Warszawa, dnia 8 października 2012 r.

Poz. 52

ZARZĄDZENIE NR 132
KOMENDANTA GŁÓWNEGO POLICJI

z dnia 5 października 2012 r.

zmieniające zarządzenie w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych i innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego informacji niejawnych w Policji

Na podstawie art. 47 ust. 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228) zarządza się, co następuje:

§ 1. W zarządzeniu nr 2020 Komendanta Głównego Policji z dnia 30 grudnia 2010 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych i innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego informacji niejawnych w Policji (Dz. Urz. KGP z 2011 r. Nr 1, poz. 5) wprowadza się następujące zmiany:

1) w § 1:

a) w pkt 4 uchyla się lit. c,

b) pkt 6 otrzymuje brzmienie:

„6) dobór i stosowanie środków bezpieczeństwa fizycznego.”;

2) w § 2 ust. 1 uchyla się pkt 4, 6, 10 i 12-14;

3) w § 19:

a) ust. 1 otrzymuje brzmienie:

„1. W kancelarii prowadzi się następujące urządzenia ewidencyjne:

1) rejestr dzienników ewidencji i teczek;

2) dziennik ewidencyjny;

3) książkę doręczeń przesyłek miejscowych;

4) wykaz przesyłek nadanych;

5) rejestr wydanych przedmiotów.”,

b) po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. Wzory urządzeń ewidencyjnych, o których mowa w ust. 1, określają odpowiednio załączniki nr 1, 2, 4, 5 i 6 do rozporządzenia Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. Nr 276, poz. 1631).”;

4) § 21 otrzymuje brzmienie:

„1. Urządzenia ewidencyjne określone w § 19 ust. 1 pkt 2, 3, 5 i ust. 5 podlegają zarejestrowaniu w rejestrze dzienników ewidencji i teczek, który jest nadrzędnym urządzeniem ewidencyjnym w stosunku do innych urządzeń prowadzonych przez kancelarię i nie podlega ewidencjonowaniu.

2. Urządzenia ewidencyjne, o których mowa w § 19 ust. 1 pkt 2, 3, 5 i ust. 5, oraz ich kolejne tomy rejestruje się pod odrębnymi pozycjami.”;

5) w § 22:

a) ust. 1 otrzymuje brzmienie:

„1. Informację o zarejestrowaniu urządzenia ewidencyjnego, o którym mowa w § 19, w rejestrze dzienników ewidencji i teczek odnotowuje się na karcie tytułowej tego urządzenia.”,

b) ust. 5 otrzymuje brzmienie:

„5. W urządzeniu ewidencyjnym, o którym mowa w § 19 ust. 1 pkt 2, umieszcza się na środku na górze i dole karty tytułowej i okładki odpowiednią klauzulę tajności.”,

c) ust. 6 otrzymuje brzmienie:

„6. Czynności, o których mowa w ust. 2-4, dokonuje się także w stosunku do urządzenia ewidencyjnego, o którym mowa w § 19 ust. 1 pkt 2, 3, 5 i ust. 5.”;

6) § 25 otrzymuje brzmienie:

„§ 25. 1. W przypadku stwierdzenia uszkodzenia otrzymanej przesyłki lub śladów jej otwierania pracownik kancelarii kwitujący odbiór przesyłki sporządza w obecności doręczającego, w trzech jednobrzmiących egzemplarzach, protokół w sprawie uszkodzenia przesyłki. Pierwszy egzemplarz przekazuje się nadawcy, drugi doręczającemu, a trzeci pozostaje w kancelarii przyjmującej przesyłkę.

