WYTYCZNE NR 4 /2013

Dyrektora Generalnego Służby Więziennej

z dnia 10 czerwca 2013 r.

w sprawie określenia standardów systemów zabezpieczeń elektronicznych w jednostkach organizacyjnych Służby Więziennej

Na podstawie art. 11 ust. 1 pkt 3 ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej (Dz. U. Nr 79, poz. 523 z późn. zm.[1)]), ustala się co następuje:

Rozdział 1

Przepisy ogólne

§ 1.

1. Wytyczne określają standardy projektowania i instalacji systemów zabezpieczeń elektronicznych eksploatowanych w jednostkach organizacyjnych Służby Więziennej, zwanych dalej „jednostkami", obejmujące:

   1) analizę zagrożeń jednostek;

   2) podział jednostek na strefy ochrony za pomocą zabezpieczeń elektronicznych;

   3) minimalne wymagania dotyczące stosowania systemów zabezpieczeń elektronicznych w ramach utworzonych stref;

   4) minimalne parametry techniczne poszczególnych elementów systemów zabezpieczeń elektronicznych jednostek;

[1)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2010 r. Nr 182, poz. 1228 i Nr 238, poz. 1578, z 2011 r. Nr 112, poz. 654 i Nr 291, poz. 1707 oraz z 2012 r. poz. 664 i poz. 951.

5) zasady projektowania, instalacji, odbioru, eksploatacji, napraw i konserwacji systemów zabezpieczeń elektronicznych jednostek;

6) wymaganą dokumentację.

2. Wytyczne nie obejmują zasad:

1) projektowania i instalacji systemów sygnalizacji pożarowej;

2) planowania i realizacji inwestycji.

3. Wytyczne należy stosować przy modernizacji istniejących oraz budowie nowych systemów zabezpieczeń elektronicznych jednostek.

4. Wszelkie odstępstwa od niniejszych wytycznych, wynikające z uwarunkowań architektonicznych jednostki, wymagają pisemnej zgody Dyrektora Generalnego Służby Więziennej.

§ 2.

Ilekroć w dalszej części wytycznych mowa o:

1) **alarmie,** rozumie się przez to ostrzeżenie o istnieniu zagrożenia dla zdrowia lub życia, mienia lub środowiska;

2) **analizie zagrożeń,** rozumie się przez to identyfikowanie zagrożeń powodujących zainicjowanie alarmu oraz oszacowanie prawdopodobieństwa ich wystąpienia;

3) **dokumentacji powykonawczej**, rozumie się przez to dokument, w którym są zapisane szczegóły zainstalowanego systemu;

4) **instalatorze,** rozumie się przez to osobę odpowiedzialną za instalację systemu;

5) **konserwacji systemu,** rozumie się przez to utrzymanie systemu w dobrym stanie, na które składają się przeglądy, naprawy, kontrola działania;

6) **monitorowaniu,** rozumie się przez to proces sprawdzania poprawnego działania połączeń wewnętrznych i urządzeń;

7) **przeglądzie systemu,** rozumie się przez to sprawdzenie stanu technicznego z reguły w określonych odstępach czasu;

8) **sabotażu,** rozumie się przez to umyślne zakłócenie działania systemu zabezpieczenia elektronicznego lub jego części;

9) **strefie,** rozumie się przez to wyznaczony lub wydzielony obszar, w którym mogą być wykryte nienormalne warunki (np. ruch intruza);

10) **zagrożeniu,** rozumie się przez to źródło potencjalnej szkody lub okoliczności potencjalnie szkodliwe;

11) **zasadzie wiedzy koniecznej,** rozumie się przez to zobowiązanie każdego funkcjonariusza i pracownika do posiadania wiedzy o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.

§ 3.

1. W jednostkach stosuje się następujące systemy zabezpieczeń elektronicznych:
   1) systemy sygnalizacji włamania i napadu;
   2) systemy kontroli dostępu;
   3) systemy telewizji dozorowej.
2. Systemy, o których mowa w ust. 1 pkt 1 i 2, mają charakter podstawowy, system określony w ust. 1 pkt 3 jest systemem uzupełniającym.
3. Systemy należy projektować, instalować i użytkować zgodnie z polskimi normami wskazanymi w załączniku nr 1.
4. System sygnalizacji włamania i napadu powinien spełniać wymogi zabezpieczenia w stopniu minimum 3 wg normy PN-EN 50131-1.
5. W celu podniesienia bezpieczeństwa i niezawodności całości systemu stosuje się integrację systemów wymienionych w ust. 1

§ 4.

