

**WYTYCZNE W ZAKRESIE PLANOWANIA, ORGANIZACJI ORAZ
FUNKCJONOWANIA OCHRONY OBIEKTÓW
PAŃSTWOWEGO GOSPODARSTWA WODNEGO WODY POLSKIE
(PGW WP)**

Warszawa, 05.07.2021 r

SPIS TREŚCI

Rozdział 1	Organizacja systemu ochrony obiektów PGW WP	3
Rozdział 2	Ochrona fizyczna obiektów	5
Rozdział 3	Ochrona techniczna obiektów	11
Rozdział 4	Szkolenie w zakresie ochrony obiektów	28
Rozdział 5	Kontrola systemu ochrony obiektów	28

Załączniki:

Załącznik nr 1	Wybrane elementy umowy na świadczenie usługi w zakresie ochrony fizycznej obiektów	30
Załącznik nr 2	Zawartość Planu ochrony szczególnej obiektu kategorii I	40
Załącznik nr 3	Zawartość Instrukcji ochrony	42
Załącznik nr 4	Obowiązki administratora systemu ochrony technicznej	44
Załącznik nr 5	Wymagania dla depozytorów kluczowych	45
Załącznik nr 6	Dokumentacja dotycząca eksploatacji systemów i urządzeń alarmowych	46

WYKAZ DOKUMENTÓW NORMATYWNYCH

1. Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. 2020 poz.838).
2. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2020 poz.1856).
3. Ustawa z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz.U. 2019 poz. 2418).
4. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.U. 2010 nr 83 poz. 541).
5. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz.U. 2010 nr 83 poz. 542).
6. Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony (Dz.U. 2003 nr 116 poz. 1090 z późn. zm.).
7. Rozporządzenia Ministra Spraw Wewnętrznych z dnia 16 grudnia 2013 r. w sprawie dokumentowania działalności gospodarczej w zakresie usług ochrony osób i mienia (Dz.U. 2013 poz. 1739).
8. Decyzja Nr 22/MON Ministra Obrony narodowej z dnia 26 lutego 2021 r. w sprawie wprowadzenia „Wytucznych w sprawie przygotowania i prowadzenia szczególnej ochrony obiektów kategorii I” (Dz. Urz. MON 2021 poz. 27).
9. „Narodowy Program Ochrony Infrastruktury Krytycznej” – tekst jednolity.
10. „Metodyka uzgadniania planów ochrony obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie”.

kierownictwa jednostki organizacyjnej, kancelarie niejawne, serwerownie, archiwa, pomieszczenia techniczne, magazyny itp.

W obiektach kategorii IV nie zaleca się wyposażania w techniczne środki ochronne wszystkich pomieszczeń.

Dyrektorzy (Kierownicy) jednostek organizacyjnych PGW WP, których obiekty są zakwalifikowane do grupy IV zobowiązani są do opracowania dla nich Instrukcji ochrony. Przedmiotowy dokument powinien określać zasady i organizację ochrony, w tym procedury postępowania pracowników i sił ochronnych w przypadku napadu, podłożenia ładunku wybuchowego, zagrożenia atakiem bioterrorystycznym, włamania i zdarzeń losowych. Zawartość Instrukcji ochrony określa **załącznik nr 3**.

Rozdział 3

OCHRONA TECHNICZNA OBIEKTÓW

3.1. Wymagania ogólne

Organizując nowy system ochrony lub planując modernizację istniejącego systemu, należy w jak najszerszym zakresie uwzględnić wszystkie możliwe do zastosowania techniczne środki wspomagające ochronę fizyczną, które mogą ograniczyć do niezbędnego minimum liczebność sił ochronnych.

Niniejsze wymagania dotyczą obiektów i budowli hydrotechnicznych, które są zakwalifikowane do grupy I-III (wyszczególniając z tych obiektów ważne z punktu widzenia obronności i bezpieczeństwa państwa pomieszczenia, magazyny, urządzenia hydrotechniczne itp.) oraz pomieszczeń kierownictwa jednostki organizacyjnej, kancelarii niejawnych, serwerowni, archiwów, pomieszczeń technicznych, magazynów, itp. w obiektach zaliczonych do grupy IV. Opisane poniżej wymagania techniczno-eksploatacyjne należy stosować w nowobudowanych systemach ochrony technicznej.

Wymagania dotyczące zabezpieczenia technicznego nie dotyczą obiektów wynajmowanych, które zostały wyposażone w urządzenia ochronne przez wynajmującego.