2. Wzór protokołu w sprawie uszkodzenia przesyłki określa załącznik nr 1 do rozporządzenia Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. Nr 271, poz. 1603).”;

7) § 26 otrzymuje brzmienie:

„§ 26. Wysłanie z kancelarii przesyłek na podstawie wykazu przesyłek nadanych obejmuje:

1) porównanie ilości przesyłek otrzymanych i przeznaczonych do wysłania z ilością pozycji w wykazie przesyłek nadanych;

2) sprawdzenie całości opakowania i prawidłowości oznaczenia oraz zaadresowania przesyłek;

3) zapakowanie przesyłki w kopertę zewnętrzną i jej zaadresowanie, zabezpieczenie w sposób uniemożliwiający nieuprawniony dostęp do zawartości, a także ostemplowanie pieczęcią nagłówkową i oznaczenie numerem wykazu;

4) wpisanie przesyłki do wykazu przesyłek nadanych sporządzonego w dwóch egzemplarzach;

5) kontrolę ilości przesyłek z ilością pozycji w wykazie przesyłek nadanych;

6) przekazanie całości korespondencji wraz z jednym egzemplarzem wykazu przesyłek nadanych kurierowi poczty specjalnej, który potwierdza jej odbiór podpisem, zapisem liczbowym i słownym ilości przyjętych przesyłek oraz odciskiem pieczęci "do pakietów".”;

8) w § 29 ust. 5 otrzymuje brzmienie:

„5. Wzór karty zapoznania się z dokumentem określa załącznik nr 3 do rozporządzenia, o którym mowa w § 19 ust. 1a.”;

9) w § 33 ust. 5 otrzymuje brzmienie:

„5. W przypadku odłączenia od pisma przewodniego jednego lub więcej załączników, w rubryce dziennika ewidencyjnego "Adnotacje o wysłaniu dokumentu lub załącznika (pozycja w książce doręczeń przesyłek miejscowych/ pozycja wykazu przesyłek nadanych/załącznik do pisma nr…)" zamieszcza się adnotację, zawierającą jedną z następujących informacji:

1) "załączniki odesłano przy dokumencie nr …" (należy podać numer z dziennika ewidencyjnego, za którym przesłano dokument wraz z załącznikami);

2) "załącznik nr … odesłano przy dokumencie nr …" (należy podać, który załącznik odesłano oraz jakim numerem oznaczono dokument w dzienniku ewidencyjnym).”;

10) Rozdział 6 otrzymuje brzmienie:

„**Rozdział 6**

Przetwarzanie informacji niejawnych na informatycznych nośnikach danych

§ 37. 1. Informatyczne nośniki danych, zwane dalej w skrócie „IND”, z utrwalonymi na nich dokumentami elektronicznymi podlegają rejestracji w rejestrze wydanych przedmiotów w kancelarii tajnej komórki wprowadzającej IND do eksploatacji.

2. Otrzymane IND z utrwalonymi na nich dokumentami elektronicznymi podlegają procedurze określonej w § 27. Przesyłanie IND odbywa się za pismem.

3. Dokumenty elektroniczne podlegają zaewidencjonowaniu w dzienniku ewidencyjnym. Dokumenty elektroniczne i dokumenty nieelektroniczne posiadające tę samą treść oznaczane są tą samą sygnaturą literowo-cyfrową.

4. Wydruki dokumentów elektronicznych z IND podlegają zarejestrowaniu w dzienniku ewidencyjnym.

5. Klauzulę tajności nanosi się, o ile to możliwe, na dokumencie elektronicznym.

6. W rejestrze wydanych przedmiotów powinien być wpisany numer seryjny IND.

§ 38. 1. Dokument elektroniczny oznacza się metryką, o której mowa w rozporządzeniu Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. Nr 288, poz. 1692).

2. Treść metryki dokumentu elektronicznego określają przepisy rozporządzenia, o którym mowa w ust. 1.

3. Metryka dokumentu elektronicznego stanowi jego integralną część.

4. IND w postaci dysków twardych indywidualnych oraz będących elementami macierzy dyskowych, służące do przetwarzania informacji niejawnych powinny posiadać naniesione w sposób trwały oznaczenie zawierające:

1) numer, pod którym IND jest zarejestrowany w rejestrze wydanych przedmiotów;

2) klauzulę tajności IND.