1. Analizę zagrożeń przeprowadza się na podstawie protokołu rozpoznania jednostki. Protokół rozpoznania służy także do ustalenia potrzeb w zakresie wyposażenia jednostki organizacyjnej w zabezpieczenia techniczno – ochronne, środki łączności, sygnalizacji i alarmowania oraz ich rozmieszczenia.
2. Ustala się następujący podział na strefy ochrony jednostek za pomocą zabezpieczeń elektronicznych:
   1) strefa A – budynki zakwaterowania osadzonych;
   2) strefa B – budynki bezpośrednio przyległe do budynków zakwaterowania osadzonych oraz wyznaczony obszar zewnętrzny przyległy do budynków zakwaterowania osadzonych i obiektów bezpośrednio do nich przyległych;
   3) strefa C – pas ochronny, bramy wjazdowe i wyjazdowe oraz wejścia i wyjścia do i z terenu jednostki;
   4) strefa D – obszar, który nie został ujęty w strefie A, B, C i E;
   5) strefa E – pomieszczenia i obiekty mające szczególne znaczenie dla bezpieczeństwa jednostki np.: serwerownie, magazyny, place spacerowe, kancelarie tajne, magazyny broni, archiwa itd.

§ 5.

1. Osoba odpowiedzialna za ocenę zagrożeń oraz projektowanie, instalowanie, konserwacje i naprawy systemu powinna posiadać odpowiednie kwalifikacje (np. licencja pracownika zabezpieczenia technicznego).

2. Informacje związane z projektowaniem, instalacją, obsługą i konserwacją systemu przeznaczone są wyłącznie do użytku służbowego. Przy dostępie do powyższych informacji należy kierować się zasadą wiedzy koniecznej.

Rozdział 2

Zasady projektowania systemów zabezpieczeń elektronicznych

§ 6.

Zabezpieczenia stosowane w strefie A powinny spełniać następujące warunki:

1) wejścia i wyjścia do i ze strefy wyposaża się w system śluzowania (blokada wykluczająca);

2) śluzy wyposaża się w system zapewniający obserwację bezpośredniego obszaru przed wejściem/wyjściem, system kontroli dostępu z pełną identyfikacją osób, system zapewniający sygnalizację otwarcia drzwi;

3) wejście lub wyjście do i ze strefy wymaga podwójnej autoryzacji;

4) przejścia w strefie wyposaża się w system kontroli dostępu i telewizji dozorowej. Wymagana jest pełna identyfikacja osób wchodzących i wychodzących;

5) ciągi komunikacyjne, miejsca i pomieszczenia wyznaczone do: pracy, nauki, widzeń, odprawiania nabożeństw, spotkań religijnych oraz zajęć kulturalno-oświatowych, z zakresu kultury fizycznej i sportu wyposaża się w system telewizji dozorowej;

6) dyżurki oddziałowych wyposaża się w urządzenia umożliwiające obserwację nadzorowanych pomieszczeń i oddziałów;

7) wszystkich pracowników i funkcjonariuszy przebywających w strefie A wyposaża się w przyciski napadowe z funkcją lokalizacji pomieszczenia w którym wywołano alarm. Alarm powinien być sygnalizowany na stanowisku dowodzenia oraz w dyżurce właściwego oddziałowego;

8) włazy dachowe i klapy oddymiające wyposaża się w system sygnalizacji otwarcia.

§ 7.

Zabezpieczenia stosowane w strefie B powinny spełniać następujące warunki:

1) wyposażenie w system sygnalizacji włamania i napadu zawierający urządzenia wykrywające obecność osób;

2) weryfikacja alarmów z systemu sygnalizacji włamania i napadu powinna być dokonywana na podstawie system dozoru wizyjnego opartego o kamery. Rozmieszczenie kamer musi zapewnić obserwację całego chronionego obszaru. Dopuszcza się stosowanie kamer obrotowych. Obraz musi zapewniać identyfikację zdarzenia w celu pozyskania informacji o ujawnieniu osoby.

§ 8.

Zabezpieczenia stosowane w strefie C powinny spełniać następujące warunki:

1) na pasie ochronnym stosuje się system sygnalizacji włamania i napadu wyposażony w urządzenia wykrywające obecność osób;

2) do weryfikacji alarmów z systemu sygnalizacji włamania i napadu stosuje się system dozoru wizyjnego oparty o kamery stałopozycyjne. Rozmieszczenie kamer musi zapewnić obserwację całego pasa ochronnego bez martwych stref. Obraz musi zapewniać identyfikację zdarzenia w celu pozyskania informacji o ujawnieniu osoby;

3) wejścia i wyjścia z pasa ochronnego wyposaża się w sygnalizację otwarcia. Dopuszcza się stosowanie systemów kontroli dostępu;

4) bramy wjazdowe i wyjazdowe oraz wejścia i wyjścia piesze z terenu jednostki wyposaża się w system śluzowania (blokada wykluczająca);

5) bramy, wejścia i wyjścia wyposaża się w sygnalizację otwarcia. Dopuszcza się stosowanie kontroli dostępu;

6) w śluzach dla pojazdów stosuje się system telewizji dozorowej zapewniający:

   a) obserwację bezpośredniego, zewnętrznego obszaru przed bramą wjazdową na teren jednostki,

   b) pełną identyfikację pojazdu znajdującego się wewnątrz śluzy,

   c) obserwację podwozia i dachu pojazdu znajdującego się wewnątrz śluzy;

7) w śluzach pieszych stosuje się systemy zapewniające:

   a) obserwację bezpośredniego obszaru przed wejściem i wyjściem na i z terenu jednostki,

   b) kontrolę dostępu z pełną identyfikacją osób;

8) stanowisko pracy bramowego wyposaża się w urządzenia umożliwiające monitorowanie i obserwację nadzorowanych przez niego obszarów.

