SpW, na podstawie wniosku COL SpW oraz protokołu stanu technicznego, o którym mowa w pkt. 5, sekcji 0905.

7. Na podstawie zatwierdzonego przez gestora SpW wniosku, przeklasyfikowany do kat. V, bez IND sprzęt klasy TEMPEST (wraz z certyfikatami) WOG przekazuje do właściwej RBLog, zgodnie z obowiązującymi przepisami logistyczno-finansowymi.
8. Przeznaczony do wycofania z eksploatacji w Siłach Zbrojnych RP sprzęt klasy TEMPEST właściwa RBLog gromadzi w wydzielonej części pomieszczenia magazynowego, a następnie:
 - a. w ramach procesu niszczenia wstępnego prowadzi demontaż części/elementów/podzespołów wskazanych przez SKW, (przy uwzględnieniu rodzaju urządzeń poddanych Certyfikacji Typu), jako podlegających szczególnej ochronie;
 - b. zdemontowane części/elementy/podzespoły, podlegające szczególnej ochronie, poddaje się procedurze zniszczenia ostatecznego (przetopienie/rozpuszczenie w kwasie/zmielenie/pocięcie) zgodnie z opracowanymi przez właściwą RBLog i zaakceptowanymi przez SKW procedurami niszczenia sprzętu klasy TEMPEST we właściwej RBLog. W procedurach niszczenia uwzględnia się poszczególne typy (modele) sprzętu, który podlega zniszczeniu. Dopuszcza się odstępnie od demontażu niewielkiego gabarytowo sprzętu klasy TEMPEST i przeprowadzenie niszczenia ostatecznego całego urządzenia;
 - c. elementy, nie podlegające szczególnej ochronie (po pozbawieniu etykiet i innych identyfikujących je opisów oraz zaewidencjonowaniu, jako złom użytkowy lub odpady elektroniczne i elektryczne), przekazuje do dalszego zagospodarowania przez Agencję, zgodnie z obowiązującymi w tym zakresie przepisami;
 - d. celem utylizacji dopuszcza się przekazanie sprzętu klasy TEMPEST producentowi.

0906. Deklasyfikacja i wymazywanie danych z informatycznych nośników danych eksploatowanych w systemach teleinformatycznych przetwarzających informacje niejawne

1. Deklasyfikacja polega na wykonaniu procedury wymazania danych z IND, pozbawieniu go klauzuli tajności oraz dokonaniu zmian w odpowiednich urządzeniach ewidencyjnych.
2. W resorcie obrony narodowej nie przeprowadza się procedur deklasyfikacji IND.
3. Wymazanie danych to wykonanie w sposób celowy czynności (działań nieuszkodzających nośnika) prowadzących do uniemożliwienia lub znacznego utrudnienia odczytania informacji utrwalonych na IND z zachowaniem dotychczasowej klauzuli tajności nośnika. Typy IND podlegających wymazaniu, metody wymazywania oraz przypadki, w jakich wymazywanie jest wymagane określają zalecenia SKW.
4. Do wymazywania IND można stosować urządzenia lub narzędzia posiadające właściwy certyfikat wydany przez ABW lub SKW, albo przez organy bezpieczeństwa NATO, UE lub państwa członkowskiego tych organizacji. Dozwolone jest stosowanie innych narzędzi do wymazywania danych, przeznaczonych dla danej kategorii nośników pod warunkiem potwierdzenia przez organizatora systemu realizacji metod zalecanych przez SKW oraz uwzględnienie stosownej procedury w dokumentacji bezpieczeństwa systemu teleinformatycznego.
5. Wymazywanie danych prowadzi się w ramach procesu niszczenia wstępnego, w stosunku do określonego w zaleceniach SKW typu IND dla metod przewidujących wymazywanie oraz w przypadku wycofywania IND z systemu celem dalszego wykorzystania w systemach teleinformatycznych przetwarzających informacje niejawne. Dopuszcza się odstępnie od wymazywania danych w ramach procesu niszczenia wstępnego IND w sytuacji, w której z przyczyn technicznych nie jest możliwe wymazanie danego IND.

6. Wymazywanie danych z dysków twardych przeprowadza się w ramach tej samej komórki/jednostki organizacyjnej resortu obrony narodowej, w której były one wykorzystywane, z zastrzeżeniem pkt. 9, sekcji 0906.
7. Z procesu wymazywania danych sporządza się protokół wymazania danych zgodnie ze wzorem zawartym w załączniku K.
8. Wymazanie danych z IND nie uprawnia do zmiany jego klauzuli tajności.
9. W przypadku rozformowania komórki/jednostki organizacyjnej resortu obrony narodowej w szczególnie uzasadnionych przypadkach, po uzyskaniu pozytywnej opinii organu akredytującego, proces wymazywania danych może przeprowadzić następcą prawny danej komórki/jednostki organizacyjnej lub w przypadku IND o klauzuli „zastrzeżone” organ wsparcia teleinformatycznego obsługujący system teleinformatyczny, w którym eksploatowane były IND. IND należy wówczas przekazać do docelowej komórki/jednostki organizacyjnej poprzez kancelarię. Nowa komórka/jednostka organizacyjna może użytkować przyjęty IND dopiero po przeprowadzonym procesie wymazywania danych, z zastrzeżeniem pkt 10, sekcji 0906.
10. W przypadku, gdy następcą prawny rozformowanej lub przeformowanej (zreorganizowanej) komórki/jednostki organizacyjnej resortu obrony narodowej kontynuuje zadania niniejszej jednostki/komórki organizacyjnej dopuszcza się odstąpienie od przeprowadzania procesu wymazywania danych przed przystąpieniem do dalszej eksploatacji systemu teleinformatycznego po uzyskaniu pozytywnej opinii organu akredytującego.
11. W przypadku IND, z którego z przyczyn technicznych nie jest możliwe wymazanie danych, można odstąpić od wymazywania i przejść do kolejnego etapu niszczenia wstępnego. Dopuszcza się przejście bezpośrednio do etapu niszczenia ostatecznego IND, w sytuacji, w której proces ten zostanie przeprowadzony w komórce/jednostce organizacyjnej, która była ostatnim użytkownikiem IND.

0907. Niszczenie informatycznych nośników danych eksploatowanych w systemach teleinformatycznych przetwarzających informacje niejawne

1. Niszczenie IND przeprowadza się zgodnie z procedurami zawartymi w zaleceniach SKW chyba, że dokumentacja bezpieczeństwa systemu teleinformatycznego stanowi inaczej. Niszczeniu podlegają IND wycofane z eksploatacji w Siłach Zbrojnych RP. Niszczenie IND obejmuje proces niszczenia wstępnego i niszczenia ostatecznego.
2. Niszczenie wstępne IND to zamierzone wykonanie czynności prowadzących do uszkodzenia IND, w sposób uniemożliwiający, bez zastosowania specjalnych narzędzi (sprzętu informatyki lub oprogramowania), odzyskanie zapisanych na nich danych oraz jednocześnie zapewniający, że cechy identyfikujące nośnik (klauzula, numer ewidencyjny, producent, numer seryjny, oznaczenie pojemności, itp.) pozostaną czytelne do czasu jego zniszczenia ostatecznego.
3. Niszczenie ostateczne IND to fizyczne zniszczenie IND, w sposób uniemożliwiający odtworzenie jego zawartości i niewywołujący negatywnych skutków ekologicznych.
4. IND przed uruchomieniem procesów niszczenia wstępnego i ostatecznego poddaje się szczegółowej identyfikacji (na podstawie cech fizycznych, numerów fabrycznych i ewidencyjnych) oraz porównaniu z danymi zawartymi w ewidencji ilościowo-wartościowej i ilościowo-jakościowej WOG oraz ewidencji kancelaryjnej.
5. Niszczenia wstępnego IND dokonuje komisja, o której mowa w pkt. 16, sekcji 0907.
6. Zniszczenie wstępne IND dokumentuje się w protokole zniszczenia wstępnego IND, którego wzór określa załącznik L.
7. Protokół zniszczenia wstępnego upoważnia do zdjęcia IND z ewidencji logistyczno-finansowej, nie upoważnia do zdjęcia z ewidencji kancelaryjnej.

