75

ZARZĄDZENIE Nr 22 DYREKTORA GENERALNEGO SŁUŻBY ZAGRANICZNEJ

z dnia 17 października 2011 r.

w sprawie wdrożenia i eksploatacji Systemu Przetwarzania Informacji Niejawnych — Poufnych w Ministerstwie Spraw Zagranicznych i w placówkach zagranicznych

Na podstawie art. 25 ust. 4 pkt 1 w związku z ust. 10 ustawy z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. U. Nr 227, poz. 1505 oraz z 2009 r. Nr 157, poz. 1241, Nr 219, poz. 1706 i Nr 157, poz. 1241) zarządza się, co następuje:

Rozdział 1

Przepisy ogólne

§ 1

Zarządzenie określa:

1) zasady wdrożenia, eksploatacji oraz administrowania systemem przetwarzania informacji niejawnych o klauzuli „Poufne", „Confidentiel UE/EU Confidential" i „NATO Confidential" włącznie, zwanym dalej „systemem SPIN-P" w Ministerstwie Spraw Zagranicznych oraz w placówkach zagranicznych;
2) zadania komórek organizacyjnych Ministerstwa Spraw Zagranicznych, zwanych dalej „komórkami organizacyjnymi" i placówek zagranicznych oraz obowiązki zatrudnionych w nich pracowników związane z wdrożeniem, utrzymaniem, użytkowaniem i zarządzaniem systemem SPIN-P.

§ 2

Pojęcia używane w zarządzeniu są zgodne z definicjami zawartymi w słowniku obowiązujących pojęć dla potrzeb Księgi Norm Teleinformatycznych i Teletechnicznych, ustalonym w odrębnym trybie.

§ 3

1. Wprowadza się do eksploatacji system SPIN-P w Ministerstwie Spraw Zagranicznych i w placówkach zagranicznych.
2. Dyrektor komórki organizacyjnej właściwej w sprawach teleinformatyki, w porozumieniu z dyrektorem komórki organizacyjnej właściwej w sprawach ochrony informacji niejawnych, jest upoważniony do wydania i aktualizowania instrukcji, wytycznych i poleceń określających szczegółowe zasady wdrażania systemu SPIN-P oraz jego wykorzystania do realizacji zadań służbowych.
3. Użytkownicy i administratorzy ponoszą odpowiedzialność służbową za nieprzestrzeganie zasad użytkowania systemu SPIN-P, określonych w „Procedurach Bezpiecznej Eksploatacji systemu SPIN-P", instrukcjach, wytycznych i poleceniach, o których mowa w ust. 2.
4. Inspektor Bezpieczeństwa Teleinformatycznego ponosi odpowiedzialność służbową za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu SPIN-P ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji, instrukcji, wytycznych i poleceń, o których mowa w ust. 2 a także za realizację zadań określonych w § 14 rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 159, poz. 948).
5. Dyrektor komórki organizacyjnej właściwej w sprawach teleinformatyki jest upoważniony do przekazywania do urzędów polskiej administracji publicznej urządzeń szyfrujących zakupionych przez Ministerstwo Spraw Zagranicznych, w celu ich dalszego wykorzystania na stanowisku roboczym systemu SPIN-P w danym urzędzie.

Rozdział 2

System SPIN-P

§ 4

1. System SPIN-P składa się z infrastruktury serwerowej zainstalowanej w Centrali Ministerstwa Spraw Zagranicznych, brzegowych urządzeń dostępowych oraz stacji roboczych.
2. Infrastruktura serwerowa obejmuje serwery: aplikacyjne, poczty elektronicznej, plików i urządzeń szyfrujących.

§ 5

1. System SPIN-P umożliwia przetwarzanie i przesyłanie informacji niejawnych do klauzuli „Poufne", „Confidentiel UE/EU Confidential" i „NATO Confidential" włącznie.
2. System SPIN-P jest eksploatowany w Ministerstwie Spraw Zagranicznych, w placówkach zagranicznych, a także w wybranych urzędach polskiej administracji publicznej.
3. System SPIN-P posiada następujące środowiska:
   1) produkcyjne;
   2) szkoleniowe;
   3) testowe;
   4) rozwojowe.
4. Zasady obiegu informacji niejawnych w systemie SPIN-P określają odrębne przepisy.