Biorąc powyższe pod uwagę należy wyjść z założenia, że obiektów nie chronią systemy i urządzenia alarmowe, gdyż pełnią one tylko rolę wspomagającą dla sił ochronnych. Każdy zainstalowany system, urządzenie alarmowe w obiekcie powinno być nadzorowane przez ochronę fizyczną realizowaną siłami ochronnymi (w obiekcie lub poprzez zewnętrzną stację monitorowania alarmów).

1. W skład technicznych środków wspomagających ochronę fizyczną wchodzi:
 - 1) ogrodzenia,
 - 2) oświetlenie obiektów,
 - 3) środki łączności sił ochronnych,
 - 4) systemy i urządzenia alarmowe,
 - 5) zabezpieczenia mechaniczne.
2. Podział chronionego obiektu na strefy ochrony:
 - 1) **strefa ochrony zewnętrznej** – obszar bezpośrednio przyległy do ogrodzenia wewnętrznego i do poszczególnych budynków, urządzeń rozmieszczonych na

- terenach obiektu, gdzie instaluje się zewnętrzne urządzenia alarmowe (UA), systemy telewizji dozorowej (STD), systemy kontroli dostępu (SKD),
- 2) **strefa ochrony wewnętrznej** – obszar wewnątrz budynków pomieszczeń i urządzeń, gdzie instaluje się wewnętrzne urządzenia alarmowe (UA), systemy telewizji dozorowej (STD), systemy kontroli dostępu (SKD).
3. Funkcje systemu ochrony technicznej:
- 1) **wczesne wykrycie wtargnięcia** – każda próba wtargnięcia musi być wykryta przez urządzenie alarmowe znajdujące się w strefie ochrony zewnętrznej lub strefie wewnętrznej,
 - 2) **rozpoznanie źródła alarmu** – każdy wywołany w systemie alarm musi być rozpoznawany pod kątem źródła, które go wywołało (alarm techniczny np. niesprawność czujki, alarm właściwy – intruz,
 - 3) **opóźnienie działania intruza** – ewentualny intruz na swej drodze musi napotkać bariery mechaniczne w postaci ogrodzeń, drzwi antywłamaniowych, krat, szyb wzmocnionych, kłódek itp. wydłużające czas jego dotarcia do obiektu tak, aby umożliwić skuteczne przeciwdziałanie,
 - 4) **właściwa komunikacja** – każda informacja, począwszy od urządzenia alarmowego, czujki, przycisku napadowego, kamery itp. musi dotrzeć do właściwego centrum nadzoru systemu i uruchomić te siły i środki, które są niezbędne do przeciwdziałania zagrożeniu,
 - 5) **przeciwdziałanie** – każdy rozpoznany alarm powinien spowodować podjęcie odpowiednich kroków interwencyjnych przez siły ochronne.
4. Systemy i urządzenia alarmowe stosowane w obiektach PGW WP powinny spełniać następujące warunki:
- 1) wykorzystywać optymalnie parametry techniczne czujek w chronionym rejonie, obszarze, terenie lub pomieszczeniu,
 - 2) nie utrudniać codziennej pracy personelu w chronionym obszarze, rejonie, terenie, obiekcie lub pomieszczeniu, a sposób działania systemu powinien być uzgodniony z osobami odpowiedzialnymi za ochronę obiektów,
 - 3) uwzględniać już istniejące inne systemy sygnalizacji zagrożeń (np. pożarowe) oraz stanowić uzupełnienie innych rodzajów środków zabezpieczających,
 - 4) nie mieć szkodliwego wpływu na zdrowie ludzi przebywających w chronionym obszarze, obiekcie lub pomieszczeniu, w których są one zamontowane,
 - 5) funkcjonować poprawnie niezależnie od warunków środowiskowych.

Realizując inwestycję technicznego zabezpieczenia obiektu wykorzystujemy następujące typy systemów ochrony technicznej:

- 1) systemy alarmowe,
- 2) systemy telewizji dozorowej,
- 3) systemy kontroli dostępu,
- 4) systemy transmisji alarmów.

3.2. Wymagania dla poszczególnych typów systemów ochrony technicznej

Niniejsze wymagania dla różnych typów systemów ochrony technicznej nie są zróżnicowane w zależności od grupy ochrony, do której zostały zakwalifikowane i należy je stosować dla każdej z nich.

Ponadto poniższe wymagania należy stosować przy opracowywaniu specyfikacji warunków zamówienia (SWZ) w zakresie elektronicznego zabezpieczenia obiektów.