8. Zezwala się na odstąpienie od wstępnego niszczenia IND i poddanie ich bezpośrednio niszczeniu ostatecznemu na zasadach określonych w pkt. od 13 do 20 sekcji 0907, dla IND niszczonych ostatecznie w komórce/jednostce organizacyjnej resortu obrony narodowej, która była ich ostatnim użytkownikiem.
9. Obligatoryjnemu procesowi niszczenia wstępnego podlegają IND, które w celu ich ostatecznego zniszczenia są przekazywane do innej komórki/jednostki organizacyjnej resortu obrony narodowej lub podlegają procesowi niszczenia ostatecznego w firmach zewnętrznych spoza resortu obrony narodowej, przeprowadzanego zgodnie z zaleceniami SKW.
10. IND zniszczony wstępnie, do czasu zniszczenia ostatecznego przechowuje się i przesyła za pośrednictwem kancelarii.
11. Zniszczenie wstępne IND nie upoważnia do zmiany jego klauzuli tajności.
12. Przetwarzanie lub odzyskiwanie informacji ze wstępnie zniszczonych IND jest dopuszczalne wyłącznie na etapie postępowań wyjaśniających, kontrolnych i śledczych. Każda inna próba odzyskiwania danych z nośników przeznaczonych do niszczenia stanowi incydent komputerowy, jest naruszeniem przepisów o ochronie informacji niejawnych i podlega zgłoszeniu do właściwych organów bezpieczeństwa.
13. Niszczeniu podlegają wszystkie IND wycofane z eksploatacji w Siłach Zbrojnych RP, wykorzystywane w systemach teleinformatycznych przetwarzających informacje niejawne.
14. Niszczenia ostatecznego IND dokonuje się w miarę możliwości w komórce/jednostce organizacyjnej resortu obrony narodowej, która była ich ostatnim użytkownikiem, z zastrzeżeniem pkt. 15, sekcji 0907. Niszczenia ostatecznego IND dokonuje komisja, o której mowa w pkt. 16, sekcji 0907.
15. IND, których ostateczne zniszczenie w komórce/jednostce organizacyjnej resortu obrony narodowej, ze względów ekologicznych, ekonomicznych, technicznych, itp. jest niemożliwe, po zniszczeniu wstępnym podlegają przesłaniu wraz z protokołem wstępnego zniszczenia do komórki/jednostki

organizacyjnej resortu ON posiadającej możliwości niszczenia ostatecznego IND wskazanej przez COL SpW, w uzgodnieniu z gestorem SpW.

16. Niszczenia IND dokonuje komisja w składzie, co najmniej trzech osób wyznaczonych rozkazem (decyzją) kierownika komórki/jednostki organizacyjnej resortu obrony narodowej. Do składu komisji wyznacza się osoby posiadające odpowiednie kompetencje, wiedzę i znajomość w zakresie problematyki związanej ze sprzętem informatyki i oprogramowaniem. W skład komisji powinien wchodzić Inspektor Bezpieczeństwa Teleinformatycznego, bądź inny przedstawiciel komórki wewnętrznej właściwej ds. ochrony informacji niejawnych. Wszystkie osoby wyznaczone do składu komisji muszą posiadać odpowiednie uprawnienia do dostępu do informacji niejawnych, co najmniej zgodne z klauzulą sprzętu przedstawianego do niszczenia.
17. IND przesłane przez komórki/jednostki organizacyjne, zgodnie z pkt. 15, sekcji 0907, celem ostatecznego zniszczenia, muszą być możliwe do jednoznacznej identyfikacji na podstawie danych zawartych w protokole wstępnego zniszczenia.
18. Procesowi niszczenia poddaje się w szczególności elementy IND, które przechowują informacje niejawne. Pozostałe elementy (w tym, np. obudowy), po usunięciu elementów umożliwiających identyfikację poprzedniego wykorzystania niszczonego nośnika, mogą zostać ponownie wykorzystane, przekazane do utylizacji, recyklingu, itp., zgodnie z obowiązującymi w tym zakresie przepisami. Zagospodarowanie elementów i odpadów pozostających po ostatecznym zniszczeniu IND można realizować, po ich wcześniejszym zaewidencjonowaniu.
19. Zniszczenie ostateczne IND dokumentuje się w protokole zniszczenia ostatecznego IND, którego wzory określają załączniki M i N.
20. Protokół zniszczenia ostatecznego IND upoważnia do zdjęcia z ewidencji kancelaryjnej oraz w przypadku odstąpienia od niszczenia wstępnego, z ewidencji logistyczno-finansowej.

0908. Kontrola systemów teleinformatycznych przetwarzających informacje niejawne

1. Zasady prowadzenia działalności kontrolnej i rozliczeniowej w odniesieniu do systemów teleinformatycznych przetwarzających informacje niejawne określają odrębne przepisy.
2. Eksploatowane w resorcie obrony narodowej systemy teleinformatyczne podlegają kontroli w zakresie gospodarki materiałowo-technicznej, w odniesieniu do sprzętu, urządzeń i oprogramowania wykorzystywanego w danym systemie teleinformatycznym przetwarzającym informacje niejawne.
3. Osoby wyznaczone do prowadzenia działalności kontrolnej i rozliczeniowej są zobligowane do posiadania właściwych upoważnień, poświadczeń bezpieczeństwa, zgodnie z dokumentacją bezpieczeństwa systemu.

ROZDZIAŁ 10 ZAKOŃCZENIE

1001. Postanowienia końcowe

1. Realizacja procesów logistyczno-finansowych związanych z prowadzeniem gospodarki sprzętem informatyki i oprogramowaniem, opisanych w instrukcji, może odbywać się z wykorzystaniem wdrożonego Zintegrowanego Wieloszczeblowego Systemu Informatyczny Resortu Obrony Narodowej.
2. Za realizację postanowień zawartych w instrukcji w zakresie organizacji prowadzenia gospodarki materiałowo-technicznej sprzętu informatyki i oprogramowania w resorcie obrony narodowej odpowiada kierownik komórki/jednostki organizacyjnej resortu obrony narodowej lub wyznaczona w rozkazie/decyzji przez niego osoba funkcyjna.
3. Osoby funkcyjne, komórki i jednostki organizacyjne resortu obrony narodowej, które są użytkownikami przydzielonego im sprzętu informatyki i oprogramowania, zobowiązane są do przestrzegania dyscypliny gospodarczej, w tym przestrzegania zasad dyscypliny finansów publicznych.
4. Za naruszenie dyscypliny gospodarczej, w tym dyscypliny finansów publicznych ponosi się odpowiedzialność na zasadach określonych w odrębnych przepisach.
5. W celu zapewnienia prawidłowego funkcjonowania gospodarki materiałowo-technicznej sprzętem informatyki i oprogramowaniem oraz optymalnych warunków jego eksploatacji gestor SpW lub COL SpW organizuje odprawy szkoleniowe i narady z osobami funkcyjnymi odpowiedzialnymi za prowadzenie gospodarki materiałowo-technicznej, co najmniej raz w roku i dodatkowo po zmianie przepisów (w zależności od potrzeb).
6. Działalność kontrolną oraz nadzór nad realizacją i przestrzeganiem postanowień zawartych w instrukcji, zgodnie z zakresem posiadanych kompetencji, sprawują:
 - a. gestor SpW;
 - b. COL SpW;

- c. osoby odpowiedzialne za gospodarkę materiałowo-techniczną, z racji zajmowanego stanowiska służbowego oraz wyznaczone osoby funkcyjne w resorcie obrony narodowej.
7. W zakresie zagadnień nieuregulowanych niniejszą instrukcją należy stosować się do obowiązujących przepisów.

"Z A T W I E R D Z A M"

Egz. nr....

(pieczęć i podpis dowódcy, data)

PROTOKÓŁ PRZYJĘCIA-PRZEKAZANIA NR.....

Sporządzony w dnia przez komisję powołaną rozkazem z dnia

na podstawie:

dokonano przyjęcia sprzętu (urządzenia), materiału

od:

do:

transport:

wartość faktury: zł.

Ilość opakowań według dokumentów: faktyczna: brak nadwyżka

Stan opakowań (plomb, pieczęci)

Skład komisji:

(stopień, imię i nazwisko członków komisji)

1.
 2.
 3.
- (Przedstawiciel dostawcy – odbiorcy)

Rodz. dok.	Nr dokumentu	Data dokumentu		P	Nr Przyjmującego		Nr Kierunek przychodu	R	Nr Wydającego		Nr Kierunek rozchodu
		Dzień	M-c		Rok	LK			LK		

Po otwarciu opakowań stwierdzono:

Lp.	Nazwa materiału	Przyjęć/ przekazane wg dokumentu		Jednolity Indeks Materiałowy	JM	Przyjęto/ przekazano faktycznie		Ind. numer wyrobu/cecha partii	Rok produkcji	Cena /zł/	Wartość /zł/	Różnica		Poz. książki lub karty	
		Ilość	Kat.			Ilość	Kat.					Brak	Nadwyżka		
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1.															
2.															

Załącznik A

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3.															
4.															
5.															
6.															
7.															

Razem ilość pozycji (słownie) orzeczenie (wnioski) Razem wartość: zł.

Wyszczególnione, sprzęt (urządzenia), materiały, zgodnie ze stanem faktycznym

Przyjął:
(stopień, imię i nazwisko oraz podpis)

Wydał:
(stopień, imię i nazwisko oraz podpis)

Data: przyjęcia – wydania

PODPISY KOMISJI

1.
 2.
 3.
-
(Przedstawiciel dostawcy – odbiorcy)

Wykonano w.... egz.