Rozdział 3

Zadania komórek organizacyjnych

§ 6

1. Dyrektor komórki organizacyjnej właściwej w sprawach teleinformatyki, pełniący funkcję Gestora systemu SPIN-P:
   1) wnioskuje do kierownika jednostki organizacyjnej, w rozumieniu przepisów o ochronie informacji niejawnych, o wyznaczenie administratorów systemu sprawujących nadzór nad realizacją zadań związanych z jego funkcjonowaniem;

2) wyznacza administratora materiałów kryptograficznych, sprawującego nadzór nad warstwą kryptograficzną systemu;
3) sprawuje nadzór nad wykonywaniem obowiązków przez administratorów systemu oraz przez administratora materiałów kryptograficznych;
4) odpowiada za planowanie środków finansowych na funkcjonowanie i rozwój systemu, w szczególności za środki przeznaczone na zakup sprzętu, akcesoriów i licencji oprogramowania;
5) współpracuje z dyrektorem komórki właściwej w sprawach finansowych w celu wykonania zadań określonych w zarządzeniu;
6) odpowiada za prowadzenie ewidencji sprzętu, akcesoriów i licencji oprogramowania niezbędnych do funkcjonowania systemu;
7) odpowiada za prowadzenie spraw formalno-prawnych związanych z wykorzystywaniem urządzeń wchodzących w skład systemu.

2. Pełnomocnik do spraw Ochrony Informacji Niejawnych Ministerstwa Spraw Zagranicznych:
1) wnioskuje do kierownika jednostki organizacyjnej, w rozumieniu przepisów o ochronie informacji niejawnych, o wyznaczenie Inspektora Bezpieczeństwa Teleinformatycznego;
2) sprawuje nadzór nad wykonywaniem obowiązków przez Inspektora Bezpieczeństwa Teleinformatycznego;
3) sprawuje nadzór nad obiegiem informacji w systemie SPIN-P.

3. Dyrektor komórki organizacyjnej właściwej w sprawach zarządzania informacją określa wymagania funkcjonalne związane z mechanizmami udostępniania, gromadzenia, wykorzystania oraz przekazywania informacji w systemie SPIN-P.

Rozdział 4

Obowiązki Administratora Głównego systemu SPIN-P

§ 7

Administrator Główny systemu SPIN-P wykonuje obowiązki określone w dokumencie „Procedury Bezpiecznej Eksploatacji systemu SPIN-P", w tym w szczególności:
1) nadzoruje prawidłowe funkcjonowanie wszystkich komponentów systemu, a w przypadku wykrycia nieprawidłowości niezwłocznie przystępuje do działań mających na celu przywrócenie jego poprawnej pracy;
2) zapewnia ciągłość działania systemu;
3) ściśle współpracuje z administratorami pomocniczymi systemu;
4) administruje kontami użytkowników i ich uprawnieniami;
5) odtwarza system i dane przetwarzane w systemie z kopii bezpieczeństwa;
6) opracowuje i aktualizuje dokumentację bezpieczeństwa, techniczną systemu oraz przedkłada ją do zatwierdzenia dyrektorowi komórki organizacyjnej właściwej w sprawach teleinformatyki;
7) powiadamia Inspektora Bezpieczeństwa Teleinformatycznego o incydentach oraz ryzykach naruszenia zasad ochrony informacji przetwarzanych w systemie;
8) wykonuje inne czynności wskazane w dokumentacji bezpieczeństwa systemu.

Rozdział 5

Obowiązki administratora materiałów kryptograficznych

§ 8

Administrator materiałów kryptograficznych realizuje zadania określone w dokumencie „Procedury Bezpiecznej Eksploatacji systemu SPIN-P", w tym w szczególności:
1) prowadzi ewidencję i nadzoruje dystrybucję materiałów kryptograficznych przeznaczonych dla stacji roboczych systemu;
2) wskazuje Inspektorowi Bezpieczeństwa Teleinformatycznego ewentualne nieprawidłowości w procesie posługiwania się materiałami kryptograficznymi przez użytkowników systemu;
3) wytwarza materiały kryptograficzne na stacji generacji kluczy SPIN-P, służące identyfikacji użytkownika w systemie.