§ 9.

W strefie D stosuje się system telewizji dozorowej. Obraz musi zapewniać identyfikację zdarzenia w celu pozyskania informacji o ujawnieniu osoby.

§ 10.

Zabezpieczenia stosowane w strefie E powinny spełniać następujące warunki:

1) pomieszczenia serwerowni wyposaża się w:

   a) system kontroli dostępu,

   b) system sygnalizacji włamania i napadu zapewniający detekcję dymu, ruchu, otwarcia drzwi, stłuczenia szyb i zalania wodą,

   c) system monitorujący temperaturę i wilgotność powietrza,

   d) system informujący o zaniku zasilania;

2) pomieszczenia magazynów wyposaża się w system sygnalizacji włamania i napadu zapewniający detekcję dymu, ruchu i otwarcia drzwi;

3) place spacerowe wyposaża się w system telewizji dozorowej. Rozmieszczenie kamer musi zapewnić obserwację całego chronionego obszaru bez martwych stref. Obraz musi zapewniać identyfikację zdarzenia w celu pozyskania informacji o ujawnieniu osoby. Posterunek spacerowego w razie konieczności wyposaża się w urządzenia umożliwiające obserwację nadzorowanych placów spacerowych;

4) sposób ochrony magazynów broni, kancelarii tajnych, archiwów określają odrębne przepisy.

§ 11.

1. Minimalne wymagania techniczne poszczególnych elementów systemów telewizji dozorowej i kontroli dostępu określa załącznik nr 2.

2. Jako układ zbliżeniowy (bezstykowy) dla kart dostępowych w systemach kontroli dostępu wyznacza się standard MIFARE Plus X[2)], który posiada 4KB pamięci EEPROM oraz 7-bajtowy unikalny numer seryjny nadawany przez producenta wg ISO/IEC 14443. Elektroniczny układ bezstykowy musi umożliwiać pracę z zastosowaniem algorytmu AES (Advanced Encryption Standard) z kluczami 128 bitowymi.

[2)] Nazwa Mifare Plus X jest określeniem standardu opracowanego dla kart zbliżeniowych (bezstykowych).

Rozdział 3

Budowa nowych i modernizacja istniejących systemów zabezpieczeń elektronicznych

§ 12.

1. Budowa nowych oraz modernizacja istniejących systemów zabezpieczeń elektronicznych jednostek wymaga opracowania koncepcji i założeń do projektu budowy lub modernizacji systemów zabezpieczeń elektronicznych.
2. Proces opracowywania koncepcji i założeń do projektu budowy lub modernizacji systemów zabezpieczeń elektronicznych jednostek przedstawia załącznik nr 3.

§ 13.

Budowa nowych lub modernizacja systemów zabezpieczeń elektronicznych składa się z następujących etapów:

1) projektowanie systemu;
2) wykonanie systemu;
3) sprawdzenie, uruchomienie i przekazanie systemu do eksploatacji.

§ 14.

1. Projekt systemu powinien zawierać w szczególności:
   1) dane inwestora;
   2) dane obiektu, którego dotyczy projekt (adres, nr działki);
   3) dane projektanta/biura projektowego (uprawnienia);
   4) uzgodnienia ze zleceniodawcą projektu (spisane notatką po wizji lokalnej);
   5) uzgodnienia budowlane;
   6) wykaz norm związanych z projektem;
   7) stopień zabezpieczenia i klasę systemu alarmowego;
   8) klasy środowiskowe elementów systemu;
   9) opis konfiguracji systemu i lokalizacji urządzeń;

10) dane dotyczące sygnalizacji;

11) sposób reakcji i interwencji na alarmy;

12) plan konserwacji;

13) zestawienie urządzeń;

14) świadectwa i certyfikaty urządzeń i materiałów wykorzystywanych do budowy systemu;

15) schemat blokowy systemu;

16) podkłady budowlane z rozmieszczeniem elementów systemu i tras kablowych.

2. Na podstawie projektu wykonany zostaje kosztorys inwestorski i przedmiar robót.

§ 15.

1. Systemy zabezpieczeń elektronicznych mogą być wykonywane we własnym zakresie lub przez podmiot zewnętrzny.

2. Wykonanie systemu zabezpieczeń elektronicznych realizuje się zgodnie z aktualnie obowiązującymi przepisami o zamówieniach publicznych oraz uregulowaniami obowiązującymi w jednostce.

§ 16.

1. Urządzeń i elementów systemu nie należy instalować w pobliżu źródeł ciepła, np. grzejników, urządzeń klimatyzacyjnych, jeżeli mogłoby to wpłynąć ujemnie na ich działanie.

2. Prace, które będą wykonywane w miejscu zainstalowania urządzeń i elementów systemu powinny obejmować:

   a) wstępne przygotowanie miejsca pracy;

   b) rozprowadzenie kabli i przewodów;

   c) rozmieszczenie urządzeń;

   d) łączenie urządzeń i elementów.