5. Na IND stanowiące macierz dyskową lub na IND w innych stanowiskach, w których nie ma dostępu do IND, numer rejestru wydanych przedmiotów umieszcza się na obudowie IND.

6. Sposób postępowania z materiałami zawierającymi informacje niejawne wykorzystywane w urządzeniach lub systemach przeznaczonych do wykonywania czynności operacyjno-rozpoznawczych, w szczególności z urządzeniami, częściami urządzeń lub IND określono w rozporządzeniu, o którym mowa w ust.1.

7. Dopuszcza się wykorzystywanie IND przeznaczonych do utrwalania informacji niejawnych w postaci dokumentów elektronicznych przez użytkowników określonego systemu teleinformatycznego, jeżeli dokumentacja bezpieczeństwa systemu teleinformatycznego tego nie zabrania, ale tylko w niezbędnym zakresie oraz po spełnieniu, w przypadku IND typu pamięć USB lub karta pamięci, następujących warunków:

1) IND musi posiadać jednoznacznie odczytywalny numer seryjny;

2) system operacyjny jest tak skonfigurowany, iż tylko dopuszczone IND są przez niego wykrywane.

8. Dopuszcza się wykorzystanie IND do przetwarzania informacji jawnych, w systemach niejawnych, w celu realizacji niezbędnych zadań Policji po zaewidencjonowaniu ich w wykazie prowadzonym przez kierownika komórki organizacyjnej, który dla IND określonych w ust. 7 pkt 1 musi zawierać ich numer seryjny.

9. Wynoszenie lub wywożenie niejawnych IND poza strefy ochronne powinno być dozwolone jedynie pod warunkiem zastosowania certyfikowanych, kryptograficznych metod ochrony lub przez spełnienie wymagań określonych w przepisach rozporządzenia, o którym mowa w § 25 ust. 2.

10. W przypadku niejawnych IND zalecane jest szyfrowanie znajdujących się na nich informacji algorytmem AES-256 z 8-znakowym hasłem dla informacji o klauzuli niższej niż tajne i 14-znakowym hasłem w innych przypadkach.

§ 39. 1. Informacje niejawne w postaci dokumentów elektronicznych wolno przetwarzać wyłącznie na zarejestrowanych IND przygotowanych według zasad określonych w § 37 i § 38. IND typu pamięć USB oraz karta pamięci należy uprzednio sprawdzić pod kątem prawidłowości jednoznacznie odczytywalnego numeru seryjnego.

2. Zapisywanie dokumentów jawnych na IND jest dozwolone, jeżeli tworzą razem z utrwalonymi na nich niejawnymi dokumentami elektronicznymi całość sprawy.

3. Formatowanie IND w postaci dysku twardego stanowiska systemu przetwarzającego informacje niejawne oraz wszystkie operacje wykonane na tym IND wymagają odnotowania tego faktu w odpowiednim dzienniku stanowiska komputerowego dla określonego systemu.

4. Zabrania się zapisu na IND informacji prywatnych.

5. Zabrania się rejestrowania prywatnych IND.

§ 40. 1. IND z utrwalonymi na nich dokumentami elektronicznymi należy chronić przed zniekształceniem bądź zniszczeniem zapisanej informacji pod wpływem temperatury, pól elektrycznych, magnetycznych i innych czynników.

2. IND z utrwalonymi na nich dokumentami elektronicznymi powinny być przechowywane w opakowaniu ochronnym.

3. Każdy użytkownik zobowiązany jest do okresowej kontroli stanu technicznego posiadanych IND, przy czym w przypadku stwierdzenia nieprawidłowości polegającej na niemożliwości odczytu, zapisu lub innego uszkodzenia, powinien zgłosić ten fakt do pełnomocnika ochrony, który podejmie decyzję o dalszym postępowaniu.

§ 41. 1. Zabronione jest wynoszenie lub wywożenie niejawnych IND poza jednostkę organizacyjną, w związku z naprawą lub konserwacją sprzętu komputerowego przez podmioty zewnętrzne.