Egz. nr

Egz. nr

Egz. nr

Egz. nr

Egz. nr

Wykonat:

1. Eksploatacja urządzenia

Data otrzymania	Nr jednostki wojskowej/ pododdziału	Odpowiedzialny	Nr rozkazu dziennego	Podpis i pieczęć

2. Kategoria urządzenia

Data	Podstawa zmiany		Kategoria po zmianie	Podpis i pieczęć	Uwagi
	Nazwa dokumentu	Numer, z dnia			

3. Kontrole stanu technicznego, naprawy

Data kontroli/ naprawy	Podstawa kontroli/ naprawy	Ocena stanu technicznego	Kto przeprowadził kontrolę/naprawę (data i podpis)

4. Inne zapisy służbowe, uwagi organów kontrolujących

ZASADY DOKONYWANIA WPISÓW W KARCIE SPRZĘTU

STRONA PIERWSZA

Lewy górny róg: wpisuje się nazwę i adres komórki/jednostki organizacyjnej RON wytwarzającej kartę sprzętu;

Prawy górny róg: wpisuje się datę wytworzenia karty sprzętu. Data powinna być zgodna z datą - sprzętu (datą przyjęcia na protokole przyjęcia-przekazania);

KARTA SPRZĘTU NR...: wpisuje się kolejny numer karty sprzętu zarejestrowany w Rejestrze obrotów dowodów materiałowych symbol Gm-6. Rejestr musi być zaewidencjonowany w kancelarii i podlegać archiwizacji zgodnie z wymaganiami określonymi w przepisach dotyczących zasad i trybu postępowania z materiałami archiwalnymi i inną dokumentacją w resorcie obrony narodowej;

Nazwa sprzętu: wpisuje się właściwą nazwę sprzętu, zgodnie z JIM;

JIM: wpisuje się właściwy jednolity indeks materiałowy;

Nr fabryczny: wpisuje się numer fabryczny nadany przez producenta, znajdujący się na sprzęcie i w dokumentacji technicznej/eksploatacyjnej;

Data produkcji: wpisuje się datę produkcji;

Podstawa przyjęcia: wpisuje się numer „Protokołu przyjęcia-przekazania” oraz dokumentu dostawy(zakupu);

Wyposażenie: w tabeli wpisuje się elementy wyposażenia sprzętu wymienione w dokumencie zakupu, umowie lub protokole przyjęcia-przekazania;

Lp.: wpisuje się kolejną pozycję wyposażenia sprzętu lub kompletu sprzętu;

JIM: wpisuje się właściwy jednolity indeks materiałowy;

Nazwa urządzenia, przedmiotu lub materiału: wpisuje się nazwę zgodną z JIM;

Jednostka miary: wpisuje się właściwą jednostkę miary określoną w JIM, np.: szt., kpl., itp.;

Ilość: wpisuje się faktyczną ilość wyposażenia dodatkowego;

Kierownik Magazynu: wpisuje się czytelnie imię i nazwisko, ewentualnie pieczęć imienną, podpis osoby przyjmującej sprzęt na stan ewidencyjny. Osoba ta jest odpowiedzialna za właściwe wytworzenie karty sprzętu;

Kierownik komórki/jednostki organizacyjnej przyjmującej: wpisuje się czytelnie imię i nazwisko, ewentualnie pieczęć imienną, podpis kierownika komórki/jednostki organizacyjnej lub osoby wyznaczonej rozkazem (decyzją) kierownika sprawującej merytoryczny nadzór nad powierzonym mieniem.

STRONA DRUGA

Wpisy na drugiej stronie należy wykonać komputerowo w czasie wytwarzania dowodu urządzenia lub czarnym/niebieskim długopisem, czytelnie i bez poprawek. W przypadku błędnego wpisu przekreśla się cały wiersz na czerwono, tak aby zachować czytelność błędnego wpisu, potwierdzając ten fakt podpisem – czytelnie imię i nazwisko osoby poprawiającej błędny wpis. Właściwego wpisu dokonuje się w kolejnym wierszu.

1. **Eksploatacja urządzenia:** wpisuje się po raz pierwszy w komórce/jednostce organizacyjnej przyjmującej sprzęt do eksploatacji lub przechowywania, zgodnie z opisem wskazanym w poszczególnych kolumnach.
2. **Kategoria urządzenia:** wypełnia się zgodnie z treścią poszczególnych rubryk w czasie eksploatacji urządzenia w komórce/jednostce organizacyjnej.
3. **Kontrole stanu technicznego, naprawy:** wpisuje się adnotacje o konserwacjach i naprawach sprzętu, w tym badania dozоровe, metrologiczne, elektroenergetyczne, jeżeli sprzęt(urządzenie) podlega tym badaniom. Kolejne kolumny wypełnia się zgodnie z ich opisem (krótki i czytelny wpis osoby realizującej dane przedsięwzięcie).
4. **Inne zapisy służbowe, uwagi organów kontrolujących:** wpisy dokonuje i potwierdza kierownik komórki/jednostki organizacyjnej lub osoba wyznaczona jego rozkazem (decyzją), sprawująca merytoryczny nadzór nad powierzonym mieniem.

Wpisów obowiązkowych dokonuje się w przypadku wykonania następujących czynności:

- dołączenia dodatkowych stron karty sprzętu (np. dołączono 1 kartkę „*karty sprzętu*”),
- inne okoliczności mające wpływ na użytkowanie lub przechowywanie sprzętu nie ujęte w karcie sprzętu(np. zdjęcie z ewidencji i przeznaczenie do szkolenia),
- uwagi organów kontrolujących.

Załącznik G

WNIOSEK NA OPROGRAMOWANIE NR Z DNIA

Nazwa komórki/jednostki organizacyjnej resortu obrony narodowej	
Wojskowy Oddział Gospodarczy	
Dane kontaktowe²	

Pozycje zamówienia/rezygnacji³:

Lp.	Nazwa i wersja oprogramowania	JIM	Uzasadnienie⁴	Ilość licencji
ZAMÓWIENIE OPROGRAMOWANIA				
Z1				
Z2				
...				
REZYGNACJA Z OPROGRAMOWANIA				
R1				
R2				
...				

DOWÓDCA⁵*(podpis)*

² Stopień imię i nazwisko, telefon, fax, e-mail wnioskodawcy (osoby odpowiedzialnej za dystrybucję oprogramowania w komórce/jednostce organizacyjnej resortu obrony narodowej).

³ Należy skreślić niewłaściwą operację.

⁴ Rodzaj sieci teleinformatycznej (np. INTER-MON, BSK, SEC-WAN, PF-WAN, AUTONOMICZNE, INNE – dla INNE proszę podać nazwę/kryptonim systemu/sieci).

⁵ Kierownik komórki/jednostki organizacyjnej resortu obrony narodowej.

Załącznik H

		Warszawa, dnia _____ 20__r. Egz. nr ____
UPOWAŻNIENIE NR _____/20__		
Upoważnia się:		
Nazwa komórki/jednostki organizacyjnej resortu obrony narodowej		
Do instalacji i użytkowania oprogramowania:		
Nazwa oprogramowania		
Wersja oprogramowania		
Numer licencji		
Indeks licencji		
Na okres		
Informacje dodatkowe		
Oryginały certyfikatów licencyjnych oraz kopia umowy zakupu w/w oprogramowania znajdują się do wglądu w Bibliotece Teleinformatycznej Resortowego Centrum Zarządzania Projektami Informatycznymi (tel. 840-173).		

KOMENDANT RCZPI

.....

Wykonano w 3 egz.:

Egz. nr 1 – Odbiorca

Egz. nr 2 – Biblioteka RCZPI – ad acta

Egz. nr 3 – właściwy wojskowy oddział gospodarczy

ZA TWIERDZAM

.....
(kierownik komórki/jednostki organizacyjnej resortu obrony narodowej)*

ARKUSZ ZGŁOSZENIA AWARII

Nazwa urzędnika	JIM	Nr seryjny	Rok produkcji	Miejsce - adres Zainstalowania	Osoba do kontaktu
<i>Przykład:</i> DRUKARKA EPSON STYL/S21 ATR A4 K.NOU1	7025PL1524168	GMTE035489	2007	Warszawa ul. Rydza 5 bud 89 pom.45	ppłk Adam STON

Opis występującej usterki, błędu, zacięcia.....
.....
.....

Użytkownik

.....

**CZĘSTOTLIWOŚĆ REALIZACJI PRZEDSIĘWZIĘĆ NADZORCZYCH W ZAKRESIE GOSPODARKI
SPRZĘTEM INFORMATYKI I OPROGRAMOWANIEM**

Lp	Przedsięwzięcia nadzorcze	Osoby funkcyjne WOG/ komórki (jednostek) organizacyjnych pełniących funkcję WOG ⁸⁾						Osoby funkcyjne pododdziałów gospodarczych pozostających na zaopatrzeniu WOG					Uwagi
		Kierownik komórki (jednostki) organizacyjnej/komisja	Szef Logistyki	Szef Wydziału Technicznego	Szef Służby Sprzętu Łączności i Informatyki ⁷⁾	Kierownik Magazynów (równorzędny)	Magazyner	Kierownik komórki (jednostki) organizacyjnej/komisja	Osoba upoważniona przez kierownika (przedstawiciel S-4 lub równorzędny) ⁷⁾	Dowódca batalionu (dywizjonu), wyznaczona osoba	Dowódca kompanii (równorzędny)	Technik kompanii (równorzędny)/dowódca plutonu	
1.	Kontrola przestrzegania przepisów dotyczących gospodarowania mieniem sprzętu łączności i informatyki: - w pododdziałach własnych; - w JW będących na zaopatrzeniu.	R	R	P	K		R	P	K	M	T	Książka przeglądów kontrolnych/ Książka ewidencji mienia w pododdziale/ Protokół	
2.	Sprawdzenie zgodności ewidencji ilościowo-wartościowej z ewidencją ilościowo-jakościową magazynów i pododdziałów.				P ⁸⁾	P ⁸⁾				P ⁸⁾		Książka ewidencji mienia w pododdziale/ ewidencja w systemie informatycznym	
3.	Kontrola przestrzegania przepisów gospodarki materiałowo-magazynowej w magazynach oddziałowych.	R	R	P	K	K						Książka przeglądów kontrolnych/ Książka kontroli magazynu	
4.	Sprawdzenie stanu technicznego, utrzymania i ukończenia SpW oraz dokumentacji eksploatacyjnej w pododdziałach własnych i magazynach.		R	P	K	K					T	Książka ewidencji mienia w pododdziale/Książka kontroli magazynu	
5.	Komisyjne sprawdzenie wykonania czynności obsługowych w czasie obsługi rocznego.	R ⁴⁾	R ⁹⁾	R ⁹⁾	R ⁹⁾							Protokół z wykonania OR	
6.	Nadzór nad wykonywaniem obsługiwań bieżących sprzętu łączności i informatyki.				B						B	Protokół z wykonania OR	

LEGENDA:

R – raz w roku; P – raz na pół roku; K – raz na kwartał; M – raz na miesiąc; D – raz na dekadę, B – na bieżąco, w miarę potrzeb.