3. Parametry przewodów elektrycznych (przekrój - rezystancja) powinny być takie, aby przy przepływie maksymalnego prądu napięcie między określonymi zaciskami urządzeń lub elementów nie było mniejsze niż jego określona wartość robocza, (np. w przypadku sygnalizatorów, czujek, barier instalowanych w znacznej odległości od centrali). Izolacja przewodów musi być dostosowana do stosowanego napięcia roboczego.

4. Połączenia przewodów elektrycznych powinny mieć odpowiednią wytrzymałość mechaniczną i elektryczną oraz powinny być od siebie odizolowane elektrycznie. Do

połączeń przewodów należy wykorzystywać listwy zaciskowe pokryte materiałem izolacyjnym lub puszki połączeniowe o szczelności obudowy dostosowanej do warunków środowiskowych.

5. Inne elementy łączące (np. wtyczka i gniazdo lub specjalne złącza firmowe) mogą być zastosowane pod warunkiem, jeśli połączenia przewodów z tymi elementami spełniają wymagania określone w ust. 4.

6. Połączenia giętkie powinny być takie, aby przewody i izolacja były odporne na zmęczenie lub naprężenia występujące w konkretnym zastosowaniu.

7. Okablowanie powinno być odpowiednio zamocowane i rozprowadzone albo zabezpieczone w celu uniknięcia uszkodzeń mechanicznych i klimatycznych w środowisku, w którym jest stosowane.

§ 17.

1. Sprawdzenie systemu odbywa się w obecności Administratora systemów zabezpieczeń elektronicznych.

2. Po sprawdzeniu systemu sporządza się protokół odbioru.

3. Instalator przekazuje Administratorowi systemów zabezpieczeń elektronicznych informacje dotyczące odpowiedniego poziomu/poziomów dostępu do systemu.

4. Po zatwierdzeniu protokołu odbioru osobą odpowiedzialną za użytkowanie systemu staje się Administrator systemów zabezpieczeń elektronicznych. Osobie tej należy przyznać uprawnienia do wykonywania prac niezbędnych do utrzymania systemu alarmowego w stanie sprawności, dokonywania odpowiednich zapisów oraz obsługi.

§ 18.

Dokumentacja powykonawcza powinna zawierać:

1) dane firmy instalacyjnej;

2) projekt wykonawczy systemu z naniesionymi ewentualnymi zmianami (w opisie, zestawieniu materiałów jak i rysunkach);

3) instrukcję obsługi systemu, szczegółową na tyle, by zminimalizować możliwość niewłaściwego użytkowania. Instrukcja powinna mieć dwie części: pierwszą - dotyczącą włączania/wyłączania, weryfikacji stanu alarmu, kasowania, blokowania i testowania, drugą - opisującą pozostałe funkcje systemu;

4) instrukcję reagowania na alarmy i postępowania w przypadku awarii systemu;

5) instrukcję konserwacji i napraw z danymi kontaktowymi osoby odpowiedzialnej za konserwację/naprawy;

6) protokół z przeszkolenia obsługi przekazywanego systemu z zapisem miejsca, daty oraz danych osób szkolących i przeszkolonych;

7) protokół odbioru;

8) deklarację zgodności dla urządzeń zastosowanych w systemie, które wymagają klasyfikacji wg norm.

Rozdział 4

Eksploatacja i konserwacja systemów zabezpieczeń elektronicznych

§ 19.

Podczas eksploatacji systemów zabezpieczeń elektronicznych kierownik jednostki jest w szczególności zobowiązany do:

1) zadbania o odpowiedni poziom wyszkolenia użytkowników systemu;

2) ustalenia procedur postępowania z alarmami, ostrzeżeniami o uszkodzeniu, wyłączeniu części lub całego systemu ze stanu działania;

3) takiej organizacji współpracy z osobami odpowiedzialnymi za konserwację budynku, jego remonty itp., aby wykonywane przez te osoby czynności nie spowodowały uszkodzeń lub innych zakłóceń działania systemu.

§ 20.

1. Konserwacja okresowa powinna być przeprowadzana nie rzadziej niż w okresach zgodnych z wymaganiami dotyczącymi danego systemu.
2. Podczas każdej konserwacji okresowej należy wykonać następujące sprawdzenia i wszelkie niezbędne poprawki:

1) sprawdzenie instalacji, właściwego rozmieszczenia i zamocowania wyposażenia i urządzeń na podstawie dokumentacji technicznej;
2) sprawdzenie poprawności działania wszystkich urządzeń, łącznie z urządzeniami uruchamianymi ręcznie;
3) sprawdzenie zgodności z wymaganiami wszystkich połączeń giętkich;
4) sprawdzenie czy zasilacze główne i rezerwowe pracują i są sprawne;
5) sprawdzenie centrali alarmowej i jej obsługi zgodnie z procedurą zakładu instalacji alarmowych;
6) sprawdzenie poprawności działania każdego urządzenia transmisji alarmu przy współpracy z odpowiedzialną władzą albo z odpowiednim alarmowym centrum odbiorczym;
7) sprawdzenie poprawności działania każdego dźwiękowego, świetlnego, dźwiękowo/świetlnego sygnalizatora alarmowego;
8) sprawdzenie czy system jest całkowicie w stanie gotowości.