Opracowaną specyfikację warunków zamówienia należy przesłać do KZGW, celem jej zaopiniowania. W obiektach, w których zostały zainstalowane systemy ochrony technicznej należy wyznaczać administratorów tych systemów. Obowiązki administratora systemów ochrony technicznej przedstawiono w **załączniku nr 4**.

1. Wymagania środowiskowe

W zależności od miejsca instalowania elektronicznych urządzeń ochronnych (systemu alarmowego, systemu telewizji dozorowej, systemu kontroli dostępu) powinny one spełniać następujące wymagania klas środowiskowych:

- 1) urządzenia instalowane w pomieszczeniach zamkniętych ogrzewanych – klasy środowiskowej I według Normy PN-EN-50130:2012,
- 2) urządzenia instalowane w pomieszczeniach zamkniętych nieogrzewanych lub ogrzewanych z przerwami – klasy środowiskowej II według Normy PN-EN-50130:2012,
- 3) urządzenia instalowane na zewnątrz nie w pełni narażone na warunki pogodowe – klasy środowiskowej III według Normy PN-EN-50130:2012,
- 4) urządzenia instalowane na zewnątrz – klasy środowiskowej IV według Normy PN-EN-50130:2012.

2. Wymagania dla zasilania

Systemy ochrony technicznej powinny:

- 1) posiadać zasilanie podstawowe z jednej fazy prądu przemiennego 230V +10% -15%, 50 Hz $\pm 2\%$, z wydzielonego i nadzorowanego punktu zasilania z własnym zabezpieczeniem nadprądowym i przepięciowym, zlokalizowanym w obrębie obszaru chronionego,
- 2) mieć zasilanie awaryjne ze źródła rezerwowego, które zapewni normalną pracę systemu, w stanie normalnej pracy oraz w stanie alarmu trwającego 15 min, w czasie nie krótszym niż:
 - a) 36 h dla obiektów, w których istnieje ciągły dozór ludzki lub stan zasilania jest monitorowany przez uzbrojone stanowisko interwencyjne (USI) i dla których zagwarantowane są usługi serwisowe podejmowane w ciągu 4 godzin,
 - b) 72 h dla pozostałych obiektów, w tym bez ciągłego dozoru ludzkiego,
- 3) zapewniać samoczynne przełączanie zasilania ze źródła podstawowego na rezerwowe i odwrotnie bez zakłócania pracy systemu,
- 4) sygnalizować w centrum nadzoru (CN) lub USI awarię zasilania podstawowego i powrót zasilania podstawowego.

W przypadku funkcjonowania w obiekcie agregatów prądotwórczych uruchamiających się samoczynnie w czasie do 30 min przy awarii zasilania podstawowego i gwarantujących nieprzerwaną 36-godzinną pracę, jako źródło rezerwowe, należy stosować również akumulatorowe źródła zasilania rezerwowego podtrzymujące zasilanie przez okres co najmniej 2 h.

Zasilacze powinny sygnalizować spadek napięcia rezerwowego źródła zasilania poniżej wymaganego poziomu, przy którym systemy ochrony technicznej pracują poprawnie.

3.2.1. Wymagania dla systemów alarmowych

Instalowane systemy alarmowe powinny być wykonane w stopniu adekwatnym do oszacowanego ryzyka, jednak nie niższym niż w stopniu 2 według normy *PN-EN 50131-1 Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 1: Wymagania systemowe*. W obiektach grupy I zaleca się wykonanie systemu alarmowego w stopniu 3.

1. W strefie ochrony zewnętrznej należy stosować urządzenia lub systemy alarmowe naziemne, podziemne lub ogrodzeniowe. Przy wyborze urządzeń wchodzących w skład poszczególnych systemów należy zwracać uwagę na ich zasięgi dostosowane do wielkości ochraniających obiektów. Zaleca się aby zainstalowane urządzenia alarmowe współpracowały z systemami telewizji dozorowej jako weryfikacja powstałych zdarzeń alarmowych. Zamontowany w tej strefie system powinien wykrywać:

- 1) ruch w chronionej strefie,
- 2) sabotaż urządzeń systemu alarmowego,

oraz sygnalizować użycie ostrzegacza napadowego.

