

WYTYCZNE NR 6 /2024
Dyrektora Generalnego Służby Więziennej

z dnia 21 października 2024 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. z 2023 r. poz. 1683 i 1860 oraz z 2024 r. 1222) oraz art. 249a pkt 9 ustawy z dnia 6 czerwca 1997 r. Kodeks karny wykonawczy (Dz.U. z 2024 r. poz. 706), ustala się co następuje:

Rozdział I
Przepisy ogólne

§ 1. Ilekcć w dalszej części wytycznych mowa o:

- 1) administratorze SłiZE (Systemów łączności i Zabezpieczeń Elektronicznych), rozumie się przez to wyznaczonego przez kierownika jednostki funkcjonariusza lub pracownika pionu informatyki i łączności;
- 2) alarmie, rozumie się przez to ostrzeżenie o istnieniu zagrożenia dla zdrowia lub życia, mienia lub środowiska;
- 3) analizie zagrożeń, rozumie się przez to identyfikowanie zagrożeń w poszczególnych strefach powodujących zainicjowanie alarmu oraz oszacowanie prawdopodobieństwa ich wystąpienia;
- 4) CCTV, rozumie się przez to system telewizji przemysłowej;
- 5) DGSW, rozumie się przez to Dyrektora Generalnego Służby Więziennej;
- 6) dokumentacji powykonawczej, rozumie się przez to dokument, w którym są zapisane szczegóły zainstalowanego systemu;
- 7) instalatorze, rozumie się przez to osobę odpowiedzialną za instalację systemu;
- 8) jednostce, rozumie się przez to jednostkę organizacyjną Służby Więziennej;
- 9) kierownikowi jednostki, rozumie się przez to kierownika jednostki organizacyjnej Służby Więziennej;
- 10) konserwacji systemu, rozumie się przez to utrzymanie systemu w dobrym stanie, na które składają się przeglądy, naprawy, kontrola działania;
- 11) operatorze przejścia, rozumie się przez to osobę, która znajduje się poza chronioną strefą i realizuje funkcję autoryzacji przejścia (np.: operator monitoringu);
- 12) przeglądzie systemu, rozumie się przez to sprawdzenie stanu technicznego z reguły w określonych odstępach czasu;
- 13) podwójnej autoryzacji, rozumie się przez to zastosowanie dwóch wykluczających się sposobów autoryzacji jednej osoby (np.: karta + PIN) lub jednego sposobu

- autoryzacji osoby, połączonego z autoryzacją realizowaną przez operatora przejścia (np.: PIN + operator przejścia lub karta + operator przejścia);
- 14) serwerze NTP (ang. *Network Time Protocol*), rozumie się przez to serwer synchronizacji czasu wzorcowego;
 - 15) SKD, rozumie się przez to System Kontroli Dostępu;
 - 16) sabotażu, rozumie się przez to umyślne zakłócenie działania systemu zabezpieczenia elektronicznego lub jego części;
 - 17) SSWiN, rozumie się przez to System Sygnalizacji Włamania i Napadu;
 - 18) strefie, rozumie się przez to wyznaczony lub wydzielony obszar;
 - 19) zagrożeniu, rozumie się przez to źródło potencjalnej szkody lub okoliczności potencjalnie szkodliwej;
 - 20) zasadzie wiedzy koniecznej, rozumie się przez to zobowiązanie każdego funkcjonariusza i pracownika do posiadania wiedzy o systemie, do którego ma dostęp, ograniczonej wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.

§ 2. 1. Wytyczne określają standardy projektowania i instalacji systemów zabezpieczeń elektronicznych w jednostkach, 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;
- 5) zasady projektowania, instalacji i odbioru 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, po uzyskaniu pozytywnej opinii właściwego dyrektora okręgowego, wymagają pisemnej zgody DGSW.

§ 3. 1. W jednostkach stosuje się następujące systemy zabezpieczeń elektronicznych:

- 1) SSWiN;
- 2) SKD;
- 3) CCTV.

2. Systemy należy projektować, instalować i użytkować zgodnie z aktualnie obowiązującymi polskimi normami.

3. Elementy składowe SSWiN (centrale, kontrolery, ekspandery, manipulatory) muszą spełniać wymogi zabezpieczenia w stopniu minimum 3 wg normy PN-EN 50131-1. Wszystkie pozostałe elementy i systemy wchodzące w skład SSWiN, (np. czujki dymu, temperatury, zalania wodą, przyciski sterowania itp.) są elementami i systemami uzupełniającymi i nie wymagają spełniania normy w stopniu 3.