3. Konserwacja powinna odbywać się zgodnie z przewidzianymi w normach czasookresami. Jeżeli takiego czasookresu nie przewidziano - wówczas nie rzadziej niż co 6 miesięcy.

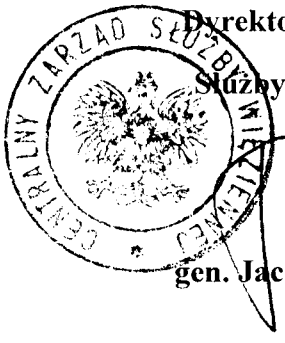
4. Czasookres funkcjonowania systemu dla potrzeb konserwacji rozpoczyna się niezwłocznie po jego zainstalowaniu.

Rozdział 5

Przepisy końcowe

§ 21.

Wytyczne wchodzą w życie z dniem 15 czerwca 2013 r.



Dyrektor Generalny

Służby Więziennej

gen. Jacek Włodarski

UZASADNIENIE

Obecnie brak jednolitych minimalnych wymagań dotyczących zastosowania elektronicznych systemów zabezpieczeń elektronicznych w jednostkach organizacyjnych Służby Więziennej.

W związku z szybkim postępem technologicznym w zakresie dziedziny elektronicznej ochrony obiektów oraz oferowanych na rynku różnorodnych rozwiązaniach w tym zakresie, zaistniała potrzeba opracowania dokumentu zawierającego jednoznaczne wytyczne określające minimalne wymagania dla mających zastosowanie w więziennictwie systemów elektronicznych, jak również minimalne parametry techniczne poszczególnych elementów systemów. Niniejsze wytyczne zawierają również zasady projektowania, instalacji, eksploatacji, konserwacji oraz prowadzenia niezbędnej dokumentacji (w tym jej aktualizacji) elektronicznych systemów zabezpieczeń. Dokument ten wyznacza też minimalne standardy, które powinny być zastosowane podczas określania wymagań funkcjonalnych i technicznych systemów.

Przepisy zawarte w niniejszym dokumencie mają zastosowanie do nowobudowanych jednostek organizacyjnych, części rozbudowy dotychczasowych bądź ich remontów, w których zawarto zadania dotyczące instalacji nowego systemu zabezpieczeń elektronicznych.

Wejście w życie wytycznych nie spowoduje dodatkowych kosztów dla budżetu więziennictwa.

Załącznik nr 1
do wytycznych nr 4../2013
Dyrektora Generalnego Służby Więziennej
z dnia 10 czerwca 2013 r.

Wykaz polskich norm znajdujących zastosowanie podczas projektowania, instalowania i użytkowania systemów zabezpieczeń elektronicznych

PN-EN 50130-5:2012 – *Systemy alarmowe – część 5: Próby środowiskowe;*

PN-EN 50131-1:2009 – *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – część 1: Wymagania systemowe;*

PN-EN 50131-2-2:2009 – *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – część 2-2: Czujki sygnalizacji włamania – Pasywne czujki podczerwieni;*

PN-EN 50131-2-3:2010 – *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – część 2-3: Wymagania dotyczące czujek mikrofalowych;*

PN-EN 50131-2-4:2009 – *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – część 2-4: Wymagania dotyczące dualnych czujek pasywnych podczerwieni i mikrofalowych;*

PN-EN 50131-2-5:2010 – *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – część 2-5: Wymagania dotyczące dualnych czujek pasywnych podczerwieni i ultradźwiękowych;*

PN-EN 50131-2-6:2012 – *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – część 2-6: Czujki otwarcia stykowe(magnetyczne);*

PN-EN 50131-3:2010 – *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – część 3: Urządzenia sterujące i obrazujące;*

PN-EN 50131-6:2009 – *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – część 6:Zasilanie;*

PKN-CLC/TS 50131-7:2011 – *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – część 7: Wytyczne stosowania;*

PN-EN 50132-1:2012 – *Systemy alarmowe – Systemy dozorowe CCTV stosowane w zabezpieczeniach – Część 1: Wymagania systemowe;*

PN-EN 50132-7:2003 – *Systemy alarmowe – Systemy dozorowe CCTV stosowane w zabezpieczeniach – Część 7: Wytyczne stosowania;*

PN-EN 50133-1:2007 – *Systemy alarmowe – Systemy kontroli dostępu w zastosowaniach dotyczących zabezpieczenia – Część 1: Wymagania systemowe;*

PN-EN 50133-7:2002 – *Systemy alarmowe – Systemy kontroli dostępu w zastosowaniach dotyczących zabezpieczenia – Część 7: Zasady stosowania;*

Specyfikacja techniczna POLALARM ST 01/01 – *Systemy alarmowe – Część 1: Systemy sygnalizacji włamania i napadu – Wymagania ogólne i zasady stosowania. Wersja 01.03.2010 r.*

NO-04-A004-1:2010

NO-04-A004-2:2010

NO-04-A004-3:2010

NO-04-A004-4:2010

NO-04-A004-5:2010

NO-04-A004-6:2010

NO-04-A004-7:2010

NO-04-A004-8:2006

Załącznik nr 2
do wytycznych nr 4../2013
Dyrektora Generalnego Służby Więziennej
z dnia 10 czerwca 2013 r.