Ponadto urządzenia zewnętrzne powinny zapewniać:

- 1) jednolitą czułość detekcji w całym paśmie pracy, z możliwością regulacji ręcznej i automatycznej;
 - 2) automatyczną regulację parametrów pracy kompensującą niekorzystny wpływ warunków atmosferycznych;
 - 3) minimalny zasięg pracy czujek przy bardzo złych warunkach atmosferycznych (granicznych), nie mniejszy niż 60% (dla czujek podczerwieni) oraz 80 % (dla czujek mikrofalowych) ich maksymalnego zasięgu w warunkach normalnych;
 - 4) odporność na zmianę polaryzacji stałego napięcia zasilającego;
 - 5) odporność na zakłócenia impulsowe nanosekundowe i elektromagnetyczne o wartości do 2 kV;
 - 6) odporność na wyładowania elektryczności statycznej, w tym wyładowania atmosferyczne o wartości do 10kV;
 - 7) bezpośrednią cyfrową transmisję danych z kontrolą łączności pomiędzy urządzeniami i oprogramowaniem do wizualizacji;
 - 8) cyfrową obróbkę sygnału przy wykorzystaniu inteligentnego algorytmu analizy sygnału.
2. W strefie ochrony wewnętrznej należy stosować czujki alarmowe (podczerwieni, mikrofalowe, ultradźwiękowe, dualne, wibracyjne, stłuczenia szkła, magnetyczne stykowe), ostrzegacze napadowe, itp. Zamontowany w tej strefie system powinien wykrywać:
- 1) ruch w chronionej strefie,
 - 2) otwarcie drzwi, okien i innych zamknięć chronionej strefy,
 - 3) penetrację okien i innych zamknięć chronionej strefy bez jej otwierania,
 - 4) sabotaż urządzeń systemu alarmowego,

oraz sygnalizować użycie ostrzegacza napadowego.

W strefie ochrony zewnętrznej jak i wewnętrznej do sygnalizowania stanów alarmów w chronionych obiektach należy wykorzystywać sygnalizatory akustyczno-optyczne.

3. Parametry techniczno-użytkowe dla urządzeń stosowanych w systemach alarmowych:

- 1) odporność na zakłócenia impulsowe nanosekundowe i elektromagnetyczne o wartości do 2 kV,
- 2) właściwą pracę przy krótkotrwałych zanikach napięcia zasilania trwających nie dłużej niż 20 ms,
- 3) jednolitą czułość detekcji w całym zakresie pracy, z możliwością regulacji ręcznej i automatycznej poziomu czułości czujek,
- 4) odporność czujek na zakrycie ich pola detekcji (antymasking),
- 5) każde urządzenie alarmowe (czujka alarmowa, ostrzegacz alarmowy) powinno być włączone do wejścia centrali alarmowej rozróżnianego jako jedna linia alarmowa (za wyjątkiem czujek magnetycznych, które można grupować na jedną linię gdy chronią np. trzy skrzydła okien – na każdym skrzydle okna czujka),
- 6) nadzór nad wszystkimi sygnałami, informacjami o stanie systemów i urządzeń alarmowych w obiekcie sprawuje centrum nadzoru (CN).
- 7) centrale alarmowe oraz inne urządzenia decyzyjno-nadzorujące pracę systemu alarmowego powinny znajdować się w pomieszczeniach CN sił ochronnych, w których pełniona jest całodobowa praca, lub innych wydzielonych pomieszczeniach odpowiednio zabezpieczonych.
- 8) centrum nadzoru należy wyposażać w *Rejestr zdarzeń alarmowych*, który powinien być prowadzony przez obsługę CN. Wzór Rejestru przedstawiono w Tabeli 3 **załącznika nr 6**.
- 9) w przypadku monitorowania obiektu przez firmę zewnętrzną powyższy Rejestr powinna prowadzić obsługa uzbrojonego stanowiska interwencyjnego,
- 10) centrale alarmowe powinny umożliwiać obsłudze systemu otrzymanie bieżącej informacji o załączeniu poszczególnych stref ochrony przez użytkowników, stanie technicznym urządzeń, ich załączeniu lub wyłączeniu oraz stanie czuwania,
- 11) centrale alarmowe powinny posiadać możliwość archiwizowania wszystkich zdarzeń z co najmniej 30 dni,
- 12) w przypadku stosowania klawiatur służących do załączania, wyłączania ochrony poszczególnych stref ochrony, muszą one sygnalizować i rejestrować wyłączenie strefy kodem pod przymusem. Wprowadzenie kodu przymusu nie powinno powodować oznak alarmu w danej strefie, a jedynie zasygnalizować ten fakt w pomieszczeniu centrum nadzoru lub uzbrojonym stanowisku interwencyjnym,
- 13) czujki magnetyczne (kontaktrony) w przypadku instalowania ich na drzwiach oknach pomieszczeń należy je montować na każdym skrzydle okna czy drzwi. Przedstawione rozwiązanie nie wymaga włączania na oddzielną linię każdej czujki. Można je pogrupować jako oddzielna linia okno, drzwi,
- 14) ostrzegacze napadowe, w które wyposażamy siły ochronne obiektu powinny po przyciśnięciu alarmować centrum nadzoru w obiekcie lub uzbrojone stanowisko interwencyjne. Wykorzystanie ostrzegacza nie powinno powodować alarmu w miejscu jego użycia.