2. W przypadku cyklicznej wymiany informacji niejawnych z instytucjami spoza Policji zaleca się używanie grupy IND dedykowanych dla każdej z tych instytucji.

§ 42. 1. Uszkodzone niejawne IND podlegają zniszczeniu fizycznemu, przy czym przed fizycznym zniszczeniem IND należy, o ile jest to możliwe, dokonać usunięcia z niego danych.

2. Niszczenie niejawnych IND zarządza kierownik komórki organizacyjnej Komendy Głównej Policji, w której zaewidencjonowano IND z dokumentem elektronicznym, powołując komisję, w skład której wchodzą:

1) przedstawiciel komórki organizacyjnej, na której stanie jest zaewidencjonowany IND;

2) kierownik kancelarii tajnej lub osoba przez niego upoważniona, a w uzasadnionych przypadkach inspektor bezpieczeństwa teleinformatycznego lub osoba przez niego upoważniona;

3) użytkownik IND lub inna osoba upoważniona przez jego przełożonego;

4) przedstawiciel pionu informatyki – gdy zachodzi konieczność wymontowania IND z chroniącej go obudowy.

3. W przypadku terenowych jednostek organizacyjnych lub komórek organizacyjnych kierownik tej jednostki lub komórki, w porozumieniu z inspektorem bezpieczeństwa teleinformatycznego lub pełnomocnikiem ochrony, powołuje komisję, o której mowa w ust. 2, w skład której wchodzą:

1) przedstawiciel jednostki organizacyjnej lub komórki organizacyjnej, na której stanie jest zaewidencjonowany niejawny IND;

2) inspektor bezpieczeństwa teleinformatycznego lub wyznaczony przez pełnomocnika ochrony policjant lub pracownik pionu ochrony celem merytorycznego nadzoru;

3) lokalny przedstawiciel pionu informatyki, gdy zachodzi konieczność wymontowania IND z chroniącej go obudowy.

4. Kierownik jednostki organizacyjnej lub komórki organizacyjnej, o której mowa w ust. 3, może nie powoływać komisji, lecz przekazać zakwalifikowany do fizycznego zniszczenia niejawny IND do kancelarii tajnej macierzystej jednostki organizacyjnej lub komórki organizacyjnej.

5. Każdorazowo przed zniszczeniem niejawnego IND w postaci dysku twardego, dyskietki lub dysku magnetooptycznego, sam nośnik informacji musi zostać wymontowany z chroniącej go obudowy.

6. Komisja, o której mowa w ust. 2 i 3, każdorazowo określa konkretny sposób zniszczenia, w zależności od rodzaju i typu IND oraz innych lokalnych możliwości.

§ 43. 1. Zniszczenia niejawnych IND wykonanych z plastiku, w szczególności: CD, DVD, FDD, MO, kart magnetycznych i mikroprocesorowych, można dokonać w niszczarkach zapewniających odpowiedni do klauzuli tajności stopień poziomu bezpieczeństwa według normy DIN32757-1.

2. Niszczarki, o których mowa w ust. 1, powinny spełniać następujące normy:

1) dla klauzuli "tajne" lub "ściśle tajne":

   a) poziom bezpieczeństwa 3-go stopnia: paski ≤ szer. 4 mm i dł. 80 mm lub fragmenty o powierzchni ≤ 320 mm^2,

   b) poziom bezpieczeństwa 2-go stopnia: paski ≤ szer. 6 mm lub fragmenty o powierzchni ≤ 800 mm^2 pod warunkiem zastosowania dodatkowych procedur ochrony (przykładowo wymieszania powstałej masy plastikowej z identyczną masą plastikową po nośnikach zawierających informacje jawne, następnie rozdzielenia całości i wrzucenia do kilku pojemników na odpady plastikowe);

2) dla klauzuli zastrzeżone lub poufne - poziom bezpieczeństwa 2-go stopnia: paski nie szersze niż 6 mm lub fragmenty o powierzchni ≤ 800 mm^2.