- 1) - Rocznie 100% jednostek będących na zaopatrzeniu WOG.
- 2) - Rocznie nie mniej niż 50 % jednostek będących na zaopatrzeniu WOG.
- 3) - Rocznie nie mniej niż 25 % jednostek będących na zaopatrzeniu WOG.
- 4) - Kontrola wykonania obsługiwanego rocznego realizowana jest przez komisję powołaną rozkazem (decyzją) kierownika WOG, po złożeniu meldunku o zakończeniu obsługiwanego rocznego przez pododdziały własne WOG.
- 5) - Kontrola wykonania obsługiwanego rocznego realizowana jest przez komisję powołaną rozkazem kierownika komórki/jednostki organizacyjnej realizującej zadania pododdziału gospodarczego, po złożeniu meldunku dowódcy pododdziału o zakończeniu obsługiwanego rocznego.
- 6) - Zapis – „Osoby funkcyjne komórek (jednostek) organizacyjnych WOG/pełniących funkcję WOG” – dotyczy również RBLog. w zakresie pełnienia funkcji WOG, inne czynności nadzorcze RBLog wg własnych planów.
- 7) - Kierownik komórki/jednostki organizacyjnej resortu obrony narodowej może zgodnie ze swoim rozkazem (decyzją) wyznaczyć osobę funkcyjną w Zespole Zabezpieczenia/pododdziale do realizacji przedsięwzięć wykonywanych przez Szefa Służby Sprzętu Łączności/S-4.
- 8) - Sprawdzenie losowo wybranej ilości asortymentu.
- 9) - Udział w komisji zgodnie z rozkazem (decyzją) kierownika WOG.

Załącznik K

Egz. nr

Z A T W I E R D Z A M*(nazwa stanowiska służbowego kierownika
komórki/jednostki organizacyjnej)**(stopień wojskowy, imię i nazwisko, data)***PROTOKÓŁ
WYMAZANIA DANYCH**

Zgodnie z rozkazem (decyzją)*) Nr kierownika komórki/jednostki organizacyjnej z dnia roku, komisja w składzie:

przewodniczący:.....

członkowie:

.....

przeprowadziła w dniu roku wymazanie danych z następujących informatycznych nośników danych:

Lp.	Producent/ typ nośnika danych	Numer seryjny (fabryczny)	Klauzula tajności nośnika danych	Numer ewidencyjny nośnika danych	Nazwa użytego programu i metody wymazywania	U w a g i
...	
...	

Komisja stwierdza, że proces wymazywania danych wymienionych informatycznych nośników danych:

1. w poz. zakończył się powodzeniem*);
2. w poz. zakończył się niepowodzeniem*).

Niniejszy protokół nie stanowi podstawy do zdjęcie z ewidencji kancelaryjnej.

PODPISY:

.....

.....

.....

Wykonano w 2 egz.:

Egz. nr – ad acta

Egz. nr – (stopień wojskowy, imię i nazwisko administratora niejawnego systemu teleinformatycznego)

*) Niepotrzebne skreślić.

Załącznik L

Egz. nr

Z E Z W A L A M

na zniszczenie nośników danych wyszczególnionych w protokole

*(nazwa stanowiska służbowego kierownika komórki/jednostki organizacyjnej)**(stopień wojskowy, imię i nazwisko, data)***PROTOKÓŁ****ZNISZCZENIA WSTĘPNEGO INFORMATYCZNYCH NOŚNIKÓW DANYCH**

Zgodnie z rozkazem (decyzją*) Nr kierownika komórki/jednostki organizacyjnej z dnia roku, komisja w składzie:

przewodniczący:

członkowie:

w dniu roku zakwalifikowała następujące informatyczne nośniki danych do zniszczenia wstępnego:

Lp.	Producent/ typ nośnika/ pojemność	Numer seryjny (fabryczny)	Klauzula tajności nośnika danych	Numer ewidencyjny nośnika danych	Numer dowodu urządzenia/książki materiałowej/karty sprzętu	U w a g i
...	
...	

PODPISY:

.....

Zgodnie z rozkazem (decyzją*) Nr kierownika komórki/jednostki organizacyjnej z dnia roku, komisja w składzie:

przewodniczący:

członkowie:

w dniu roku wstępnie zniszczyła informatyczne nośniki danych wymienione w poz.przez(np. trzykrotne przewiercenie w płaszczyźnie pionowej w obszarze talerzy dyskowych). Pojemnik ze zniszczonymi wstępnie IND zamknięto i opieczetowano pieczęcią numerowa do teczek pracy nr

PODPISY:

.....

Wstępnie zniszczone IND wymienione w protokole przesłano do zniszczenia ostatecznego za pismem**):

*(nr pisma, z dnia – wypełnia właściwa kancelaria)***Wykonano w 4 egz.:**

Egz. nr 1 - ad acta

Egz. nr 2 - RCZBSiUT lub inna komórka/jednostka organizacyjna

Egz. nr 3 - *(stopień wojskowy, imię i nazwisko administratora niejawnego systemu teleinformatycznego)*Egz. nr 4 - *(właściwy wojskowy oddział gospodarczy)*

*) Niepotrzebne skreślić.

**) Stanowi podstawę do zdjęcia z ewidencji kancelaryjnej.

Załącznik M

Egz. nr

Z E Z W A L A M

na zniszczenie nośników danych wyszczególnionych w protokole

*(nazwa stanowiska służbowego kierownika komórki/jednostki organizacyjnej)**(stopień wojskowy, imię i nazwisko, data)***PROTOKÓŁ
ZNISZCZENIA OSTATECZNEGO INFORMATYCZNYCH NOŚNIKÓW DANYCH
NIENISZCZONYCH WSTĘPNIE**

Zgodnie z rozkazem (decyzją)*) Nr kierownika komórki/jednostki organizacyjnej z dnia roku, komisja w składzie:

przewodniczący:

członkowie:

w dniu roku zakwalifikowała następujące informatyczne nośniki danych do zniszczenia ostatecznego (wypełnia się w przypadku odstąpienia od niszczenia wstępnego):

Lp.	Producent/ typ nośnika/ pojemność	Numer seryjny (fabryczny)	Klauzula tajności nośnika danych	Numer ewidencyjny nośnika danych	Numer dowodu urządzenia/książki materiałowej/karty sprzętu	U w a g i
...	
...	

PODPISY:

.....

.....

Zgodnie z rozkazem (decyzją)*) Nr kierownika komórki/jednostki organizacyjnej z dnia roku, komisja w składzie:

przewodniczący:

członkowie:

.....

w dniu roku nadzorowała ostateczne zniszczenie informatycznych nośników danych wymienione w poz.

Komisja stwierdza, że informatyczne nośniki danych, o których mowa w wyżej wymienionych pozycjach, zostały zniszczone ostatecznie w *(nazwa komórki/jednostki organizacyjnej lub firmy komercyjnej wykonującej usługi ostatecznego niszczenia nośników danych, adres komórki/jednostki organizacyjnej lub firmy i miejsce przeprowadzenia zniszczenia ostatecznego)* przez *(zastosowana metoda zniszczenia)*.**PODPISY:**

.....

.....

Wykonano w egz. pojedynczym/2 egz. *:

Egz. pojedynczy/nr 1*-ad acta

Egz. nr 2* - właściwy wojskowy oddział gospodarczy (tylko w przypadku odstąpienia od niszczenia wstępnego)

*) Niepotrzebne skreślić.