Rozdział 6

Obowiązki Administratorów systemów wspierających

§ 9

1. Administratorzy systemów i usług wspierających są zobowiązani:
1) ściśle współpracować z Administratorem Głównym systemu SPIN-P;
2) powiadamiać Administratora Głównego systemu SPIN-P o wystąpieniu zdarzeń zagrażających utracie ciągłości działania lub bezpieczeństwu systemu SPIN-P;
3) we współpracy z Administratorem Głównym systemu SPIN-P podejmować czynności w celu usunięcia awarii.

2. Administratorzy systemów wspierających są zobowiązani do przestrzegania zasad użytkowania systemu określonych w dokumentacji bezpieczeństwa systemu SPIN-P.

Rozdział 7

Obowiązki użytkownika systemu SPIN-P

§ 10

1. Użytkownik systemu SPIN-P jest zobowiązany:
1) przestrzegać zasad użytkowania, określonych w instrukcji, o której mowa w § 3 ust. 2, dokumentacji bezpieczeństwa oraz stosować wytyczne i polecenia wydane w tym zakresie przez dyrektora komórki organizacyjnej właściwej w sprawach teleinformatyki oraz działającego z jego upoważnienia Administratora Głównego systemu SPIN-P;

2) zapoznać się z dokumentem „Procedury Bezpiecznej Eksploatacji Systemu SPIN-P", a w szczególności z częścią odpowiadającą zakresowi obowiązków;

3) uczestniczyć w szkoleniach dotyczących zasad działania systemu SPIN-P;

4) korzystać z systemu SPIN-P wyłącznie w celu realizacji zadań służbowych;

5) korzystać z systemu SPIN-P w taki sposób, aby ograniczyć ryzyko nieuprawnionego zapoznania się osób postronnych z informacjami przetwarzanymi za pomocą systemu SPIN-P;

6) chronić dane pozwalające na uwierzytelnienie się pozwalające na dostęp do systemu SPIN-P;

7) nie udostępniać indywidualnego konta użytkownika żadnej innej osobie;

8) wylogować się z systemu SPIN-P za każdym razem, gdy opuszcza stanowisko pracy;

9) nie pozostawiać bez nadzoru, w tym zabezpieczenia technicznego pomieszczenia, w którym zainstalowane jest stanowisko systemu SPIN-P;

10) każdorazowo po zakończeniu pracy na stanowisku sprawdzić stan zabezpieczenia pomieszczenia, w którym zlokalizowane jest stanowisko, w tym w szczególności zamknięcie drzwi i włączenie systemów zabezpieczenia technicznego pomieszczenia;

11) bezzwłocznie powiadomić Administratora Głównego systemu SPIN-P oraz Inspektora Bezpieczeństwa Teleinformatycznego o incydentach oraz przypadkach wystąpienia ryzyka naruszenia zasad ochrony informacji niejawnych przetwarzanych w systemie.

2. Użytkownik powinien przestrzegać następujących ograniczeń:

1) zabronione jest samowolne instalowanie lub usuwanie oprogramowania komputerowego;

2) zabroniona jest samowolna zmiana ustawień i modyfikacji systemu operacyjnego komputera lub parametrów systemu SPIN-P;

3) zabronione jest samowolne przełączanie kabli sieciowych oraz dokonywanie innych modyfikacji konfiguracji sprzętowej stanowiska SPIN-P;

4) zabronione jest dokonywanie prób uzyskania nielegalnego dostępu do plików lub danych uwierzytelniających innych użytkowników.

Rozdział 8

Bezpieczeństwo systemu SPIN-P

§ 11

1. Administratorzy systemu odpowiadają za bezpieczeństwo systemu SPIN-P, w tym proponują reguły bezpieczeństwa i po ich zatwierdzeniu przez Departament Bezpieczeństwa Teleinformatycznego ABW wdrażają je w systemie SPIN-P.

2. Administratorzy systemu uzgadniają reguły, o których mowa w ust. 1, z Inspektorem Bezpieczeństwa Teleinformatycznego.

Rozdział 9

Zasady przyłączenia stanowisk do systemu SPIN-P

§ 12

1. Stanowisko systemu SPIN-P może być zainstalowane w Ministerstwie Spraw Zagranicznych oraz w jednostkach organizacyjnych podległych Ministrowi Spraw Zagranicznych na wniosek skierowany do dyrektora komórki organizacyjnej właściwej w sprawach teleinformatyki. Z wnioskiem takim wystąpić może:

1) kierownik placówki zagranicznej;

2) dyrektor komórki organizacyjnej w Ministerstwie Spraw Zagranicznych;

3) członek Kierownictwa Ministerstwa Spraw Zagranicznych.