4. W SSWiN stosuje się parametryzowanie linii.

5. W celu podniesienia bezpieczeństwa i niezawodności całości systemu stosuje się integrację systemów wymienionych w ust. 1.

6. Dopuszcza się stosowanie systemów uzupełniających, innych niż wymienione w ust. 1.

7. W urządzeniach posiadających możliwość synchronizacji czasu z serwera NTP, należy tę funkcjonalność uruchomić.

8. Nadrzędnym serwerem czasu dla wszystkich systemów zabezpieczeń elektronicznych jest centralny serwer NTP.

9. Czasookres przechowywania logów systemowych w systemach wymienionych w ust. 1 wynosi minimum 30 dni.

§ 4. 1. Kierownik jednostki zleca kierownikowi działu ochrony przeprowadzenie analizy zagrożeń oraz podziału jednostki na strefy ochronne wraz z określeniem wymagań funkcjonalnych dla każdej z nich.

2. Ustala się następujący podział na strefy ochrony jednostek za pomocą zabezpieczeń elektronicznych:

- 1) strefa A - budynki zakwaterowania osadzonych oraz budynki lub ich części, w których realizowane są widzenia;
- 2) strefa B – wyznaczona linia lub obszar przy budynkach zakwaterowania osadzonych i obiektów bezpośrednio do nich przyległych będące dodatkowym zabezpieczeniem strefy A;
- 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.

3. Podział na strefy, o którym mowa w ust. 2, jednostki wykonują w oparciu o plan sytuacyjny, stanowiący załącznik instrukcji ochronnej.

§ 5. 1. Osoba odpowiedzialna za projektowanie, instalowanie, konserwację i naprawy systemu powinna posiadać odpowiednie kwalifikacje.

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 II

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) dopuszcza się wyłączenie systemu, o którym mowa w pkt. 1, jedynie na czas niezbędny, wyłącznie w uzasadnionych przypadkach, w tym w przypadku zagrożenia zdrowia, życia lub mienia;
- 3) śluzy wyposaża się w CCTV zapewniający obserwację bezpośredniego obszaru przed wejściem/wyjściem, SKD z identyfikacją osób, system zapewniający sygnalizację otwartych drzwi;
- 4) wejście lub wyjście do i ze strefy wymaga podwójnej autoryzacji;
- 5) przejścia w strefie wyposaża się w SKD i CCTV; wymagana jest identyfikacja osób wchodzących i wychodzących;
- 6) ciągi komunikacyjne, miejsca i pomieszczenia wyznaczone do pracy, nauki, widzeń, odprawiania nabożeństw, spotkań religijnych oraz zajęć kulturalno-oświatowych oraz z zakresu kultury fizycznej i sportu wyposaża się w CCTV;
- 7) dyżurki oddziałowych wyposaża się w urządzenia umożliwiające obserwację nadzorowanych pomieszczeń i oddziałów;
- 8) wszystkich pracowników i funkcjonariuszy realizujących zadania w strefie A, w tym w pomieszczeniach sal widzeń, wyposaża się w przyciski napadowe zgodne z aktualnymi wytycznymi DGSW w sprawie wymagań technicznych i ochronnych dla pawilonów zakwaterowania osadzonych w jednostkach;
- 9) sterowane elektronicznie włazy dachowe i klapy wyposaża się w sygnalizację otwarcia.

§ 7. Zabezpieczenia stosowane w strefie B powinny spełniać następujące warunki:

- 1) wyposażenie w SSWiN zawierający urządzenia wykrywające obecność osób;
- 2) dopuszcza się zabezpieczenie obiektu przyległego bezpośrednio do budynków zakwaterowania osadzonych poprzez zabezpieczenie wyłącznie miejsca ich styku systemem, o którym mowa w pkt. 1;
- 3) weryfikacja alarmów z SSWiN powinna być dokonywana na podstawie CCTV; 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) obszar bezpośrednio przyległy do pasa ochronnego zabezpiecza się stosując SSWiN wyposażony w urządzenia wykrywające obecność osób;
- 2) w przypadku braku możliwości zastosowania rozwiązania, o którym mowa w pkt. 1, ze względu na warunki architektoniczne jednostki, dopuszcza się instalację tych systemów bezpośrednio na pasie ochronnym;
- 3) informacja optyczno-akustyczna o wystąpieniu alarmu musi być sygnalizowana na stanowisku dowódcy zmiany oraz obserwatora terenu;
- 4) do weryfikacji alarmów z SSWiN stosuje się CCTV oparty o kamery stałopozycyjne; rozmieszczenie kamer musi zapewnić obserwację całego pasa ochronnego bez martwych stref wraz z obszarem objętym systemem, o którym mowa w pkt. 1; obraz musi zapewniać identyfikację zdarzenia w celu pozyskania informacji o ujawnieniu osoby;
- 5) wejścia i wyjścia z pasa ochronnego wyposaża się w sygnalizację otwarcia; dopuszcza się stosowanie SKD;
- 6) bramy wjazdowe i wyjazdowe oraz wejścia i wyjścia piesze z terenu jednostki wyposaża się w system śluzowania (blokada wykluczająca);
- 7) bramy, wejścia i wyjścia wchodzące w skład systemu śluzowania, o którym mowa w pkt. 6, wyposaża się w sygnalizację otwarcia;
- 8) w śluzach dla pojazdów stosuje się CCTV zapewniający:
 - a) obserwację bezpośredniego zewnętrznego obszaru przed bramą wjazdową na teren jednostki,
 - b) identyfikację pojazdu wjeżdżającego do śluzy i z niej wyjeżdżającego wraz z obserwacją dachu i podwozia,
 - c) obserwację obszaru znajdującego się wewnątrz śluzy;
- 9) w śluzach pieszych stosuje się systemy zapewniające:
 - a) obserwację bezpośredniego obszaru przed wejściem i wyjściem na i z terenu jednostki,
 - b) CCTV z pełną identyfikacją osób;
- 10) stanowisko pracy bramowego wyposaża się w urządzenia umożliwiające monitorowanie i obserwację nadzorowanych przez niego obszarów.

§ 9. W strefie D mogą być stosowane systemy zabezpieczenia elektronicznego, o których mowa w § 3 ust. 1.

§ 10. Zabezpieczenia stosowane w strefie E powinny spełniać następujące warunki:

- 1) pomieszczenia serwerowni wyposaża się co najmniej w:
 - a) SKD,
 - b) drzwi antywłamaniowe w klasie RC3,
 - c) SSWiN realizujący detekcję ruchu i otwarcia drzwi wyposażony w urządzenia zapewniające detekcję dymu (w przypadku, gdy nie istnieje odrębny system

- sygnalizacji pożarowej), stłuczenia szyby (jeżeli takowa ma zastosowanie) i zalania wodą,
- d) system monitorujący temperaturę i wilgotność powietrza,
 - e) system klimatyzacji,
 - f) system informujący o zaniku zasilania;
- 2) pomieszczenia magazynów wyposaża się w SSWiN zapewniający detekcję ruchu i otwarcia drzwi doposażony w urządzenia zapewniające detekcję dymu (w przypadku, gdy nie istnieje odrębny system sygnalizacji pożarowej); kierownik jednostki określi w analizie, o której mowa § 4 ust. 1, pomieszczenia magazynowe wymagające objęcia tym systemem;
- 3) place spacerowe wyposaża się w CCTV; rozmieszczenie kamer musi zapewnić obserwację całego chronionego obszaru bez martwych stref; Obraz musi zapewniać identyfikację zdarzenia; stanowisko spacerowego wyposaża się w urządzenia umożliwiające obserwację nadzorowanych placów spacerowych;
- 4) sposób ochrony magazynów uzbrojenia, kancelarii tajnych, archiwów określają odrębne przepisy.

§ 11. 1. Minimalne wymagania techniczne poszczególnych elementów CCTV i SKD określa załącznik nr 1.

2. Dopuszcza się stworzenie w SKD „specjalnego nośnika dostępowego” o podwyższonych uprawnieniach, który umożliwia otwarcie wszystkich lub większości przejść, wejść i wyjść w jednostce, również z pominięciem mechanizmu podwójnej weryfikacji, śluzowania lub innych ograniczeń.

3. Nośnik, o którym mowa w ust. 2, deponowany jest w pomieszczeniu wartowni, w szczególnie bezpieczny sposób. Kierownik jednostki określi ograniczoną do niezbędnego minimum listę użytkowników upoważnionych do jego pobrania.