Załącznik N

Egz. nr

Z A P O Z N A Ł E M S I Ę*(nazwa stanowiska służbowego kierownika komórki/jednostki organizacyjnej)**(stopień wojskowy, imię i nazwisko, data)***PROTOKÓŁ
ZNISZCZENIA OSTATECZNEGO INFORMATYCZNYCH NOŚNIKÓW DANYCH
ZNISZCZONYCH WSTĘPNIE**

Zgodnie z rozkazem (decyzją)*) Nr kierownika komórki/jednostki organizacyjnej z dnia roku, komisja w składzie:

przewodniczący:

członkowie:

.....

w dniu roku nadzorowała ostateczne zniszczenie informatycznych nośników danych wstępnie zniszczonych, zgodnie z protokołami wstępnego zniszczenia:

1. Nr z dnia roku, przechowywanym w kancelarii
2. Nr z dnia roku, przechowywanym w kancelarii

Komisja stwierdza, że informatyczne nośniki danych, o których mowa w wymienionych protokołach, zostały zniszczone ostatecznie w *(nazwa komórki/jednostki organizacyjnej lub firmy komercyjnej wykonującej usługi ostatecznego niszczenia nośników danych, adres komórki/jednostki organizacyjnej lub firmy i miejsce przeprowadzenia zniszczenia ostatecznego)* przez *(zastosowana metoda zniszczenia)*.

PODPISY:

.....

Wykonano w 2 egz.:

Egz. nr 1 - ad acta

Egz. nr 2 - *(właściwy wojskowy oddział gospodarczy)*

*) Niepotrzebne skreślić.

SŁOWNIK TERMINÓW I DEFINICJI

- administrator systemu teleinformatycznego** – osoba lub zespół osób odpowiedzialnych za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego;
- beneficjent** – komórka organizacyjna Ministerstwa Obrony Narodowej lub jednostka organizacyjna resortu obrony narodowej na rzecz, której planowane i realizowane są zadania rzeczowe;
- bezpieczeństwo teleinformatyczne** – stan uzyskany poprzez opracowanie, wdrożenie i utrzymywanie całokształtu zabezpieczeń organizacyjno-administracyjnych, fizycznych, technicznych, osobowych, sprzętowych oraz programowych w systemie teleinformatycznym w celu ochrony przed nieautoryzowanym dostępem, nieuprawnioną eksploatacją, modyfikacją, przechwyceniem lub zniszczeniem informacji, jak też i sprzętu;
- centralne plany rzeczowe** – plany sporządzane na okres objęty programowaniem rozwoju Sił Zbrojnych RP i aktualizowane corocznie przez Zarząd Sztabu Generalnego WP właściwy do spraw planowania rzeczowego, o których mowa w decyzji Ministra Obrony Narodowej w sprawie zasad opracowywania i realizacji centralnych planów rzeczowych;
- centralny organ logistyczny SpW (COL SpW)** – organ w rozumieniu przepisów dotyczących przepisów w sprawie określenia funkcji gestorów i centralnych organów logistycznych sprzętu wojskowego w resorcie obrony narodowej;
- certyfikacja** – formalny proces prowadzony przez Agencję Bezpieczeństwa Wewnętrznego (ABW) lub Służbę Kontrwywiadu Wojskowego (SKW) w oparciu o badania i ocenę bezpieczeństwa wykonywane w celu potwierdzenia zdolności urządzenia, narzędzia lub innego środka ochrony elektromagnetycznej do ochrony informacji niejawnych;

- cykl życia** – wszelkie możliwe kolejne etapy życia SpW w rozumieniu przepisów w sprawie pozyskiwania sprzętu wojskowego i usług dla Sił Zbrojnych Rzeczypospolitej Polskiej;
- decentralne plany rzeczowe (w części dotyczącej centralnych planów rzeczowych)** – plany na rok planistyczny sporządzane przez organy planujące drugiego stopnia oraz trzeciego stopnia bezpośrednio podległe organowi planującemu pierwszego stopnia, w szczególności nie mniejszej niż szczegółowość określona dla centralnych planów rzeczowych i z wyszczególnieniem pozycji ujętych w centralnych planach rzeczowych w kwotach zbiorczych, w których dokonują oni podziału zadań rzeczowych zaplanowanych do realizacji decentralnej na podporządkowanych dysponentów środków budżetu państwa trzeciego stopnia;
- dostawa** – dostarczenie sprzętu informatyki lub oprogramowania przez dostawcę, w odpowiednim czasie i miejscu, zgodnie z zawartą umową;
- Dyrektor Generalny Ministerstwa Obrony Narodowej (DG MON)** – komórka wykonująca funkcję dysponenta środków budżetu państwa trzeciego stopnia bezpośrednio podległa Ministrowi Obrony Narodowej, jako dysponentowi części budżetowej, w imieniu którego Departament Administracyjny MON (DA MON) realizuje zadania logistycznego zabezpieczenia Ministerstwa, zgodnie z planem przydziałów gospodarczych resortu obrony narodowej;
- dysponenci środków budżetowych** – należy przez to rozumieć dysponentów środków budżetowych określonych stopni: pierwszego (głównego), drugiego i trzeciego stopnia, ustanowionych zgodnie z przepisami w sprawie planowania i wykonania budżetu resortu obrony narodowej;
- eksploatacja** – zespół celowych działań organizacyjno-technicznych i ekonomicznych podejmowanych przez użytkowników wobec sprzętu informatyki i oprogramowania oraz wzajemne relacje między nimi, od chwili ich wprowadzenia aż do wycofania.

- Proces eksploatacji obejmuje swoim zakresem obszary kierowania, użytkowania i zabezpieczenia materiałowo-technicznego;
- ewidencja ilościowo-wartościowa oraz ilościowo-jakościowa** – ewidencja prowadzona w pionie głównego księgowego (ilościowo-wartościowa) oraz w pionie logistyki (ilościowo-jakościowa), z wykorzystaniem urządzeń i systemów ewidencyjno-księgowych pozwalających na ustalenie ilości, jakości i wartości sprzętu informatyki i oprogramowania WOG w celu:
- (1) rzetelnego ewidencjonowania stanów ilościowych i jakościowych środków zaopatrzenia będących w zasobach resortu obrony narodowej,
 - (2) wyceny zgromadzonych zasobów,
 - (3) odzwierciedlenia zmian w zapasach,
 - (4) odzwierciedlenia przepływu majątku pomiędzy poszczególnymi elementami struktur organizacyjnych,
 - (5) optymalizacji stanu zapasów,
 - (6) planowania i racjonalizacji zakupów;
- fundusz dyspozycyjny** – określona procentowo ilość asortymentu sprzętu informatyki i oprogramowania naliczana i utrzymywana centralnie, przeznaczona do zabezpieczenia pilnych i nieprzewidzianych potrzeb resortu obrony narodowej (np. organizacyjnych, operacyjnych);
- gestor sprzętu wojskowego (gestor SpW)** – organ w rozumieniu przepisów dotyczących określenia funkcji gestorów i centralnych organów logistycznych sprzętu wojskowego w resorcie obrony narodowej;
- jednolity indeks materiałowy (JIM)** – odpowiednio usystematyzowany, niepowtarzalny ciąg znaków alfanumerycznych pozwalający w sposób jednoznaczny zidentyfikować dany wyrób;
- informacja** – przekazywana za pomocą znaków, mowy, sygnałów, wykresów, itp., treść komunikatu przedstawiająca fakty, zdarzenia, procesy lub idee,

- która w ustalonym kontekście ma określone znaczenie;
- informatyczny nośnik danych (IND)** – materiał lub urządzenie służące do przechowywania, zapisywania i odczytywania danych w postaci cyfrowej na:
- (1) nośnikach magnetycznych (np. dyski twarde, taśmy magnetyczne, dyski ZIP, karty magnetyczne),
 - (2) nośnikach elektronicznych (np. dyski SSD, karty pamięci, urządzenia typu FlashDrive),
 - (3) nośnikach hybrydowych – stanowiących połączenie nośnika magnetycznego i elektronicznego,
 - (4) nośnikach optycznych (np. CD, DVD, BD),
 - (5) nośnikach magnetoptycznych;
- inwentaryzacja** – proces ustalenia rzeczywistego stanu składników majątkowych i źródeł ich pochodzenia na określony dzień, weryfikacja ich gospodarczej przydatności i wycena, a następnie porównanie uzyskanych stanów z ewidencją księgową, rozliczenie i wyjaśnienie różnic oraz skorygowanie stanów ewidencji tak, aby potwierdzały stan faktyczny;
- jednostka organizacyjna resortu obrony narodowej** – Ministerstwo Obrony Narodowej, jednostka organizacyjna podległa Ministrowi Obrony Narodowej, niewchodząca w skład Ministerstwa;
- kancelaria** – kancelaria tajna, kancelaria tajna międzynarodowa lub punkt ewidencyjny;
- kierownik komórki/jednostki organizacyjnej resortu obrony narodowej** – dowódca, dyrektor, komendant, szef lub inna osoba kierująca całokształtem działalności komórki lub jednostki organizacyjnej resortu obrony narodowej;
- klasa urządzenia** – wskaźnik charakteryzujący podatność danego urządzenia na infiltrację elektromagnetyczną, określony na podstawie specjalistycznych badań realizowanych przez SKW;