2. Dyrektor komórki organizacyjnej właściwej w sprawach teleinformatyki podejmuje decyzję o zainstalowaniu stanowiska systemu SPIN-P po otrzymaniu od wnioskodawcy następujących dokumentów:

1) wypełnionej ankiety bezpieczeństwa teleinformatycznego stanowiska węzła systemu SPIN-P, której wzór został określony w załączniku do zarządzenia;

2) wniosku o określenie sprzętowej strefy ochrony elektromagnetycznej — WS-01, którego wzór określa Agencja Bezpieczeństwa Wewnętrznego;

oraz zatwierdzeniu powyższych dokumentów przez Departament Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego.

Rozdział 10

Przepisy końcowe

§ 13

1. Dyrektor komórki organizacyjnej właściwej w sprawach teleinformatyki jest zobowiązany do opracowania i wdrożenia w terminie 30 dni od dnia wejścia w życie zarządzenia instrukcji, o której mowa w § 3 ust. 2.

2. Z dniem wejścia zarządzenia w życie wycofuje się z eksploatacji zainstalowany w Ministerstwie Spraw Zagranicznych i placówkach zagranicznych system „SPIN-Z".

3. Od dnia wejścia zarządzenia w życie w placówkach zagranicznych przyłączonych do systemu SPIN-P informacje oznaczone klauzulą poufne należy przesyłać wyłącznie za pośrednictwem tego systemu.

4. Termin wdrożenia i rozpoczęcia użytkowania systemu SPIN-P wyznacza się na 17 października 2011, przy czym placówki zagraniczne, które nie są przyłączone do systemu SPIN-P w dniu wejścia zarządzenia w życie będą przyłączane do tego systemu niezwłocznie po uzyskaniu świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego.

§ 14

Zarządzenie wchodzi w życie z dniem podpisania.

Dyrektor Generalny Służby Zagranicznej

Jarosław Czubiński

Załącznik do zarządzenia Nr 22 Dyrektora Generalnego
Służby Zagranicznej z dnia 17 października 2011 r. (poz. 75)

BIURO INFORMATYKI I TELEKOMUNIKACJI
MINISTERSTWO SPRAW ZAGRANICZNYCH

Zastrzeżone – po wypełnieniu
Egz. pojedynczy

ANKIETA BEZPIECZEŃSTWA TELEINFORMATYCZNEGO WĘZŁA SYSTEMU SPIN-P

NUMER*/	
MIEJSCOWOŚĆ*/	
DATA*/	

*/ - wypełnia BIT MSZ

INFORMACJE OGÓLNE

Nazwa jednostki organizacyjnej, w której ma być zainstalowany węzeł systemu SPIN-P
Ministerstwo Spraw Zagranicznych / Ambasada RP w …….

Adres jednostki organizacyjnej

Nazwisko osoby upoważnionej do kontaktów ws. instalacji		Nr tel.	
adres e-mail osoby upoważnionej		Nr fax.	

Zastrzeżone
……./……

Zastrzeżone
Egz. pojedynczy

Rodzaj informacji niejawnych, które będą przetwarzane w węźle systemu SPIN-P**/

ZASTRZEŻONE	
POUFNE	
UE RESTRICTED	
CONFIDENTIEL UE/UE CONFIDENTIAL	
NATO RESTRICTED	
NATO CONFIDENTIAL	

**/ - zaznaczyć X we właściwym miejscu

DANE PRACOWNIKÓW ODPOWIEDZIALNYCH ZA WYKORZYSTANIE, UTRZYMANIE I OCHRONĘ SYSTEMU SPIN-P

Pełnomocnik ochrony informacji niejawnych w jednostce organizacyjnej		Inspektor BTI w jednostce organizacyjnej	
nazwisko		nazwisko	
imię		imię	
nr poświadczenia bezpieczeństwa i najwyższy poziom dostępu do i.n.		nr poświadczenia bezpieczeństwa i najwyższy poziom dostępu do i.n.	
e-mail		e-mail	
nr tel.		nr tel.	