4. Pobranie i użytkowanie nośnika, o którym mowa w ust. 2, dopuszczalne jest jedynie na czas niezbędny i wyłącznie w szczególnie uzasadnionych przypadkach, w tym zagrożenia zdrowia, życia, mienia lub bezpieczeństwa jednostki.

5. Każdorazowe pobranie lub użycie nośnika, o którym mowa w ust. 2, musi zostać udokumentowane w książce przebiegu służby dowódcy zmiany.

6. Funkcjonariuszy i pracowników realizujących zadania w strefach B-E, w wyniku przeprowadzonej analizy zagrożeń, o której mowa § 4 ust. 1, wyposaża się w przyciski napadowe stacjonarne lub bezprzewodowe, o których mowa w aktualnych wytycznych DGSW w sprawie wymagań technicznych i ochronnych dla pawilonów zakwaterowania osadzonych w jednostkach.

Rozdział III

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 2.

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

- 1) projektowanie systemu wraz z uzyskaniem pozytywnej opinii, o której mowa w załączniku nr 2;
- 2) wykonanie systemu;
- 3) wykonanie dokumentacji powykonawczej;
- 4) uruchomienie systemu wraz ze szkoleniem dla administratorów (z przekazaniem dokumentacji szkoleniowej);
- 5) sprawdzenie systemu wraz ze szkoleniem użytkowników (z przekazaniem dokumentacji szkoleniowej);
- 6) 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) opis konfiguracji systemu i lokalizacji urządzeń;
 - 8) opis organizacji zasilania podstawowego i rezerwowego wraz z bilansem mocy;
 - 9) zestawienie urządzeń;
 - 10) świadectwa i certyfikaty urządzeń i materiałów wykorzystywanych do budowy systemu;
 - 11) schemat blokowy systemu;
 - 12) podkłady budowlane z rozmieszczeniem elementów systemu i tras kablowych (w wersji papierowej oraz edytowalnej elektronicznej).
2. Na podstawie projektu wykonany zostaje kosztorys inwestorski i przedmiar robót.

§ 15. 1. Montaż systemów zabezpieczeń elektronicznych może być wykonywany 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 Służbie Więziennej.

§ 16. 1. Instalacje urządzeń należy wykonać zgodnie z ich dokumentacją techniczną.

2. Prace instalacyjne, uruchomieniowe i konserwacyjne wymagają stosowania przepisów BHP przy ich realizacji.

3. Parametry przewodów elektrycznych (typ, przekrój żył, rezystancja, rodzaj izolacji itp.) powinny być zgodne z zaleceniami producenta i zasadami wiedzy technicznej.

4. Połączenia przewodów elektrycznych powinny mieć odpowiednią wytrzymałość mechaniczną i elektryczną. Do połączeń przewodów należy wykorzystywać dedykowane urządzenia i materiały dostosowane 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. Okablowanie powinno być odpowiednio zamocowane, rozprowadzone oraz zabezpieczone w celu uniknięcia uszkodzeń mechanicznych lub wynikających z warunków środowiskowych, z uwzględnieniem bezpiecznej odległości od innych instalacji, w tym od instalacji odgromowej.

7. Elementy zabezpieczenia elektronicznego winny być instalowane w sposób uniemożliwiający ich wykorzystanie do pokonania zabezpieczeń techniczno-ochronnych.

8. Elementy zabezpieczenia elektronicznego powinny być instalowane w sposób zapewniający ich optymalne wykorzystanie, w miejscach, w których nie będą zakłócane przez inne elementy zabezpieczeń techniczno-ochronnych.

9. Działanie zainstalowanych elementów zabezpieczenia elektronicznego (w tym kamer telewizji przemysłowej) nie może być zakłócane przez inne urządzenia i systemy montowane na terenie jednostki.

§ 17. 1. Sprawdzenie systemu odbywa się w obecności kierownika działu ochrony, kierownika działu kwatermistrzowskiego oraz administratora SŁiZE.

2. Po sprawdzeniu systemu sporządza się protokół odbioru.

3. Instalator przekazuje administratorowi SŁiZE dokumentację powykonawczą zawierającą informacje dotyczące wszystkich poziomów dostępu do systemu wraz z loginami i hasłami.