3. Zniszczenia IND na podłożu metalowym można dokonać poprzez mechaniczne usunięcie z metalowego podłoża warstwy magnetycznej zawierającej informacje lub spalenie, rozpuszczenie, rozdrobnienie (pocięcie) na kawałki ≤ szer. 4 mm i dł. 80 mm lub ≤ szer. 2 mm przy powierzchni ≤ 594 mm^2 lub fragmenty o powierzchni ≤ 320 mm^2.

4. Zniszczenia IND można dokonać poprzez rozpuszczenie, rozdrobnienie, mechaniczne zmiażdżenie prasą lub młotem.

5. Kierownik jednostki organizacyjnej lub kierownik komórki organizacyjnej, w której jest zaewidencjonowany IND, odpowiada za zapewnienie koniecznej pomocy do jego zniszczenia przez, odpowiednio, inne jednostki organizacyjne lub podmioty świadczące usługi w zakresie niszczenia i utylizacji nośników albo inne komórki organizacyjne.

6. W przypadku niszczenia IND przy wykorzystaniu urządzeń podmiotu zewnętrznego należy sprawdzić czy ten podmiot posiada opracowane procedury niszczenia, przedstawia dokumentację przeprowadzenia procesu zniszczenia IND i utylizacji produktów zniszczenia.

7. Niejawne IND w postaci:

1) dysków twardych;

2) pamięci typu „flash” - pamięci pozwalającej na zapisywanie i kasowanie wielu komórek pamięci podczas operacji programowania,

przed przekazaniem do zniszczenia podmiotowi zewnętrznemu muszą być uszkodzone mechanicznie poprzez wywiercenie w nośniku minimum 5 otworów Φ 6 mm lub zdeformowanie mechaniczne wykonane młotem lub prasą, eliminujące możliwość bezpośredniego odczytania informacji po

podłączeniu do komputera, a dokument przekazujący musi zawierać ich numery seryjne i numery rejestracji w rejestrze wydanych przedmiotów.

§ 44. 1. Deklasyfikacja IND polega na zmianie oznaczenia klauzuli tajności bądź jej zniesieniu.

2. Deklasyfikacja IND dopuszczalna jest tylko dla informacji niejawnych oznaczonych klauzulą "zastrzeżone" oraz "poufne".

3. Niedopuszczalna jest deklasyfikacja IND, na których były przetwarzane informacje niejawne oznaczane klauzulą "tajne" lub "ściśle tajne".

§ 45. 1. Wycofanie niejawnego IND z użycia lub jego deklasyfikacja jest możliwa wyłącznie po przeprowadzeniu skutecznego, nieodwracalnego usunięcia zapisanych tam dokumentów elektronicznych lub utraty cech funkcjonalnych IND.

2. Skutecznego, nieodwracalnego usunięcia zapisanych dokumentów elektronicznych na IND magnetycznych dokonuje się poprzez ich demagnetyzację, z wyjątkiem dysków magnetooptycznych, natomiast dla pozostałych IND, z wyjątkiem dysków optycznych, poprzez trzykrotne nadpisanie zapisanej tam informacji oraz pozostałej wolnej przestrzeni IND metodą US DoD 5220.22-M.

3. Deklasyfikacji nie podlegają niejawne IND optyczne i magnetooptyczne jednokrotnego ani wielokrotnego zapisu.

4. Deklasyfikacji dysku twardego (pomimo że dysk twardy należy do nośników magnetycznych) można dokonać jedynie poprzez trzykrotne nadpisanie zapisanej tam informacji oraz pozostałej wolnej przestrzeni IND metodą US DoD 5220.22-M, ponieważ konstrukcja dysku twardego zawiera elektroniczne znaczniki ścieżek, które podczas procesu demagnetyzacji są usuwane, powodując niemożność dalszej jego eksploatacji, przy czym poprawność deklasyfikacji dysku twardego należy po zakończeniu czynności zweryfikować.