Zastrzeżone
……/……

Zastrzeżone
Egz. pojedynczy

Administrator stanowiska SPIN-P w jednostce organizacyjnej		Administrator bramy VPN w jednostce organizacyjnej	
nazwisko		nazwisko	
imię		imię	
nr poświadczenia		nr poświadczenia	
bezpieczeństwa i najwyższy poziom dostępu do i.n.		bezpieczeństwa i najwyższy poziom dostępu do i.n.	
e-mail		e-mail	
nr tel.		nr tel.	

ARKUSZ INFORMACJI SZCZEGÓŁOWYCH DOTYCZĄCYCH INSTALACJI I OCHRONY WĘZŁA SYSTEMU SPIN-P

1. BEZPIECZEŃSTWO FIZYCZNE WĘZŁA SYSTEMU SPIN-P:

1.1. Lokalizacja stacji roboczej oraz urządzeń teleinformatycznych węzła systemu SPIN-P w strefie ochronnej

Adres budynku:	
Kondygnacja:	
Nr pomieszczenia(ń):	

Czy węzeł systemu SPIN-P, w tym stacja(e) robocza(e), będą zainstalowane w strefie ochronnej (art. 46 uoin) , tj. w wydzielonej części budynku, w której: *- wprowadzono system kontroli wejść i wyjść,* *- określono uprawnienia do przebywania w strefach.* *Czy jeśli upoważniony personel nie przebywa w strefie 24 godziny na dobę, to z chwilą zakończenia normalnych godzin pracy, pomieszczenie(a) systemu SPIN-P są obejmowane zabezpieczeniem (np. alarm, kontrola dostępu, CCTV) po wyjściu ostatniego pracownika ?* *Jeśli zaznaczono odpowiedź „Tak" proszę opisać jakimi.* *Opis (zrzut z Google Maps, ręcznie zaznaczyć teren przedstawicielstwa, strefę/y ochronne, zaznaczyć miejsca przejść między strefami, usytuowanie pomieszczenia systemu SPIN-P, załączyć opisaną dokumentację fotograficzną zabezpieczeń):*	

Zastrzeżone
……./……

Zastrzeżone
Egz. pojedynczy

1.2. Kancelaria tajna danej jednostki organizacyjnej lub inna komórka organizacyjna odpowiedzialna za przetwarzanie materiałów niejawnych (art. 44 ust. 1 uoin)	
Wpisać najwyższe dopuszczalne klauzule tajności możliwe do przechowania w kancelarii tajnej jednostki organizacyjnej:	
informacje niejawne krajowe	
informacje niejawne UE	
informacje niejawne NATO	

1.3. Zabezpieczenie budynku (lub jego części zajmowanej przez jednostkę organizacyjną) i jego otoczenia:
1.3.1. Czy wokół budynku (lub jego części zajmowanej przez jednostkę organizacyjną – dalej całość nazywana jest „budynkiem) wyznaczona jest strefa ochronna? Czy strefa ta jest kontrolowana za pomocą CCTV? Czy jest wystarczająco oświetlona, np. dla potrzeb CCTV? Czy w otoczeniu budynku jest stosowany system wykrywania intruza PID[1]? Krótki opis środków ochrony (ogrodzenie, brama, szlabany, ochrona osobowa, telewizja dozorowa, itp.)? Opis:
1.3.2.[2] Czy w budynku jest garaż podziemny? Czy przy wjeździe do garażu jest stały posterunek ochrony osobowej (zaznaczyć czy jest to ochrona miejscowa czy kierowana z kraju)? Czy brama jest otwierana przy pomocy karty dostępu? Czy przez wejścia z garażu przyjeżdżające osoby mogą dostać się do wnętrza budynku, za linię ochrony zewnętrznej (posterunki ochrony, „kołowroty" systemu przejść, itp.)? Jak zabezpieczone są wejścia z garażu do budynku ? Załączyć dokumentację fotograficzną wraz z opisem wejść do obiektu (bramy, furtki, zastosowane środki kontroli dostępu) Opis:

[1] ang. Perimeter Intrusion Detection System
[2] Punkt wypełniają jednostki, które są właścicielem/najemcą całego budynku