4. Hasła, o których mowa w ust. 3, podlegają niezwłocznej zmianie po odbiorze systemu, przed oddaniem go do użytkowania.

5. Po zatwierdzeniu protokołu odbioru osobą odpowiedzialną za funkcjonowanie systemu staje się administrator SŁiZE.

6. Użytkownik systemu odpowiedzialny jest za niezwłoczne zgłaszanie administratorowi SŁiZE wszelkich nieprawidłowości i usterek systemów.

§ 18. Dokumentacja powykonawcza powinna zawierać:

- 1) dane firmy instalacyjnej;
- 2) projekt wykonawczy systemu z naniesionymi ewentualnymi zmianami (w opisie, zestawieniu materiałów jak i rysunkach), opatrzony zapisem – „DOKUMENTACJA POWYKONAWCZA” zgodnie z aktualnym Prawem budowlanym wraz z atestami, certyfikatami oraz pomiarami instalacji elektrycznych i teletechnicznych;
- 3) instrukcję eksploatacji systemu;
- 4) harmonogram konserwacji z danymi kontaktowymi osoby odpowiedzialnej za konserwację/naprawy;
- 5) protokół z przeszkolenia obsługi przekazywanego systemu z zapisem miejsca, daty oraz danych osób szkolących i przeszkolonych;
- 6) protokół odbioru;
- 7) deklarację zgodności dla urządzeń zastosowanych w systemie, które wymagają klasyfikacji według norm.

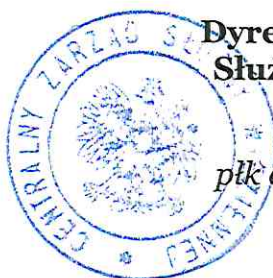
Rozdział IV **Przepisy końcowe**

§ 19. Czynności, o których mowa w § 4 ust. 1, wykonują wszystkie jednostki w terminie do dnia 30 kwietnia 2025 roku.

§ 20. Szczegółowe zasady eksploatacji i konserwacji systemów zabezpieczeń elektronicznych zostały określone w obowiązującym zarządzeniu DGSW w sprawie szczegółowych zasad eksploatacji i rozwoju systemów łączności i zabezpieczeń elektronicznych w jednostkach.

§ 21. Tracą moc Wytyczne Nr 4/2022 Dyrektora Generalnego Służby Więziennej z dnia 30 grudnia 2022 r. w sprawie określenia standardów systemów zabezpieczeń elektronicznych w jednostkach organizacyjnych Służby Więziennej.

§ 22. Wytyczne wchodzi w życie z dniem 1 listopada 2024 r.

**Dyrektor Generalny**
Służby Więziennej
plk dr Andrzej Pecka

UZASADNIENIE

W związku z nieustającym postępem technologicznym w zakresie dziedziny elektronicznej ochrony obiektów oraz oferowanymi na rynku różnorodnymi rozwiązaniami w tym obszarze, zaistniała potrzeba zmodyfikowania istniejącego dokumentu zawierającego 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 i instalacji elektronicznych systemów zabezpieczeń. Dokument ten wyznacza jednocześnie minimalne standardy, które powinny być zastosowane podczas określania wymagań funkcjonalnych i technicznych systemów.

Przepisy zawarte w niniejszym dokumencie mają zastosowanie do nowobudowanych lub modernizowanych jednostek lub ich części, w których zawarto zadania dotyczące instalacji nowego systemu zabezpieczeń elektronicznych.

Załącznik nr 1

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

1. Zasilanie urządzeń wchodzących w skład telewizji przemysłowej :

- 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 zespołów prądowców i zabezpieczone ochronnikami przepięć.
- 1.2. Zasilacze buforowe z akumulatorami i UPS-y powinny umożliwić pracę podłączonych urządzeń do czasu uruchomienia zasilania z zespołów prądowców - nie krócej jednak niż przez 30 minut.