- komórka organizacyjna resortu obrony narodowej** – komórka organizacyjna Ministerstwa Obrony Narodowej wchodząca w skład Ministerstwa – Sekretariat Ministra, departament, zarząd, biuro;
- konflikt interesów** – sytuacja prawna lub faktyczna, w której interes prywatny (osobisty, bądź majątkowy) osoby podejmującej czynność opisaną w decyzji lub jego małżonka, a także osoby z nią spokrewnionej lub powinowaczonej lub podmiotu, który te osoby reprezentują lub z którym pozostają w jakimkolwiek stosunku faktycznym lub prawnym, wpływa, bądź może wpływać na obiektywne i bezstronne wykonanie tych czynności;
- modernizacja techniczna** – obszar zadaniowy obejmujący m.in.:
- (1) zakupy sprzętu wojskowego,
 - (2) modernizację i modyfikację sprzętu wojskowego,
 - (3) prace rozwojowe,
 - (4) zakupy innych przedmiotów i urządzeń, niż uznawane za sprzęt wojskowy, jeżeli jednostkowa wartość przedmiotu(urządzenia) lub zakres rzeczowy zamówienia wskazuje, że finansowanie zakupu będzie się odbywać w ramach wydatków majątkowych;
- modernizacja** – proces unowocześnienia SpW polegający na zmianie jego parametrów użytkowych i eksploatacyjnych, w tym w szczególności parametrów krytycznych. Wynikiem modernizacji jest nowy SpW;
- modyfikacja** – proces unowocześniania SpW polegający na wymianie, zastąpieniu lub rozbudowie istniejących podzespołów, funkcji lub oprogramowania, bez zmiany jego zasadniczego przeznaczenia. Wynikiem modyfikacji nie jest nowy SpW;
- naprawa** – zespół czynności mających na celu odtworzenie sprawności technicznej sprzętu informatyki przez usunięcie powstałych niesprawności (uszkodzeń) i wykonanie określonych czynności zgodnie z wymaganą technologią;

**normy należności
naliczeniowego sprzętu
informatyki**

- określony, w decyzji Ministra Obrony Narodowej w sprawie wprowadzenia do użytku służbowego norm należności naliczeniowego sprzętu informatyki w resorcie obrony narodowej, rodzaj oraz ilość sprzętu informatyki przysługującego użytkownikom indywidualnym (żołnierzom zawodowym, członkom korpusu służby cywilnej i pracownikom wojska) oraz użytkownikom zbiorowym (komórkom i jednostkom organizacyjnym resortu obrony narodowej);

**oprogramowanie/
produkt programowy**

- (ang. software product) zgodnie z normą PN ISO/IEC 12207 jest to „zbiór programów komputerowych, skojarzonych z nimi struktur danych (baz danych) wraz z ich dokumentacją (użytkową i techniczną)”. Może być on dystrybuowany w dwóch postaciach: Wykonywalnej/Binarnej oraz Kodu Źródłowego. Obejmuje w szczególności:

- (1) **oprogramowanie systemowe** (podstawowe, bez którego komputer nie będzie wykonywał żadnych operacji na plikach ani działań matematycznych) – kontroluje i koordynuje użycie zasobów sprzętowych poprzez różne programy użytkowe dla różnych użytkowników, jest programem, który działa, jako pośrednik między użytkownikiem komputera a sprzętem komputerowym. Zadaniem oprogramowania systemowego jest tworzenie środowiska, w którym użytkownik może wykonywać programy w wygodny i wydajny sposób,
- (2) **oprogramowanie narzędziowe** (usprawnia konfigurację lub naprawia system) – wspomaga zarządzanie zasobami sprzętowymi poprzez dogodne interfejsy użytkowe oraz usprawnia, modyfikuje oprogramowanie systemowe w celu usprawnienia wykonywania programów w bardziej wygodny i wydajny sposób, a przy tym pozbawiony błędów,

- (3) **oprogramowanie użytkowe** (zwane też aplikacyjnym, aplikacjami) – określa sposób, w jaki zostaną użyte zasoby systemowe do rozwiązywania problemów obliczeniowych zadanych przez użytkownika (kompilatory, systemy baz danych, gry, oprogramowanie biurowe, wspomaganie prac inżynierskich – CAD, itp.). Zazwyczaj jest to program komputerowy, który zapewnia interakcję użytkownika z komputerem i nie jest częścią większego programu. Z technicznego punktu widzenia jest to oprogramowanie korzystające z usług oprogramowania systemowego,
- (4) **oprogramowanie wbudowane w sprzęt** (ang. embedded software) – oprogramowanie stanowiące integralną część obsługiwanego sprzętu (firmware) lub system operacyjny wraz ze specjalizowanym oprogramowaniem, zapewniające podstawowe procedury jego wykorzystania i obsługi – np. systemy sterujące samolotami, bombami inteligentnymi, pociskami raketowymi, radiostacjami, centralami telefonicznymi, itp., ale również stosowane powszechnie systemy i sterowniki drukarek, kserokopiarek, telefonów komórkowych, pojazdów mechanicznych oraz wszelkiego rodzaju urządzeń elektromechanicznych;

organizator systemu teleinformatycznego

- kierownik jednostki organizacyjnej organizującej system teleinformatyczny lub upoważniony przez niego kierownik komórki organizacyjnej;

organizator systemu informatycznego

- jednostka (komórka) organizacyjna wyznaczona do nadzoru nad przebiegiem prac projektowo-wdrożeniowych oraz eksploatacji użytkowej systemu informatycznego, wspierającego proces planowania zasobów, usług i robót budowlanych;

Organizator Systemu Funkcjonalnego (OSF)

- organ wg decyzji Ministra Obrony Narodowej w sprawie Organizatorów Systemów Funkcjonalnych Sił Zbrojnych Rzeczypospolitej Polskiej;

- organ planujący** – organ w rozumieniu przepisów dotyczących planowania i wykonywania budżetu resortu obrony narodowej;
- plan modernizacji technicznej SZ** – centralny plan rzeczowy w rozumieniu przepisów dotyczących zasad opracowywania i realizacji centralnych planów rzeczowych;
- plany rzeczowe** – wykaz zadań/asortymentu niezbędnych do zabezpieczenia zamierzeń w roku planistycznym – sporządzane przez właściwe organy planujące, w ramach posiadanych kompetencji – na etapie wstępnego planowania budżetowego zgodnie z rozporządzeniem Ministra Finansów w sprawie szczegółowego sposobu, trybu i terminów opracowania co roku na podstawie art. 138 ust. 6 ustawy o finansach publicznych. Plany rzeczowe obejmują: centralne plany rzeczowe i decentralne plany rzeczowe;
- pododdział gospodarczy** – jednostka organizacyjna resortu obrony narodowej lub komórka organizacyjna MON posiadająca odrębny numer identyfikacyjny, eksploatująca/użytkująca sprzęt informatyki i oprogramowanie, pozostająca na zaopatrzeniu logistyczno-finansowym WOG, zgodnie z planem przydziałów gospodarczych resortu obrony narodowej. Dla dowództw RSZ, funkcję pododdziału gospodarczego może pełnić jednostka wsparcia teleinformatycznego resortu obrony narodowej realizująca zadania zabezpieczenia teleinformatycznego;
- przeklasyfikowanie** – zdarzenie gospodarcze związane ze zmianą kategorii określonych składników majątku. Efektem przeklasyfikowania może być również zmiana ceny określonych partii środków zaopatrzenia;
- przetwarzanie danych** – uporządkowane wykonywanie operacji na zbiorze danych, na przykład: operacje arytmetyczne lub operacje logiczne na danych, łączenie lub sortowanie danych, asemblowanie lub kompilowanie programów, operacje na tekście, takie jak: redagowanie, sortowanie, łączenie,

- zapamiętywanie, wyszukiwanie, wyświetlanie lub drukowanie;
- przetwarzanie informacji niejawnych** – wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;
- regionalna baza logistyczna (RBLog)** – organ wykonawczy terytorialnego systemu zabezpieczenia podporządkowany Inspektoratowi Wsparcia Sił Zbrojnych (IWsp SZ), realizujący zaopatrywanie przydzielonych na zaopatrzenie WOG, w określonym obszarze kompetencyjnej odpowiedzialności zadaniowej;
- rok budżetowy** – rok realizacji budżetu resortu obrony narodowej;
- rok planistyczny** – rok, na który planowany jest budżet resortu obrony narodowej;
- rok przedplanowy** – rok przed rokiem planistycznym;
- sieć komputerowa** – zestaw sprzętu i oprogramowania pozwalający przekazywać informacje między komputerami;
- sieć teleinformatyczna** – organizacyjne i techniczne połączenie systemów informatycznych wraz z łączącymi je urządzeniami i liniami teleinformatycznymi;
- specyfikacja** – dokument, który precyzyjnie (dokładnie) opisuje istotne wymagania funkcjonalne i techniczne, jakie powinien spełniać wyrób, proces lub usługa;
- sprawozdanie** – dokument zawierający informacje z danej dziedziny działalności, opracowywany w formie tekstowej, tabelarycznej lub graficznej, podpisany przez osobę uprawnioną i przekazywany w ustalonych przedziałach czasowych lub po wykonaniu nakazanych czynności do nadrzędnego szczebla dowodzenia (zarządzania);
- sprzęt klasy TEMPEST** – sprzęt przewidziany do przetwarzania informacji niejawnych, w którym zastosowano rozwiązania zabezpieczające przed wystąpieniem lub ograniczające zjawisko elektromagnetycznego przenikania informacji (w postaci ujawniającej emisji