3.2.2. Wymagania dla systemów telewizji dozorowej

1. W strefie ochrony zewnętrznej należy integrować systemy telewizji dozorowej z systemami alarmowymi w celu natychmiastowej weryfikacji generowanych sygnałów alarmowych przez urządzenia alarmowe zainstalowane w tej strefie. Powyższa weryfikacja powinna się odbywać na zasadzie przełączenia obrazu z miejsca zdarzenia na monitor alarmowy z jednoczesnym rozpoczęciem rejestracji

zdarzenia z tzw. „prealarmem”. System powinien być skonfigurowany w taki sposób, aby odtworzył obraz obszaru, w którym wystąpił alarm poczynając od momentu 5 s przed jego powstaniem. Prędkość rejestracji powinna być nie mniejsza niż 6 klatek/s.

2. Systemy telewizji dozorowej należy również wykorzystywać do obserwacji chronionych obszarów obiektów lub pomieszczeń, stosując w nich głowice uchylno – obrotowe lub kamery obrotowe oraz obiektywy o zmiennej ogniskowej sterowane przez obsługę CN lub USI. Do tego celu należy wykorzystywać pulpity sterujące.
3. Systemy telewizji dozorowej mogą wykorzystywać wizyjną detekcję ruchu, której głównym zadaniem jest wykrywanie, sygnalizowanie i śledzenie określonych zmian w zdefiniowanych strefach chronionych znajdujących się w polu widzenia kamer.
4. Urządzenia rejestrujące obrazy z systemów telewizji dozorowej powinny umożliwiać odtwarzanie zdarzeń zaistniałych w tym systemie, z co najmniej 30 dni.
5. W systemach telewizji dozorowej wykorzystujących kamery telewizyjne z transmisją cyfrową można stosować kamery z transmisją analogową przy wykorzystaniu konwerterów przetwarzających sygnał analogowy na cyfrowy. Rozdzielczość konwertera nie powinna być mniejsza niż 720 x 576 pikseli.
6. W rejonach o zwiększonym natężeniu wyładowań atmosferycznych, urządzenia systemów telewizji dozorowej, montowane w strefach ochrony zewnętrznej powinny być wyposażone w ochronę przeciwprzepięciową, montowaną na kablach sygnałowych i zasilających. Urządzenia ochrony przeciwprzepięciowej należy stosować na początku i końcu linii kablowej. Stosowane urządzenia ochrony przeciwprzepięciowej powinny być oznaczone typ T1 zgodnie z normą PN-EN 61643-11:2013.
7. Części składowe systemów telewizji dozorowej, w tym kamery, oświetlacze, wysięgniki i maszty przeznaczone do instalowania w warunkach niekorzystnych występujących na zewnątrz obiektów lub pomieszczeń, takich jak: duże wahania temperaturowe, kurz, wilgoć, oblodzenia, silne opady deszczu i śniegu itp. powinny być zbudowane z materiałów niepodatnych na szkodliwe działanie tych warunków.
8. Zaleca się aby systemy telewizji dozorowej były odporne na działanie zakłóceń o wysokich poziomach pochodzących od innego sprzętu, urządzeń lub źródeł zewnętrznych takich jak: pole elektromagnetyczne, wyładowania elektryczności statycznej w tym na wyładowania atmosferyczne oraz stany przejściowe w zasilaniu. W tym celu można zabezpieczać tory sygnałowe i zasilające poprzez zastosowanie:
 - 1) ochronników przeciwprzepięciowych sygnałów wizyjnych,
 - 2) ochronników przeciwprzepięciowych sygnałów sieci teleinformatycznej,
 - 3) ograniczników przepięć,
 - 4) separatorów elektronicznych rozdzielających obwody o różnych potencjałach masy,
 - 5) listew zasilających przeciwprzepięciowych,
 - 6) innych elementów i urządzeń.