Minimalne wymagania techniczne urządzeń wchodzących w skład systemu telewizji dozorowej (CCTV).

1. Zasilanie urządzeń wchodzących w skład telewizji dozorowej (CCTV):

1.1. Sposób zasilania wszystkich urządzeń wchodzących w skład telewizji dozorowej musi gwarantować ich nieprzerwaną, ciągłą pracę. W celu zapewnienia takiego funkcjonowania stosuje się zasilacze buforowe z akumulatorami i UPS-y. Obwody elektryczne stanowiące źródło zasilania dla zasilaczy buforowych i UPS-ów muszą być podłączone do agregatów prądotwórczych.

1.2. Zasilacze buforowe z akumulatorami i UPS-y powinny umożliwić pracę podłączonych urządzeń do czasu uruchomienia zasilania z agregatów - nie krócej jednak niż przez 1 godzinę.

2. Dobór standardu CCTV:

2.1. Dopuszcza się budowanie systemów telewizji dozorowej w technologii analogowej lub cyfrowej (IP) z zastrzeżeniem punktów 2.2 i 2.3.

2.2. Nowe zakłady karne i areszty śledcze wyposaża się w system telewizji dozorowej w technologii cyfrowej IP. Do budowy infrastruktury kablowej stosuje się normy dotyczące budowy okablowania strukturalnego.

2.3. W przypadku modernizacji, rozbudowy lub naprawy istniejących systemów CCTV linie sygnałowe toru audio-wideo należy realizować na bazie skrętki komputerowej kategorii minimum 5e lub światłowodu i konwerterów sygnału. Przyjmuje się dla jednego toru audio-wideo jeden przewód skrętkowy. Umożliwi to w przyszłości płynne przejście do standardu CCTV IP.

3. Punkty kamerowe:

3.1. Punkt kamerowy to zestaw zawierający kamerę wraz z obiektywem i niezbędnym wyposażeniem pomocniczym umieszczane w zależności od potrzeb w osłonie zabezpieczającej przed uszkodzeniami mechanicznymi lub środowiskowymi.

3.2. Parametry minimalne określono dla kamer analogowych. W przypadku zastosowania rozwiązań opartych o technologię CCTV IP należy przyjąć minimalną rozdzielczość obrazu kamery na poziomie 800x600 pikseli (px) co odpowiada w przybliżeniu 0,5 Mpx. Pozostałe parametry należy przyjąć tak jak dla kamer analogowych.

3.3. Kamery montowane w celach mieszkalnych, kącikach sanitarnych:

Obudowa kamery	Stopień ochrony przed uderzeniem IK-10 (obudowa wandaloodporna) IK10=wytrzymywana energia upadku na urządzenie ciężaru 5 kg z wysokości 40 cm
Stopień ochrony	IP66
Temperatura pracy / wilgotność	+ 0°C - +40°C / do 70%
System pracy	Kolor z automatycznym przełączeniem na B/W z mechanicznym filtrem podczerwieni
Doświetlanie obserwowanej sceny	Punkt kamerowy powinien zapewnić widoczność obserwowanej sceny w każdych warunkach oświetleniowych w odległości minimum 12 m.

Przetwornik obrazu	Matryca CCD o przekątnej 1/3"
Rozdzielczość pozioma	Tryb kolor: 520 linii, tryb B/W: 560 linii
Czułość na oświetlenie	Tryb kolor: 0,3 Lux, tryb B/W z wł. LED: 0 Lux
Obiektyw	Zmiennoogniskowy z regulacją ręczną Długość ogniskowej 2,8 - 8 mm
Pole widzenia	Poziomo: 90 stopni, pionowo: 60 stopni
Kompensacja tylnego oświetlenia	TAK
Tryb dzień / noc	TAK, automatyczne przełączenie
Filtr szumów	TAK
Maskowanie obszarów prywatności	TAK, 4 strefy
Menu ekranowe OSD	TAK w języku polskim
Zasilanie	12V DC lub 24V AC lub dla kamer IP PoE
Kodeki dla kamer IP	H.264 lub lepszy

3.4. Kamery montowane w łaźniach:

Specyfikacja jak w 3.3 z następującymi zmianami	
Temperatura pracy / wilgotność	+ 0°C - +50°C / 90% odporność na kondensację (kontakt z wodą)

3.5. Kamery montowane w korytarzach, świetlicach, salach widzeń, pokojach przesłuchań, pomieszczeniach pracy, nauki, odprawiania nabożeństw, spotkań religijnych oraz zajęć kulturalno-oświatowych, z zakresu kultury fizycznej i sportu:

Specyfikacja jak w 3.3 z następującymi zmianami	
Maskowanie obszarów prywatności	NIE WYMAGANE