§ 46. 1. Kancelaria tajna lub komórka organizacyjna, w której jest zaewidencjonowany zdeklasyfikowany niejawny IND, prowadzi zatwierdzony przez pełnomocnika ochrony wykaz zdeklasyfikowanych IND, który powinien zawierać typ IND, numer protokołu deklasyfikacji wraz z datą, nazwisko i imię osoby, na której stanie znajduje się IND, oraz nazwę komórki organizacyjnej.

2. Zwrot IND do kancelarii tajnej może nastąpić wyłącznie po usunięciu zapisanych tam dokumentów elektronicznych z wyłączeniem IND deponowanych tam tymczasowo lub podlegających archiwizacji.

§ 47. 1. Usuwanie zapisanych na IND dokumentów elektronicznych odbywa się na zasadach jak dla dokumentów nieelektronicznych.

2. Fakt deklasyfikacji lub zniszczenia niejawnego IND potwierdza się protokołem deklasyfikacji lub zniszczenia, którego wzór określa załącznik nr 10 do zarządzenia.

§ 48. Kierownik lub pracownik kancelarii tajnej, odpowiedzialny za przetwarzanie materiałów niejawnych, w których jest zarejestrowany IND, na podstawie zatwierdzonego protokołu przeprowadza aktualizację rejestracji w rejestrze wydanych przedmiotów.

§ 49. Bieżąca kontrola użytkowania IND zarejestrowanego w rejestrze wydanych przedmiotów jest przeprowadzana przez inspektora bezpieczeństwa teleinformatycznego każdorazowo, podczas wykonywania czynności określonych w art. 52 ust. 1 pkt 1 ustawy oraz na każde polecenie kierownika jednostki organizacyjnej lub kierownika komórki organizacyjnej albo pełnomocnika ochrony.”;

11) Rozdział 7 otrzymuje brzmienie:

„**Rozdział 7**

Dobór i stosowanie środków bezpieczeństwa fizycznego

§ 50. 1. System bezpieczeństwa informacji niejawnych obejmuje środki bezpieczeństwa fizycznego stosowane w celu zapewnienia poufności, integralności i dostępności tych informacji.

2. W zależności od określonego w jednostkach organizacyjnych poziomu zagrożeń dla pomieszczeń lub obszarów, należy stosować odpowiednią kombinację następujących środków bezpieczeństwa fizycznego:

1) personel bezpieczeństwa – osoby przeszkolone, nadzorowane, a w razie konieczności posiadające odpowiednie uprawnienie do dostępu do informacji niejawnych, wykonujące czynności związane z fizyczną ochroną informacji niejawnych, w tym:

   a) kontrolę dostępu do pomieszczeń lub obszarów, w których przetwarzane są informacje niejawne,

   b) nadzór nad systemem dozoru wizyjnego,

   c) reagowanie na zagrożenia, alarmy lub sygnały awaryjne;

2) bariery fizyczne – środki chroniące granice miejsca, w którym przetwarzane są informacje niejawne, w szczególności:

   a) drzwi,

   b) zamki,

   c) okna,

   d) ściany,

   e) bramy,

   f) ogrodzenia;

3) szafy i zamki – stosowane do przechowywania informacji niejawnych lub zabezpieczające te informacje przed nieuprawnionym dostępem;

4) system kontroli dostępu – stosowany w celu zagwarantowania dostępu do pomieszczenia lub obszaru, w którym przetwarzane są informacje niejawne, wyłącznie przez osoby posiadające odpowiednie uprawnienia, obejmujący:

   a) rozwiązania organizacyjne,

   b) elektroniczny system pomocniczy;

5) system sygnalizacji włamania i napadu – elektroniczny system pomocniczy stosowany w celu realizacji procedur ochrony informacji niejawnych oraz podwyższenia poziomu bezpieczeństwa, który zapewniają:

   a) bariery fizyczne,

   b) zastępujący lub wspierający personel bezpieczeństwa w pomieszczeniach i budynkach;