2. Elementy systemu CCTV:

- 2.1. Systemy telewizji przemysłowej realizuje się w technologii cyfrowej IP.
- 2.2. Do budowy infrastruktury kablowej stosuje się aktualne normy dotyczące budowy okablowania strukturalnego, przy zastosowaniu skrętki komputerowej i osprzętu minimum kategorii 6 lub światłowodu.
- 2.3. Realizacja stanowiska obserwacji monitoringu wizyjnego musi uwzględniać przepisy BHP i zasady ergonomii stanowiska pracy.
- 2.4. Zasadą jest stosowanie kamer stałopozycyjnych, kamery obrotowe są kamerami uzupełniającymi.
- 2.5. Punkty kamerowe systemu CCTV:
 - 2.5.1. Minimalne wymagania dla kamer:
 - 2.5.1.1. rozdzielczość 2 Mpx (1920×1080 przy 25kl/s),
 - 2.5.1.2. 2 niezależnie konfigurowalne strumienie,
 - 2.5.1.3. 5 jednoczesnych połączeń (w tym jeden rezerwowany dla systemów centralnych),
 - 2.5.1.4. 4 użytkowników (w tym jeden rezerwowany dla systemów centralnych),
 - 2.5.1.5. zabezpieczenie dostępu - minimum 2 poziomy dostępu: administrator i użytkownik; dostęp ograniczony hasłem,
 - 2.5.1.6. system pracy w kolorze z automatycznym przełączeniem w tryb czarno-biały z mechanicznym filtrem podczerwieni,
 - 2.5.1.7. widoczność obserwowanej sceny w każdych warunkach oświetleniowych (dopuszcza się doświetlanie sceny zewnętrznym oświetlaczem podczerwieni),
 - 2.5.1.8. automatyczny tryb dzień/noc,
 - 2.5.1.9. zasilanie PoE 802.3af/at, dopuszcza się alternatywnie zasilanie 12V lub 24V,
 - 2.5.1.10. kodek H.264 lub nowszy,
 - 2.5.1.11. strefy prywatności w ilości adekwatnej do obserwowanej sceny,
 - 2.5.1.12. dopuszczalny zakres temperatur pracy, dostosowany do faktycznych warunków użytkowania,

- 2.5.1.13. długość ogniskowej dopasowana do obserwowanej sceny,
- 2.5.1.14. obsługa protokołów sieciowych ONVIF, TCP/IP, RTSP, NTP, DHCP, DNS, HTTP, HTTPS,
- 2.5.1.15. analiza obrazu - detekcja ruchu, zmiana sceny, zmiana ostrości,
- 2.5.1.16. menu ekranowe w języku polskim.
- 2.5.2. Kamery montowane w celach mieszkalnych i kąpokach sanitarnych poza parametrami zawartymi w punkcie 2.5.1 muszą:
 - 2.5.2.1. zapewnić obserwację całego obszaru bez martwych stref,
 - 2.5.2.2. posiadać stopień ochrony IP 66.
- 2.5.3. Kamery montowane w łazniach, kuchniach i innych pomieszczeniach o podwyższonej wilgotności, poza parametrami zawartymi w punkcie 2.5.1, muszą posiadać :
 - 2.5.3.1. 90% odporność na kondensację (kontakt z wodą),
 - 2.5.3.2. stopień ochrony IP 67.
- 2.5.4. Kamery zainstalowane w sposób umożliwiający nieograniczony i bezpośredni do nich dostęp osób nieuprawnionych, wyposażone są w obudowę zapewniającą stopień ochrony przed uderzeniem IK-10 (obudowa wandaloodporna).

3. Urządzenia utrwalające obraz lub dźwięk:

3.1. Dopuszcza się stosowanie urządzeń:

- 3.1.1. serwery CCTV,
- 3.1.2. rejestratory IP,
- 3.1.3. macierze dyskowe.

3.2. W urządzeniach wymienionych w pkt. 3.1 stosuje się sprzętowy mechanizm ochrony danych na poziomie minimum RAID 1.

3.3. System realizowany w oparciu o urządzenia opisane w pkt 3.1.1 -3.1.2 musi zapewnić:

- 3.3.1. znacznik czasu nagrania - data i godzina czasu lokalnego,
- 3.3.2. obsługę protokołów sieciowych ONVIF, TCP/IP, RTSP, NTP, DHCP, DNS, HTTP, HTTPS,
- 3.3.3. kompresję H.264 lub nowszą,
- 3.3.4. zabezpieczenie dostępu - minimum 2 poziomy dostępu: administrator i użytkownik; dostęp ograniczony hasłem,
- 3.3.5. możliwość archiwizacji strumienia danych z pojedynczej kamery, kilku wybranych kamer jednocześnie lub wszystkich kamer,
- 3.3.6. minimalną rozdzielczość archiwizowanego materiału 1920×1080 przy 12kl/s,
- 3.3.7. oprogramowanie do obsługi w języku polskim.