3.6. Kamery montowane wewnątrz budynków w przejściach objętych kontrolą dostępu:

Specyfikacja jak w 3.3 z następującymi zmianami	
Maskowanie obszarów prywatności	NIE WYMAGANE

3.7. Kamery montowane na zewnątrz budynków w przejściach objętych kontrolą dostępu, w śluzach dla ruchu samochodowego i pieszego:

Specyfikacja jak w 3.3 z następującymi zmianami	
Obudowa kamery	Obudowa w wersji zewnętrznej Stopień ochrony przed uderzeniem IK-10 (obudowa wandaloodporna) IK10=wytrzymywana energia upadku na urządzenie ciężaru 5 kg z wysokości 40 cm
Maskowanie obszarów prywatności	NIE WYMAGANE
Temperatura pracy / wilgotność	- 20°C - +50°C / 90% odporność na kondensację (kontakt z wodą)

3.8. Kamery stałopozycyjne zewnętrzne:

Obudowa kamery	Obudowa w wersji zewnętrznej Stopień ochrony przed uderzeniem IK-10 (obudowa wandaloodporna) IK10=wytrzymywana energia upadku na urządzenie ciężaru 5 kg z wysokości 40 cm
Stopień ochrony	IP66
Temperatura pracy / wilgotność	- 20°C - +50°C / 90% odporność na kondensację (kontakt z wodą)
System pracy	Kolor z automatycznym przełączeniem na B/W z mechanicznym filtrem podczerwieni
Doświetlanie obserwowanej sceny	Punkt kamerowy powinien zapewnić widoczność obserwowanej sceny w każdych warunkach oświetleniowych w odległości minimum 20 m.
Przetwornik obrazu	Matryca CCD o przekątnej 1/3"
Rozdzielczość pozioma	Tryb kolor: 520 linii, tryb B/W: 560 linii
Czułość na oświetlenie	Tryb kolor: 0,3 Lux, tryb B/W z wł. LED: 0 Lux
Obiektyw	Zmiennoogniskowy z regulacją ręczną Długość ogniskowej uzależniona od obserwowanej sceny
Detekcja ruchu	TAK
Kompensacja tylnego oświetlenia	TAK
Tryb dzień / noc	TAK, automatyczne przełączenie
Filtr szumów	TAK
Menu ekranowe OSD	TAK w języku polskim
Zasilanie kamery i grzałki	12V DC lub 24V AC lub dla kamer IP PoE
Kodeki dla kamer IP	H.264 lub lepszy

3.9. Kamery obrotowe zewnętrzne:

Specyfikacja jak w 3.8 z następującymi zmianami	
Obiektyw	Zmiennoogniskowy ze zdalną regulacją Długość ogniskowej uzależniona od obserwowanej sceny, 20-krotny zoom optyczny
Prędkość obrotu głowicy	180 st./sek
Pamięć położenia (preset)	16
Protokół sterowania	minimum Pelco D RS 485

4. Urządzenia utrwalające obraz lub dźwięk (rejestratory cyfrowe):

4.1. Parametry minimalne:

Wyświetlanie w czasie rzeczywistym	PAL – D1 720x576 50 kl/sek.

Podział obrazu	do 16
Kompresja	H.264 lub lepszy
Tryb nagrywania	Ręczny, planowany, zdarzenie, awaryjny
Nadpisywanie	Ciągłe, możliwość wyłączenia
Nagrywanie	PAL – D1, minimum 3 klatki/sek dla każdego strumienia audio-wideo
Wyszukiwanie	Czas, zdarzenie, kalendarz
Sieć	TCP/IP
Obsługa protokołów sieciowych	DHCP, DNS, HTTP, NTP
Dostęp zdalny	Minimum 5 jednoczesnych połączeń
Pojemność dysków	Możliwość zamontowania minimum 2 dysków. Przestrzeń dyskowa musi zapewnić przechowywanie zarejestrowanego obrazu lub dźwięku przez okres minimum 7 dni dla każdego strumienia audio-wideo
Znacznik czasu	TAK – data i godzina czasu lokalnego
Archiwizacja nagrań przez USB lub DVD	TAK – możliwość archiwizacji strumienia danych z pojedynczej kamery, kilku wybranych kamer jednocześnie, wszystkich kamer
Zabezpieczenie dostępu	Minimum dwa poziomy dostępu: administrator, użytkownik obserwator. Dostęp ograniczony hasłem.
Wyjścia monitorowe	RGB, BNC
Dźwięk	4 kanały – rejestrowane pasmo 300 Hz – 6000 Hz, przy minimalnej dynamice 50 dB
Komunikacja / Protokoły	Ethernet, sterowanie PTZ, RS232C, RS485 / Pelco D
Sterowanie rejestratorem	Urządzenie musi umożliwiać sterowanie rejestratorem ze stanowiska monitoringu
Język OSD	Polski

Minimalne wymagania techniczne urządzeń wchodzących w skład systemu kontroli dostępu (KD).