6) system dozoru wizyjnego – elektroniczny system pomocniczy stosowany w celu bieżącego monitorowania ochronnego lub sprawdzania incydentów bezpieczeństwa i sygnałów alarmowych przez personel bezpieczeństwa;

7) system kontroli osób i przedmiotów – stosowany w celu zapobiegania próbom nieuprawnionego wnoszenia na chroniony obszar rzeczy zagrażających bezpieczeństwu informacji niejawnych lub nieuprawnionego wynoszenia informacji niejawnych z obiektów, obejmujący:

   a) rozwiązania organizacyjne polegające na dobrowolnym poddaniu się kontroli lub udostępnieniu do kontroli rzeczy osobistych,

   b) elektroniczny system pomocniczy.

3. W celu zapewnienia poufności, integralności i dostępności informacji niejawnych można zastosować również środki bezpieczeństwa fizycznego inne niż wymienione w ust. 2, jeżeli taka potrzeba wynika z analizy poziomu zagrożeń.

4. Środki bezpieczeństwa fizycznego zalecane do stosowania w strefach ochronnych określa załącznik nr 1 do zarządzenia.

§ 51. Kierownicy terenowych komórek organizacyjnych Centralnego Biura Śledczego Komendy Głównej Policji lub Biura Spraw Wewnętrznych Komendy Głównej Policji w porozumieniu z właściwymi miejscowo pełnomocnikami ochrony przygotują plany ochrony informacji niejawnych. Plany te będą stanowiły załączniki do planów ochrony informacji niejawnych komend wojewódzkich (Stołecznej) Policji.”;

12) uchyla się załączniki nr 2 – 7 oraz 11 i 12;

13) dodaje się załącznik nr 13 w brzmieniu określonym w załączniku nr 1 do niniejszego zarządzenia;

14) załącznik nr 10 otrzymuje brzmienie określone w załączniku nr 2 do niniejszego zarządzenia;

15) użyte w zarządzeniu w różnych przypadkach wyrazy „dziennik ewidencji” zastępuje się wyrazami „dziennik ewidencyjny”.

§ 2. 1. Formularze urządzeń ewidencyjnych stosowane według dotychczasowych wzorów mogą być wykorzystywane do wyczerpania zapasów, nie dłużej jednak niż do dnia 31 grudnia 2013 r.

2. Kierownicy jednostek organizacyjnych, w terminie 3 lat od dnia wejścia w życie zarządzenia, określą dobór i stosowanie środków bezpieczeństwa fizycznego zgodnie z niniejszym zarządzeniem.

§ 3. Zarządzenie wchodzi w życie po upływie 14 dni od dnia podpisania.

Komendant Główny Policji

z up. Zastępca Komendanta Głównego Policji
nadinsp. Andrzej ROKITA

Załączniki do zarządzenia nr 132
Komendanta Głównego Policji
z dnia 5 października 2012 r.