3.2.2.1. Wymagania dla wizyjnej detekcji ruchu

Systemy telewizji dozorowej z wizyjną detekcją ruchu powinny zapewniać:

- 1) wykrywanie osób (intruzów) w wyznaczonych strefach chronionych, w każdych warunkach atmosferycznych,
- 2) ciągłe śledzenie osób naruszających system podczas ich przebywania w strefie chronionej,
- 3) wywoływanie alarmu po naruszeniu przez intruza systemu, jeżeli wystąpią następujące przypadki:
 - a) poziom szarości intruza różni się od poziomu szarości tła,
 - b) intruz znajdzie się w granicach chronionej strefy,

- c) prędkość poruszania się intruza mieści się w granicach prędkości ustalonych przez administratora systemu,
 - d) wielkość intruza mieści się w granicach parametrów ustalonych przez administratora systemu,
 - e) droga przebyta przez intruza przed wywołaniem alarmu jest większa niż minimalne parametry określone dla niej przez administratora systemu,
 - f) zasłonięcie, rozogniskowanie oraz przestawienie kamery lub wystąpienie interferencji,
 - g) brak synchronizacji lub powstanie zniekształceń sygnałów wizyjnych,
 - h) ingerencja osób nieuprawnionych w urządzenia wideodetekcji.
- 4) natychmiastowe, automatyczne przełączenie na ekran monitora zobrazowania z kamery obserwującej strefę chronioną, w której nastąpiło naruszenie systemu,
 - 5) możliwość obserwacji obrazu jednocześnie ze wszystkich kamer, wyboru obrazu z określonej kamery, a także sekwencyjne przełączanie obrazu z poszczególnych kamer,
 - 6) możliwość wysyłania informacji o zdefiniowanych zdarzeniach alarmowych na odległość,
 - 7) możliwość przeglądania listy zdarzeń alarmowych,
 - 8) możliwość automatycznej zmiany parametrów systemu pod wpływem oświetlenia dzień/noc,
 - 9) możliwość natychmiastowego odtwarzania obrazów z kamery, której obrazy są aktualnie rejestrowane,
 - 10) możliwość wyboru stopnia kompresji i częstotliwości zapisu obrazów dla każdej kamery oddzielnie,
 - 11) możliwość analizy w czasie rzeczywistym obserwowanych stref chronionych i zaistniałych zdarzeń na ekranach monitorów,
 - 12) rejestrację i odtworzenie wszystkich zdarzeń wykrytych i zaistniałych w systemie z podaniem czasu, daty i typu alarmu na dysku twardym lub innym nośniku informacji,
 - 13) możliwość nagrywania zdarzeń poprzedzających wystąpienie alarmu,
 - 14) ciągłą rejestrację zdarzeń w czasie wyszukiwania i odtwarzania archiwalnych zapisów,
 - 15) możliwość automatycznego kasowania przedawnionych zapisów według ustalonych i ustawionych kryteriów,
 - 16) zapisywanie zarejestrowanych zdarzeń alarmowych i czynności obsługi systemu,
 - 17) brak możliwości kasowania zapisów zdarzeń i czynności obsługi systemu,
 - 18) brak możliwości zatrzymania pracy systemu przez obsługę systemu,
 - 19) systemową niezmienność zapisów i wykrywanie prób zmiany zawartości obrazów,
 - 20) ochronę przeciwprzepięciową,
 - 21) odporność na wyładowania elektryczności statycznej, w tym na wyładowania atmosferyczne,
 - 22) możliwość współpracy z innymi systemami i urządzeniami alarmowymi wykorzystywanymi w systemie ochrony,
 - 23) ciągłą analizę obecności i jakości sygnału wizyjnego,
 - 24) ciągłą pracę systemu przy przejściu z zasilania podstawowego na zasilanie awaryjne,
 - 25) programowanie każdej kamery osobno w zakresie różnych parametrów, takich jak:
 - a) kamera aktywna bądź pasywna (w obiektach nie wymagających stałej - ciągłej pracy, staje się kamera aktywną w określonych reżimach czasowych, po uruchomieniu przez operatora, automatycznym załączeniu w wyniku wykrycia ruchu w obiekcie),
 - b) minimalna powierzchnia intruza wyrażona w m²,

- c) maksymalna prędkość intruza wyrażona w m/s,
- d) obszar, w którym mają być wykrywane, rejestrowane i sygnalizowane powstałe zdarzenia alarmowe,
- e) czas bezruchu pomiędzy kolejnymi ruchami intruza.