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

1. Należy stosować kontrolery drzwi z niezależnym zasilaniem buforowym, które po utracie komunikacji z jednostką nadrzędną nadal umożliwiają realizację kontroli i sterowania przejściem.
2. Jako układ zbliżeniowy dla nośników dostępowych w systemach kontroli dostępu wyznacza się standard MIFARE® Plus X¹, 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 szyfrującego AES (ang. *Advanced Encryption Standard*) z kluczami 128 bitowymi.
3. Należy stosować czytniki nośników dostępowych w standardzie Mifare® Plus X, odczytujące klucz zapisany w sektorze pamięci SSN (najpierw weryfikowany jest klucz między czytnikiem a nośnikiem, dopiero po uzyskaniu pozytywnego wyniku następuje odczyt numeru CSN).
4. Do komunikacji pomiędzy kontrolerem i czytnikiem dopuszcza się protokoły Wiegand, RS485 i TCP/IP, OSDP.
5. Nośnik, o którym mowa w pkt 2 każdorazowo przed opuszczeniem terenu jednostki musi zostać deaktywowany w systemie kontroli dostępu. Aktywacja nośnika w systemie kontroli dostępu musi następować za pomocą czytników z wykorzystaniem szyfrowania numeru SSN.
6. Okablowanie systemu należy zabezpieczyć przed niepowołanym dostępem i sabotażem.
7. Należy stosować śruby z zabezpieczeniem, tak aby otwarcie obudowy czytnika wymagało specjalnego narzędzia.
8. Pojedyncze przejście (drzwi/krata) należy wyposażać w czytnik kart, kontaktron, zamek elektromechaniczny oraz system telewizji dozorowej wg parametrów opisanych w wytycznych.
9. Przejścia i wejścia do pomieszczeń muszą zapewniać każdorazową identyfikację osoby ubiegającej się o dostęp.
10. Wyjścia z pomieszczeń (np. serwerownia, magazyn) mogą odbywać się bez konieczności zachowania identyfikacji osoby wychodzącej z wykorzystaniem klamki lub przycisku wyjścia.
11. Przejścia (drzwi/kraty) muszą posiadać możliwość mechanicznego ich otwarcia kluczem.
12. Systemy kontroli dostępu muszą dostarczać sygnały z przejść takie jak: otwarte, zamknięte, uszkodzenie/sabotaż, otwarcie nieautoryzowane. Stany te powinny być zapisywane w dzienniku zdarzeń systemu.

¹ Mifare® Plus X jest określeniem standardu ISO/IEC 14443 opracowanego dla kart zbliżeniowych (bezstykowych).

Proces opracowywania koncepcji i założeń do projektu budowy lub modernizacji systemów elektronicznego zabezpieczenia jednostek

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.		1. Dział ochrony	Opracowany dokument „konceptcja i założenia funkcjonalne do projektu budowy/modernizacji systemów zabezpieczeń elektronicznych jednostki” stanowi podstawę do opracowania koncepcji i założeń technicznych. Dokument przekazywany jest do służby informatycznej i działu kwatermistrzowskiego.
2.	Opracowanie koncepcji i założeń technicznych	Dokument musi zawierać: 1. dane techniczno-informacyjne stosowanych obecnie urządzeń /systemów wymagających modernizacji; 2. założenia do projektu wraz z proponowaną realizacją techniczną funkcjonalności systemu określonych w koncepcji i założeniach funkcjonalnych (w tym ewentualne szkice koncepcyjne, rysunki sytuacyjne); 3. uzasadnienie proponowanych rozwiązań; 4. wstępne oszacowanie kosztów i określenie sposobu finansowania.		1. Służba informatyczna 2. Dział kwatermistrzowski	Opracowane dokumenty „konceptcja i założenia funkcjonalne do projektu budowy/modernizacji systemów zabezpieczeń elektronicznych jednostki” i „konceptcja i założenia techniczne do projektu budowy/modernizacji systemów zabezpieczeń elektronicznych jednostki” przekazuje 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 3. Specjalista ds. kwatermistrzowskich	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 weryfikacji CZSW	Weryfikacja zaproponowanych rozwiązań pod kątem zasadności na podstawie nadesłanej opinii OISW.		1. Biuro Ochrony i Spraw Obronnych 2. Biuro Informatyki i Łączności 3. Biuro Kwatermistrzowsko-Inwestycyjne	Zweryfikowaną dokumentację przekazuje się do właściwego OISW celem dalszego prowadzenia sprawy.