Zastrzeżone
……/……

Zastrzeżone
Egz. pojedynczy

1.3.3. Jaka jest konstrukcja budynku (cegła, beton, konstrukcja typu „Lipsk", itp.)? Czy zewnętrzne drzwi i okna wykonane są w standardzie takim jak budynek, pod względem jego odporności na siłowe wtargnięcie (okna mogą mieć niższą odporność, jeżeli znajdują się przynajmniej 5 m powyżej poziomu podłoża lub 3 m od poziomu dachu i nie można do nich dotrzeć z dachu lub przy wykorzystaniu elementów konstrukcyjnych budynku)? Jeśli odpowiedź na poprzednie pytanie jest „NIE" to proszę opisać najsłabszy element umożliwiający wejście na teren jednostki organizacyjnej. Opis:
1.3.4. Czy pracownicy wchodzący do budynku są identyfikowani, a ich wejście i wyjście jest rejestrowane (system przepustek, system kontroli dostępu z kartami, „kołowroty", inne)? Opis:
1.3.5. Czy interesanci wchodzący do budynku są rejestrowani, a ich pobyt jest nadzorowany przez upoważnionych pracowników? Czy przy wejściu do budynku stosuje się kontrolę bagażu przez jego prześwietlenie? Czy goście, którym zezwolono na wejście do obiektu lub jego części bez eskorty mają obowiązek nosić przepustkę lub kartę, która identyfikuje ich jak gości? Czy wszyscy pracownicy zobowiązani są nosić karty (identyfikatory) w widocznym miejscu? Opis:
1.3.6. Czy budynek objęty jest stałą całodobową ochroną osobową? Jaka formacja chroni (własna np. portier, delegowani eksperci BOR, agencja ochrony, inne)? Czy pracownicy ochrony posiadają poświadczenia bezpieczeństwa? Ilość osób wykonujących patrole w trakcie i po zakończeniu godzin pracy? Jakie części budynku są patrolowane (strefa administracyjna, strefa bezpieczeństwa)? Opis:
1.3.7. Czy w budynku prowadzona jest kontrola ruchu materiałowego (przepustki materiałowe, wyrywkowe kontrole bagażu, itp.)? Opis:
1.3.8. Czy pomieszczenia w budynku, a zwłaszcza drzwi dostępne z obszarów publicznych zabezpieczone są obiektowym system sygnalizacji napadu i włamania (uzbrajane po wyjściu wszystkich pracowników z budynku lub danej strefy)? Załączyć dokumentację fotograficzną wraz z opisem przejść między strefami (zastosowane środki kontroli dostępu, SSWiN). Opis:

Zastrzeżone
……./……

Zastrzeżone
Egz. pojedynczy

1.4. Zabezpieczenie pomieszczenia systemu SPIN-P
1.4.1. Czy zastosowane środki bezpieczeństwa fizycznego są adekwatne do poziom zagrożeń związanych z utratą poufności, integralności lub dostępności informacji niejawnych? *W szczególności należy opisać budowę ścian i stropów (np. zbrojony beton o grubości 150 mm, cegła o grubości 25 cm, albo inny materiał o podobnej odporności na włamanie, itp.), budowę, odporność na włamanie okien, drzwi itp. Należy opisać system alarmowy, który obejmuje pomieszczenie systemu SPIN-P Załączyć dokumentację fotograficzną wraz z opisem (drzwi, systemu alarmowego)* Opis:
1.4.2. Czy zamki w drzwiach do pomieszczenia systemu SPIN-P posiadają krajowy lub zagraniczny certyfikat bezpieczeństwa uprawnionej jednostki certyfikującej (podać klasę odporności wynikającą z certyfikatu lub świadectwa kwalifikacyjnego)? Czy jest zastosowany system kontroli dostępu do pomieszczenia (elektroniczny, dziennik wejść/wyjść, depozytor)? Opis:
1.4.3. Czy do przechowywania dokumentów niejawnych (wydruki, nośniki) są stosowane szafy (lub inne pojemniki), które spełniają wymagania rozporządzenia? Czy posiadają krajowy lub zagraniczny certyfikat bezpieczeństwa uprawnionej jednostki certyfikującej (podać klasę odporności wynikającą z certyfikatu lub świadectwa kwalifikacyjnego)? Opis:

2. OCHRONA PRZED EMISJĄ ELEKTROMAGNETYCZNĄ
2.1 Czy pomieszczenia strefy ochronnej, o której mowa w pkt. 1.1 posiadają certyfikat „Sprzętowej Strefy Ochrony Elektromagnetycznej" (SSOE) lub „Poziomu Zabezpieczenia Miejsca" (PZM) wydany przez ABW lub SKW (w przypadku odpowiedzi pozytywnej podać numer certyfikatu i wymagania co do konieczności stosowania odpowiedniej kategorii sprzętu TEMPEST? Opis:
2.2 W przypadku braku certyfikatu, o którym mowa w pkt. 2.1 proszę podać, dystans

Zastrzeżone
……./……

Zastrzeżone
Egz. pojedynczy

w metrach między granicą strefy ochronnej (pomieszczenia systemu SPIN-P) i miejscem, w którym mogłaby w sposób niezauważony znaleźć się i przebywać osoba niezaufana (publiczny parking, mieszkanie prywatne, inna jednostka organizacyjna, itp.).