Załącznik nr 1

ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO
ZALECANE DO STOSOWANIA W STREFACH OCHRONNYCH

STREFA OCHRONNA	POZIOM ZAGROŻENIA	ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO
STREFA III	POZIOM NISKI	Kontrola dostępu do pomieszczeń i obszarów lub stosowanie barier fizycznych chroniących granice miejsca.
	POZIOM ŚREDNI	1. Kontrola dostępu do pomieszczeń i obszarów lub stosowanie barier fizycznych chroniących granice miejsca. 2. Reagowanie na zagrożenia, alarmy lub sygnały awaryjne.
	POZIOM WYSOKI	1. Kontrola dostępu do pomieszczeń i obszarów lub stosowanie barier fizycznych chroniących granice miejsca. 2. Reagowanie na zagrożenia, alarmy lub sygnały awaryjne. 3. Inne środki bezpieczeństwa fizycznego wynikające z określonego poziomu zagrożeń.
STREFA II	POZIOM NISKI	1. Kontrola dostępu do pomieszczeń i obszarów lub system kontroli dostępu. 2. Szafy i zamki. 3. Inne środki bezpieczeństwa fizycznego wynikające z określonego poziomu zagrożeń.
	POZIOM ŚREDNI	1. Kontrola dostępu do pomieszczeń i obszarów lub system kontroli dostępu. 2. Reagowanie na zagrożenia, alarmy lub sygnały awaryjne. 3. Szafy i zamki. 4. Inne środki bezpieczeństwa fizycznego wynikające z określonego poziomu zagrożeń.
	POZIOM WYSOKI	1. Kontrola dostępu do pomieszczeń i obszarów lub system kontroli dostępu. 2. Nadzór nad systemem dozoru wizyjnego. 3. Reagowanie na zagrożenia, alarmy lub sygnały awaryjne. 4. Szafy i zamki. 5. Inne środki bezpieczeństwa fizycznego wynikające z określonego poziomu zagrożeń.
STREFA I	POZIOM NISKI	1. System kontroli dostępu. 2. Bariery fizyczne, tj. drzwi, zamki, okna (na parterze zabezpieczone) i ściany. 3. Inne środki bezpieczeństwa fizycznego wynikające z określonego poziomu zagrożeń.
	POZIOM ŚREDNI	1. System kontroli dostępu. 2. Bariery fizyczne, tj. drzwi, zamki, okna (na parterze zabezpieczone) i ściany. 3. Szafy i zamki. 4. Inne środki bezpieczeństwa fizycznego wynikające z określonego poziomu zagrożeń.
	POZIOM WYSOKI	1. System kontroli dostępu. 2. Bariery fizyczne, tj. drzwi, zamki, okna (na parterze zabezpieczone) i ściany. 3. Szafy i zamki. 4. System dozoru wizyjnego. 5. Inne środki bezpieczeństwa fizycznego wynikające z określonego poziomu zagrożeń.

Załącznik nr 2

„WZÓR"

Egzemplarz nr …..

Protokół nr …/…

deklasyfikacji/zniszczenia*) IND

W dniu ..... w miejscowości …….. komisja w składzie:

1. ..... /.....

(Imię i nazwisko, / stanowisko, nazwa komórki organizacyjnej)

2. ..... /.....

(Imię i nazwisko, / stanowisko, nazwa komórki organizacyjnej)

3. ..... /.....

(Imię i nazwisko, / stanowisko, nazwa komórki organizacyjnej)

dokona deklasyfikacji / zniszczenia*) nośników IND

.....

(nazwa komórki organizacyjnej i jednostki organizacyjnej, na której stanie był zarejestrowany IND)

Nr RWP/ Liczba dziennika*)	Typ nośnika	Klauzula Tajności	Sposób deklasyfikacji/zniszczenia*)	Zastosowane urządzenie lub oprogramowanie *typ i nr urządzenia lub nazwę użytego oprogramowania i nr wersji*	Nośnik zarejestrowano w wykazie nośników zdeklasyfikowanych pod poz. nr:

Uwagi:

……

……...

Podpisy członków komisji:

1. ..... 2. ..... 3. .....

Zgoda na deklasyfikację/zniszczenie

…… ……..

(podpis kierownika komórki organizacyjnej) (podpis pełnomocnika ochrony)

Komisja w dniu …… dokonała deklasyfikacji / zniszczenia wymienionych nośników IND ww. metodą.

Podpisy członków komisji:

1. ..... 2. ..... 3. .....

IND zdjęto z ewidencji ……..... / .. zarejestrowano w ……..……..……*)

(typ ewidencji) (typ ewidencji i nr pod jakim zarejestrowano)

……

(podpis kierownika KT lub komórki organizacyjnej prowadzącej RWP)

*) Niepotrzebne skreślić.

wykonano w 2 egz.

egz. nr 1 – kancelaria tajna lub inna komórka organizacyjna prowadząca RWP,

egz. nr 2 – komórka organizacyjna / jednostka organizacyjna.