3.2.2.2. Wymagania dla kamer telewizyjnych

1. Przy wyborze kamer do systemu telewizji dozorowej należy brać pod uwagę poziom oświetlenia, jakie będzie występowało w miejscu jej zainstalowania.
2. Kamery czarno-białe powinny mieć czułość nie mniejszą niż 0,02 lx przy F 1,4, a kamery kolorowe nie mniej niż 3 lx przy F 1,4.
3. Rozdzielczość kamer czarno-białych powinna być nie mniejsza niż 560 linii TV, a kamer kolorowych nie mniejsza niż 450 linii TV.
4. Kamery termowizyjne powinny posiadać rozdzielczość przetwornika nie mniejszą niż 320 x 240 pikseli.
5. W przypadku wykorzystania kamer telewizyjnych, w których sygnał wyjściowy transmitowany jest w postaci cyfrowej, rozdzielczość nie powinna być mniejsza niż 1280 x 720 pikseli.
6. Kamery telewizyjne instalowane wewnątrz lub na zewnątrz obiektu powinny mieć obudowy, które powinny chronić kamerę, obiektyw i wyposażenie pomocnicze przed uszkodzeniami mechanicznymi i środowiskowymi oraz dostępem do nich osób nieuprawnionych.
7. Kamera telewizyjna pracująca wewnątrz powinna spełniać wymagania klasy środowiskowej I lub II zgodnie z normą PN-EN 50130:2012.
8. Kamery telewizyjne pracujące na zewnątrz obiektów powinny spełniać wymagania klasy środowiskowej III lub IV oraz mieć obudowy z materiałów nierdzewnych lub zabezpieczonych przed korozją, hermetyczne, wyposażone w elementy grzewcze oraz osłony przeciwsłoneczne.
9. Obudowy kamer telewizyjnych powinny charakteryzować się:
 - 1) odpornością na uszkodzenia mechaniczne,
 - 2) możliwością łatwego dostępu do kamery dla konserwatorów i instalatorów, w celu przeprowadzenia napraw i konserwacji,
 - 3) odpornością na wzrost temperatury wewnątrz obudowy wskutek wydzielania się ciepła podczas pracy kamery i urządzeń pomocniczych;
 - 4) odpornością na przenikanie ciał stałych oraz szczelnością na wodę. Zaleca się stosowanie obudów IP 65 i IP 66, a w warunkach dużej wilgotności IP 67 lub IP 68.
10. Wymagana jest separacja masy sygnału wizji od uziemienia obudowy i lokalnego uziemienia ochronnego (z wyłączeniem sieciowych kamer IP).
11. Do przytwierdzania kamer telewizyjnych w obudowach do ścian i słupów należy stosować odpowiednie wysięgniki oraz wsporniki wraz z adapterami do montażu narożnego lub słupowego. Powinny one zapewniać stabilność mechaniczną i być dostosowane do podtrzymania maksymalnego ciężaru urządzeń oraz powinny zapewniać dostateczną sztywność dla zestawu kamerowego.

3.2.2.3. Wymagania dla oświetlaczy i oświetlenia sztucznego sceny

1. Systemy telewizji dozorowej, które są instalowane na zewnątrz obiektów lub pomieszczeń, należy wyposażać w oświetlacze, w celu podniesienia stopnia widzialności i rozpoznawania zaistniałych zdarzeń w strefie obserwowanej przez kamerę w trudnych warunkach oświetleniowych np.: nocnych. Powinny one zapewniać także równomierne oświetlenie obserwowanej strefy.

2. Oświetlacze mogą być instalowane pod kamerą bądź nad kamerą, a kierunek oświetlenia powinien być zgodny z kierunkiem patrzenia kamery, w celu uzyskania maksymalnego kontrastu dla potrzeb wykrycia intruza. W takim przypadku konieczne jest sprawdzenie, czy czułość widmowa stosowanych kamer jest dostosowana do długości fali danego źródła promieniowania.
4. Oświetlenie sztuczne strefy ochrony zewnętrznej (systemem latarni) i wewnętrznej (oświetlenie ciągów korytarzowych) powinno być podstawowym źródłem oświetlenia uwzględnionym przy zapewnieniu równomierności oświetlenia strefy, a oświetlacze powinny zapewnić prawidłowe funkcjonowanie systemu w przypadku awarii oświetlenia sztucznego.
5. W obiektach o dużych powierzchniach zaleca się stosowanie oświetlaczy dużej mocy instalowanych na kierunkach prawdopodobnego wystąpienia zagrożeń, w tym podejścia intruza, niekontrolowanego poruszania się po obiekcie osób nieupoważnionych.