Opis: Otoczenie pomieszczenia systemu SPIN-P:

3. MATRYCA ZAGROŻEŃ ORAZ OCENA RYZYKA

	Opis zagrożenia	Wpływ na bezpieczeństwo				Ocena ryzyka
		min.	mały	średni	krytycz.	
1.	Klęski żywiołowe: pożar, powódź, uderzenie pioruna, trzęsienie ziemi				**M**	akceptowalne
2	Katastrofa budowlana, awarie centralnego ogrzewania, wodno-kanalizacyjne			**M**		akceptowalne
3.	Ekstremalne temperatury, wilgotność			**Ś**		akceptowalne
4.	Awarie sprzętu teleinformatycznego			**M**		akceptowalne
5.	Awarie i zakłócenia zasilania energetycznego			**Ś**		akceptowalne
6.	Zakłócenia elektromagnetyczne, radiotechniczne	**Ś**				akceptowalne
7.	Nieuprawniony podgląd informacji z monitora			**BM**		akceptowalne
8.	Wykorzystanie emisji ujawniającej			**Ś**		akceptowalne
9.	Włamanie do systemu				**BM**	akceptowalne
10.	Kradzież informacji – wydruków, nośników, kopii, haseł dostępu			**BM**		akceptowalne

Zastrzeżone
...../.....

Zastrzeżone
Egz. pojedynczy

11	Wyłudzenie informacji przetwarzanych w systemie, szantaż użytkownika, wykorzystanie technik inżynierii społecznej, współpraca użytkownika ze zorganizowaną przestępczością			BM		akceptowalne
12.	Eksplozja ładunku wybuchowego, inne akty terroryzmu				M	akceptowalne
13	Wandalizm - uszkodzenie, zniszczenie sprzętu, nośnika			BM		akceptowalne
14	Zniszczenie sprzętu wraz ze zbiorami i programami uderzeniem zewnętrznym impulsem elektromagnetycznym	BM				akceptowalne
15	Utrata administratorów odpowiedzialnych za działanie systemu, ich niedobór lub dobór z niskimi kwalifikacjami			Ś		akceptowalne
16	Defekty oprogramowania			BM		akceptowalne
17	Błędy, pomyłki, zaniedbania administratorów		M			akceptowalne
18	Zagubienie nośnika, wydruku		BM			akceptowalne
19	Użycie złośliwego oprogramowania		BM			akceptowalne
20	Nieuprawnione działania użytkownika – korzystanie z nieuprawnionych nośników, użycie oprogramowania w nieuprawniony sposób			BM		akceptowalne
21	Nieobecność administratorów (użytkowników), brak odpowiedniego nadzoru			BM		akceptowalne
22	Niewłaściwe serwisowanie sprzętu i oprogramowania				BM	akceptowalne

Zastrzeżone
...../.....

Zastrzeżone
Egz. pojedynczy

Matryca ryzyk

Wpływ / P-stwo	min.	mały	średni	krytycz.
BM				
M				
Ś				
D				

Opis:

Prawdopodobieństwo wystąpienia zagrożenia / podatności:

Bardzo Małe – **BM** Małe – **M** Średnie – **Ś** Duże – **D**

Ryzyko dla bezpieczeństwa węzła sieci SPIN-P:

Szczątkowe – Niskie – Średnie – Wysokie –

4. DANE PRACOWNIKA ODPOWIEDZIALNEGO ZA PRZYGOTOWANIE ANKIETY	
Dane pracownika	Akceptacja zapisów zawartych w ankiecie
nr poświadczenia bezpieczeństwa i najwyższy poziom dostępu do in e-mail nr tel.	
podpis	podpis

Wyk. w egz. pojedynczym – BIT MSZ
Opracował:
Sporządził:

Zastrzeżone
...../.....