- promieniowanej i przewodzonej), posiadający stosowny certyfikat wydany przez ABW lub SKW w zakresie ochrony elektromagnetycznej;
- sprzęt powszechnego użytku** – określony przez gestora SpW sprzęt powszechnie dostępny na rynku, dla którego nie są precyzowane specjalne wymagania wojskowe, powodujące konieczność zmian cech produktu;
- sprzęt wojskowy (SpW)** – wyposażenie specjalnie zaprojektowane lub zaadaptowane do potrzeb wojskowych i przeznaczone do użycia jako broń, amunicja lub materiały wojenne;
- system informatyczny** – system, który tworzą urządzenia, narzędzia, metody postępowania i procedury stosowane przez wyspecjalizowanych pracowników, w sposób zapewniający wytwarzanie, przechowywanie, przetwarzanie lub przekazywanie informacji;
- system teleinformatyczny** – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego;
- układ pamięciowy** – urządzenie służące do zapisywania, przechowywania i odczytywania informacji, które nie jest wykorzystywane samodzielnie, ale wchodzi w skład innych urządzeń. Do układów pamięciowych zalicza się m.in:
- (1) pamięci ulotne (RAM — wykorzystywane m.in. w komputerach i kartach graficznych);
 - (2) pamięci nieulotne, w tym pamięci programowalne;
- utrzymanie** – czynności obejmujące:
- (1) **naprawy** – wykonywanie napraw gwarancyjnych przez gwaranta oraz napraw pogwarancyjnych sprzętu informatyki w wojskowych warsztatach obsługowo-naprawczych lub specjalistycznych warsztatach i punktach napraw poza resortem

- obrony narodowej. Naprawy stanowią zespół czynności mających na celu odtworzenie sprawności technicznej sprzętu informatyki przez usunięcie powstałych niesprawności (uszkodzeń) i wykonanie określonych czynności zgodnie z wymaganą technologią,
- (2) **przeglądy i konserwacje** – czynności realizowane zgodnie z zasadami przewidzianymi w instrukcjach producenta lub warunkami określonymi w gwarancji,
- (3) **kontrole** – sprawdzenie stanu technicznego oraz zgodności użytkowania z przeznaczeniem;
- użytkowanie** – wykorzystanie sprzętu informatyki i oprogramowania do realizacji zadań służbowych w przewidzianym środowisku, zgodnie z dokumentacją użytkową,
- użytkownik** – komórka/jednostka organizacyjna resortu obrony narodowej (lub osoba fizyczna) wykorzystująca do realizacji zadań służbowych sprzęt informatyki i oprogramowanie, zgodnie z przeznaczeniem i normami należności, odpowiedzialna za utrzymanie jego właściwego stanu technicznego;
- wojskowy oddział gospodarczy lub komórka organizacyjna MON/jednostka organizacyjna RON pełniąca funkcję wojskowego oddziału gospodarczego (WOG)** – specjalistyczna komórka/jednostka organizacyjna resortu obrony narodowej będąca dysponentem środków budżetowych oraz organem planującym trzeciego stopnia, prowadząca samodzielną gospodarkę materiałową i finansową (w tym ewidencję ilościowo-wartościową oraz ilościowo-jakościową) dla pododdziałów własnych (organicznych) oraz struktur organizacyjnych wojska pozostających na jego zaopatrzeniu logistyczno-finansowym (pododdziały gospodarcze) zgodnie z planem przydziałów gospodarczych resortu obrony narodowej;
- wprowadzenie SpW do Sił Zbrojnych** – dyspozycja właściwego organu wojskowego w sprawie rozpoczęcia eksploatacji danego wzoru SpW w Siłach Zbrojnych;
- wsparcie teleinformatyczne** – rodzaj zabezpieczenia technicznego zapewniającego jednostce/komórcie resortu obrony

- narodowej dostęp do rozległych sieci i systemów teleinformatycznych, wsparcie w zakresie użytkowania systemów informatycznych i aplikacji usług teleinformatycznych oraz świadczenia usług telekomunikacyjnych;
- wycofanie SpW z Sił Zbrojnych** – dyspozycja właściwego organu wojskowego w sprawie całkowitego wycofania danego wzoru SpW z Sił Zbrojnych;
- zabezpieczenie teleinformatyczne** – rodzaj zabezpieczenia technicznego mający na celu zaopatrywanie jednostki/komórki organizacyjnej resortu obrony narodowej w sprzęt informatyki, oprogramowanie, techniczne środki materiałowe oraz materiały eksploatacyjne do sprzętu i urządzeń, systemy informatyczne i aplikacje usług. Obejmuje także utrzymanie, zarządzanie i administrowanie sprzętem informatyki w określonych konfiguracjach sieciowych i systemowych oraz świadczenie usług telekomunikacyjnych;
- zakup (nabywanie)** – czynności obejmujące:
- (1) **inicjowanie procesu** – rozpoczęcie procesu nabywania sprzętu informatyki i oprogramowania przez organ realizujący nabycie (realizatora zakupu), z chwilą otrzymania limitu wydatków oraz opracowanych lub uzgodnionych przez gestora SpW danych niezbędnych do przeprowadzenia postępowań o udzielenie zamówienia publicznego,
 - (2) **przygotowanie zapytania ofertowego, zamówienia publicznego** – przygotowanie materiałów, w treści zależnej od przyjętej specyfikacji. Przywołane materiały stanowić będą dokumentację wymaganą odrębnymi przepisami dla przeprowadzenia zamówienia,
 - (3) **realizację zamówienia publicznego** – wybór wykonawcy zamówienia publicznego związanego ze sprzętem informatyki lub oprogramowaniem, zgodnie z obowiązującymi procedurami,

- (4) **kontrolę procesu nabywania** – zespół procedur wspólnego przeglądu i procesu kontroli odbioru sprzętu informatyki i oprogramowania przez organ realizujący nabycie,
- (5) **odbiór zamówionych produktów** – dokonanie oceny zgodności z umową, specyfikacją lub specyfikacją istotnych warunków zamówienia oraz opisem zawartym w dowodach dostaw, przyjęcie i udokumentowanie odbioru przez komisję – wskazanej w umowie komórki/jednostki organizacyjnej – przyjmującej pozyskany produkt na swoją ewidencję ilościowo-wartościową;

zbędny sprzęt informatyki i oprogramowanie

- składniki majątku ruchomego, które:
 - (1) nie są i nie będą mogły być wykorzystane w realizacji zadań związanych z działalnością danej komórki lub jednostki organizacyjnej resortu obrony narodowej,
 - (2) są zużytym sprzętem informatyki,
 - (3) nie nadają się do współpracy ze sprzętem używanym w danej komórce lub jednostce organizacyjnej resortu obrony narodowej, a ich przystosowanie (modyfikacja lub modernizacja) byłoby technicznie i ekonomicznie nieuzasadnione,
 - (4) znajdują się na wyposażeniu polskich jednostek wojskowych poza granicami państwa, niewykorzystywane przez te jednostki do realizacji ich zadań, jeżeli ich wartość jest niższa od kosztów ich transportu do kraju lub innego miejsca możliwego użytkowania;

zestawienia potrzeb rzeczowych

- zestawienia potrzeb w zakresie sprzętu informatyki i oprogramowania sporządzane na zasadach określonych w decyzji w sprawie systemu planowania zasobów, usług i robót budowlanych w resorcie obrony narodowej oraz decyzji w sprawie zasad opracowywania i realizacji

**zużyty sprzęt
informatyki**

- centralnych planów rzeczowych;
- składniki majątku ruchomego:
 - (1) posiadające wady lub uszkodzenia, których naprawa byłaby nieopłacalna,
 - (2) zagrażające bezpieczeństwu użytkowników lub najbliższego otoczenia,
 - (3) które całkowicie utraciły wartość użytkową,
 - (4) które są technicznie przestarzałe, a ich naprawa, modyfikacja lub modernizacja byłby ekonomicznie nieuzasadniona.

LISTA AKRONIMÓW I SKRÓTÓW

ABW	– Agencja Bezpieczeństwa Wewnętrznego,
BD	– Blue-ray Disc (format zapisu optycznego, przy zastosowaniu niebieskiego lasera),
CAD	– Computer Aided Design (sprzęt komputerowy i oprogramowanie stosowane w projektowaniu technicznym),
CD	– Compact Disc (poliwęglanowy krążek z zakodowaną cyfrowo informacją do bezkontaktowego odczytu światłem lasera optycznego),
COL SpW	– centralny organ logistyczny sprzętu wojskowego,
DA MON	– Departament Administracyjny Ministerstwa Obrony Narodowej,
DG MON	– Dyrektor Generalny Ministerstwa Obrony Narodowej,
DGW	– Dowódca Garnizonu Warszawa,
DU	– dokument uzupełniający,
DVD	– Digital Versatile Disc lub Digital Video Disc (optyczny nośnik danych o standardzie zapisu podobnym do CD, lecz o większej pojemności dzięki zwiększeniu gęstości zapisu),
FIREWALL	– ściana ogniowa, zaporę sieciową,
FIRMWARE	– oprogramowanie wbudowane w urządzenie,
GESTOR SpW	– gestor sprzętu wojskowego,
HRF	– High Readiness Forces (Siły Wysokiej Gotowości),
IND	– informatyczne nośniki danych,
IDS	– Intrusion Detection System (systemy wykrywania włamań),
IPS	– Intrusion Prevention System (systemy zapobiegania włamaniom),
ISI	– Inspektorat Systemów Informacyjnych,
IWsp SZ	– Inspektorat Wsparcia Sił Zbrojnych,
JIM	– Jednolity Indeks Materiałowy,