1. Należy stosować kontrolery drzwi z niezależnym zasilaniem buforowym, które po utracie komunikacji z jednostką nadrzędną nadal umożliwiają realizację kontroli i sterowania przejściem
2. Należy stosować czytniki kart zbliżeniowych w standardzie Mifare, odczytujące nr zapisany w sektorze pamięci zabezpieczonym hasłem (najpierw weryfikowane jest hasło między czytnikiem a kartą, dopiero po uzyskaniu pozytywnego wyniku następuje odczyt danych.
3. Do komunikacji z czytnikiem dopuszcza się protokoły Wieganda, RS485 i TCP/IP.
4. Okablowanie systemu należy zabezpieczyć przed dostępem i sabotażem.
5. Należy stosować śruby z zabezpieczeniem, tak aby usunięcie czytnika wymagało specjalnego narzędzia.
6. Pojedyncze przejście (drzwi/krata) należy wyposażyć w czytniki kart, kontaktrony oraz zamek elektromechaniczny (oraz system telewizji dozorowej wg parametrów opisanych w wytycznych oraz powyżej).
7. Przejścia należy wyposażać w obustronną pełną identyfikację, wejścia do pomieszczeń (np. serwerownia, magazyn) pełna identyfikacja jednostronna (wewnątrz klamka lub przycisk wyjścia).
8. Przejścia (drzwi/kraty) powinny posiadać możliwość mechanicznego otwarcia kluczem w przypadku awarii systemu kontroli dostępu.
9. System kontroli dostępu powinien dostarczać sygnały z przejść takie jak: otwarte, zamknięte, uszkodzenie/sabotaż, otwarcie nieautoryzowane. Stany te powinny być zapisywane w dzienniku zdarzeń sytemu.

Załącznik nr 3 - Proces opracowywania koncepcji i założeń do projektu budowy lub modernizacji systemów elektronicznego zabezpieczenia jednostek SW – do wytycznych nr 4../2013 Dyrektora Generalnego Służby Więziennej z dnia 10 czerwca 2013 r. w sprawie określenia standardów systemów zabezpieczeń elektronicznych w jednostkach organizacyjnych Służby Więziennej.

Lp.	Etap procesu	Wymogi formalne	Komórka odpowiedzialna za realizację etapu	Uwagi
1	Opracowanie koncepcji i założeń funkcjonalnych	Dokument musi zawierać: 1. zdefiniowanie zagadnienia; 2. ogólną charakterystykę chronionego obiektu; 3. określenie braków w zabezpieczeniu obiektu; 4. analizę zagrożeń i ryzyka (identyfikację zagrożeń zarówno przypadkowych jak i rozmyślnych oraz określenie prawdopodobieństwa ich wystąpienia); 5. określenie funkcjonalności systemu (czego oczekuje się od systemu, np.: zdefiniowanie miejsc i sposobu sygnalizacji stanów systemu); 6. uzasadnienie proponowanych rozwiązań.	Dział Ochrony	Opracowany dokument „koncepcja i założenia funkcjonalne do projektu budowy/modernizacji systemów zabezpieczeń elektronicznych jednostki" stanowi podstawę do opracowania koncepcji i założeń technicznych.
2	Opracowanie koncepcji i założeń technicznych	Dokument musi zawierać: 1. dane techniczno-informacyjne stosowanych obecnie urządzeń /systemów wymagających modernizacji; 2. realizację techniczną funkcjonalności systemu określonych w koncepcji i założeniach funkcjonalnych; 3. uzasadnienie proponowanych rozwiązań; 4. założenia do projektu (szkice koncepcyjne, rysunki sytuacyjne); 5. oszacowanie kosztów i określenie sposobu finansowania (środki własne, środki OISW/CZSW).	Służba Informatyczna	Opracowane dokumenty „koncepcja i założenia funkcjonalne do projektu budowy/modernizacji systemów zabezpieczeń elektronicznych jednostki" i „koncepcja i założenia techniczne do projektu budowy/modernizacji systemów zabezpieczeń elektronicznych jednostki" przekazuje się się do właściwego OISW celem zaopiniowania i weryfikacji.
3	Uzyskanie pozytywnej opinii OISW	Weryfikacja i opiniowanie zaproponowanych rozwiązań pod kątem zasadności, zgodności z wytycznymi i przepisami branżowymi.	1. Specjalista ds. służby informatycznej 2. Specjalista ds. ochronnych	1. Dokumentację, która uzyskała negatywną opinię OISW zwraca się do jednostki celem uzupełnienia i korekty. 2. Pozytywnie zaopiniowaną dokumentację zwraca się do jednostki organizacyjnej celem realizacji zadania. 3. W przypadku ubiegania się o dodatkowe środki finansowe z CZSW na realizację zadania zaopiniowaną dokumentację przekazuje się do CZSW.
4	Uzyskanie pozytywnej opinii CZSW	Weryfikacja i opiniowanie zaproponowanych rozwiązań pod kątem zasadności, zgodności z wytycznymi i przepisami branżowymi.	1. Biuro Ochrony i Spraw Obronnych 2. Biura Informatyki i Łączności	Zaopiniowaną dokumentację przekazuje się do właściwego OISW celem dalszego poprowadzenia sprawy.