JW	– Jednostka Wojskowa,
KG ŻW	– Komendant Główny Żandarmerii Wojskowej,
LAIS	– lista akronimów i skrótów,
MON	– Ministerstwo Obrony Narodowej,
NATO	– North Atlantic Treaty Organization (Organizacja Traktatu Północnoatlantyckiego),
OEM	– Original Equipment Manufacturer (Producent Oryginalnego Wyposażenia),
PKW	– Polskie Kontyngenty Wojskowe,
RAM	– Random Access Memory (pamięć o dostępie swobodnym – rodzaj pamięci cyfrowej o bezpośrednim dostępie, w którym możliwy jest wielokrotny i łatwy zapis),
RBlog	– Regionalna Baza Logistyczna,
RCZPI	– Resortowe Centrum Zarządzania Projektami Informatycznymi,
RON	– resort obrony narodowej,
RP	– Rzeczpospolita Polska,
RWP	– rejestr wydanych przedmiotów,
SKW	– Służba Kontrwywiadu Wojskowego,
SpW	– sprzęt wojskowy,
SSD	– Solid State Drive lub Solid State Disc (urządzenie pamięci masowej zbudowane w oparciu o pamięć flash),
SU	– strony użytkowe,
SZ RP	– Siły Zbrojne Rzeczypospolitej Polskiej,
UE	– Union European (Unia Europejska)
UPS	– Uninterruptible Power Supply (systemy zasilania bezprzerwowego),
WOG	– wojskowy oddział gospodarczy lub komórka organizacyjna MON/jednostka organizacyjna resortu obrony narodowej pełniąca funkcję wojskowego oddziału gospodarczego,

- WP** – Wojsko Polskie,
- WWW** – strona internetowa
- WZ** – wydanie na zewnątrz (dowód dostawy),
- ZIP** – zip (jeden z najczęściej używanych formatów kompresji i archiwizacji danych).

WYKAZ DOKUMENTÓW ŹRÓDŁOWYCH

1. Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2014 r., poz. 1502, 1662, j.t.).
2. Ustawa z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2013 r., poz. 907, z późn. zm.).
3. Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2013 r., poz. 330, j.t. z późn. zm.).
4. Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2013 r., poz. 885, z późn. zm.).
5. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2006 r. Nr 90, poz. 631, z późn. zm.).
6. Ustawa z dnia 30 maja 1996 r. o gospodarowaniu niektórymi składnikami mienia Skarbu państwa oraz o Agencji Mienia Wojskowego (Dz. U. z 2013 r., poz. 712, z późn. zm.).
7. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228).
8. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011 r. Nr 159, poz. 948).
9. Rozporządzenie Ministra Obrony Narodowej z dnia 21 listopada 2001 r. w sprawie odpowiedzialności majątkowej żołnierzy za wyrządzone przez nich szkody (Dz. U. z 2001 r. Nr 138, poz. 1557).
10. Rozporządzenie Ministra Obrony Narodowej z dnia 1 czerwca 2004 r. w sprawie szczegółowego trybu przekazywania mienia ruchomego Skarbu Państwa Agencji Mienia Wojskowego (Dz. U. z 2004 r., Nr 140, poz. 1482).
11. Rozporządzenie Ministra Obrony Narodowej z dnia 29 maja 2014 r. w sprawie szczegółowego trybu przekazywania mienia ruchomego Skarbu Państwa będącego we władaniu jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych (Dz. U. z 2014 r., poz. 759).
12. Decyzja Nr 412/MON Ministra Obrony Narodowej z dnia 20 października 2014 r. w sprawie systemu planowania zasobów, usług i robót budowlanych w resorcie obrony narodowej (Dz. Urz. MON z 2014 r., poz. 335).
13. Decyzja Nr 63/MON Ministra Obrony Narodowej z dnia 4 marca 2014 r. w sprawie planowania i wykonywania budżetu resortu obrony narodowej (Dz. Urz. MON z 2014 r., poz. 76).

14. Decyzja Nr 103/MON Ministra Obrony Narodowej z dnia 31 marca 2014 r. w sprawie zasad opracowywania i realizacji centralnych planów rzeczowych (Dz. Urz. MON z 2014 r., poz. 105).
15. Decyzja Nr 435/MON Ministra Obrony Narodowej z dnia 24 grudnia 2013 r. w sprawie określenia funkcji gestorów i centralnych organów logistycznych sprzętu wojskowego w resorcie obrony narodowej (Dz. Urz. MON z 2013 r., poz. 390).
16. Decyzja Nr 56/Org./P5 Ministra Obrony Narodowej z dnia 29 marca 2010 r. w sprawie Organizatorów Systemów Funkcjonalnych Sił Zbrojnych Rzeczypospolitej Polskiej (niepublikowana w Dz. Urz. MON).
17. Decyzja Nr 11/MON Ministra Obrony Narodowej z dnia 20 stycznia 2014 r. w sprawie wprowadzenia w resorcie obrony narodowej „Zasad opracowywania, aktualizacji doktryn i dokumentów doktrynalnych”, DA-01 (Dz. Urz. MON z 2014 r., poz. 21).
18. Decyzja Nr 42/Log./P4 Ministra Obrony Narodowej z dnia 02 lipca 2014 r. w sprawie wprowadzenia w resorcie obrony narodowej „Zasad opracowywania dokumentów logistycznych w resorcie obrony narodowej, DA-04” oraz upoważnienia Szefa Sztabu Generalnego WP do wprowadzania dokumentów oznaczonych cechą „Log./P4” do użytku w formie decyzji Ministra Obrony Narodowej (niepublikowana w Dz. Urz. MON).
19. Decyzja Nr 72/MON Ministra Obrony Narodowej z dnia 25 marca 2013 r. w sprawie pozyskiwania sprzętu wojskowego i usług dla Sił Zbrojnych Rzeczypospolitej Polskiej (Dz. Urz. MON z 2013 r., poz. 78, z późn. zm.).
20. Decyzja Nr 218/MON Ministra Obrony Narodowej z dnia 6 czerwca 2014 r. w sprawie planowania i rozliczania działalności w resorcie obrony narodowej (Dz. Urz. MON z 2014 r., poz. 179).
21. Decyzja Nr 207/MON Ministra Obrony Narodowej z dnia 25 czerwca 2009 r. w sprawie opracowania, wprowadzania i aktualizacji „Wykazu obowiązujących standardów sprzętu informatyki i oprogramowania do stosowania w resorcie obrony narodowej” (Dz. Urz. MON z 2009 r., Nr 13, poz. 145).
22. Decyzja Nr 464/MON Ministra Obrony Narodowej z dnia 13 grudnia 2010 r. w sprawie wprowadzenia do użytku służbowego „Norm należności naliczeniowego sprzętu informatyki w resorcie obrony narodowej (Dz. Urz. MON z 2010 r. Nr 23, poz. 317).
23. Decyzja Nr 230/MON Ministra Obrony Narodowej z dnia 20 czerwca 2011 r. w sprawie gospodarowania niektórymi składnikami mienia Skarbu Państwa będącego we władaniu komórek organizacyjnych Ministerstwa Obrony

Narodowej jednostek podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych (Dz. Urz. MON z 2011 r., poz. 185, z późn. zm.).

24. Decyzja Nr 46/MON Ministra Obrony Narodowej z dnia 21 lutego 2013 r. w sprawie zagospodarowania mienia ruchomego Skarbu Państwa będącego na wyposażeniu Polskiego Kontyngentu Wojskowego w Islamskiej Republice Afganistanu, niewykorzystywanego do realizacji jego zadań (niepublikowana w Dz. Urz. MON).
25. Decyzja Nr 88/MON Ministra Obrony Narodowej z dnia 20 marca 2014 r. zmieniającą decyzję w sprawie zagospodarowania mienia ruchomego Skarbu Państwa będącego na wyposażeniu Polskiego Kontyngentu Wojskowego w Islamskiej republice Afganistanu, niewykorzystywanego do realizacji jego zadań (niepublikowana w Dz. Urz. MON).
26. Decyzji Nr 444/MON Ministra Obrony Narodowej z dnia 30.12.2013 r. w sprawie zasad wprowadzania do Sił Zbrojnych Rzeczypospolitej Polskiej sprzętu wojskowego oraz wycofywania sprzętu wojskowego nieodpowiadającego wymaganiom wojska (Dz. Urz. MON z 2013 r., poz. 397).
27. Decyzja Nr 32/14 Podsekretarza Stanu Ministerstwa Obrony Narodowej pani Beaty OCZKOWICZ z dnia 26 maja 2014 r. w sprawie wprowadzenia do stosowania wytycznych w sprawie szczegółowych zasad planowania i przekazywania Agencji Mienia Wojskowego i Wojskowej Agencji Mieszkaniowej niektórych składników mienia Skarbu Państwa.

ARKUSZ ZMIAN

Numer zmiany	Nr stron wyłączonych/ włączonych	Nr wykreślonego, dodanego lub zmienionego punktu	Data i podstawa wprowadzenia zmiany	Informacje uzupełniające (w tym zakres dokonanej zmiany)