3.2.2.4. Wymagania dla rejestratorów cyfrowych

1. Rejestratory cyfrowe powinny być wykorzystywane jako **podstawowe urządzenia pozwalające na budowę samodzielnego systemu telewizji dozorowej**. Powinny one być podstawowym elementem, w oparciu o który buduje się system telewizji dozorowej.
2. Minimalna szybkość rejestracji obrazów powinna być nie mniejsza niż 6 klatek na sekundę na każdą kamerę.
3. Standardowa rozdzielczość nagrywania powinna być nie mniejsza niż 720x576 pikseli przy zachowaniu minimalnej szybkości rejestracji obrazów.
4. Rejestratory cyfrowe powinny:
 - 1) rejestrować, w trybie ciągłym, wszystkie zdarzenia (ruch) zaistniałe w telewizyjnych systemach nadzoru z określeniem daty, czasu, numeru kamery, nazwy rejestratora,
 - 2) posiadać możliwość zabezpieczenia nagrania na dysku przed nadpisaniem,
 - 3) posiadać możliwość zapisania zdarzeń alarmowych na zewnętrznym nośniku rejestrującym (płyty CD, DVD, karty pamięci, dyski zewnętrzne),
 - 4) umożliwiać jednoczesne nagrywanie i odtwarzanie,
 - 5) posiadać definiowany wielopoziomowy dostęp dla obsługi,
 - 6) zapewniać zwiększenie liczby rejestrowanych klatek obrazu w ciągu sekundy z kamery, w której obrazie wystąpiło zdarzenie alarmowe,
 - 7) posiadać sygnalizację akustyczno-optyczną zdarzeń alarmowych i zaniku sygnału wizyjnego z kamery;
 - 8) posiadać wizyjną detekcję ruchu z możliwością ustawiania jej wstępnych parametrów;
 - 9) posiadać zabezpieczenie przed próbą zmiany zapisu, wykasowania bądź jego podmiany.

3.2.2.5. Wymagania dla krosownic wizyjnych

1. Krosownice wizyjne należy wykorzystywać w przypadku potrzeby przekazywania obrazów z wielu kamer do wielu punktów odbioru wizji.
2. Krosownice wizyjne powinny być stosowane, gdy:
 - 1) system posiada wielu użytkowników,
 - 2) system posiada dużą liczbę kamer i monitorów,
 - 3) wymagana jest integracja systemu telewizji dozorowej z innymi systemami,

- 4) wymagana jest całkowita niezależność i programowanie uprawnień obsługi dla każdego z użytkowników systemu.

3.2.2.6. Wymagania dla macierzy dyskowych

1. W systemach telewizji dozorowej należy stosować macierze dyskowe, w przypadku, gdy wymagana jest w nich bardzo duża pojemność zapisu. Powinny one umożliwiać zapis, przechowywanie i udostępnianie na bieżąco przetwarzanych treści obrazów z kamer telewizyjnych.
2. Macierz dyskowa powinna umożliwiać odtworzenie pełnej treści zapisanych obrazów w przypadku uszkodzenia jednego z dysków oraz sygnalizować jej awarię. Dodatkowo, macierz powinna posiadać możliwość rozbudowy poprzez dołączenie dysków twardych lub kolejnych macierzy. Obudowa powinna być zabezpieczona przed dostępem osób nieuprawnionych.

3.2.3. Wymagania dla systemów kontroli dostępu

1. System kontroli dostępu stanowi odrębny element systemu ochrony obiektu.
2. W systemie kontroli dostępu należy stosować jako podstawowe pasywne karty zbliżeniowe, czytniki kart zbliżeniowych.
3. Dopuszcza się wykorzystywanie innych czytników np. biometrycznych.
4. System kontroli dostępu powinien mieć punkt emisji kart dostępu składający się z:
 - 1) stanowiska do nadawania indywidualnego numeru identyfikacji użytkownika,
 - 2) stanowiska do personalizacji kart dostępu.
5. Zaleca się aby system kontroli dostępu umożliwiał kontrolowane wejście (wjazd) do i wyjście (wyjazd) z obszaru chronionego nadzorowanego osobom nieposiadającym imiennych elektronicznych kart dostępu za pomocą elektronicznych kart dostępu z napisem „INTERESANT” lub „GOŚĆ”.
6. System kontroli dostępu powinien uniemożliwiać:
 - 1) wejście osobom nieuprawnionym oraz wjazd pojazdów nieuprawnionych do obszaru chronionego obiektu nadzorowanego przez ten system,
 - 2) wejście powtórne do obszaru chronionego obiektu bez uprzedniego odnotowania wyjścia (tzw. antypassback).
7. System kontroli dostępu powinien umożliwiać:
 - 1) płynną i kontrolowaną przepustowość pracowników, interesantów oraz pojazdów,
 - 2) wejście do obszaru chronionego w przypadku awarii czytnika kart dostępu poprzez zwolnienie zamknięcia drzwi lub innego mechanicznego urządzenia blokującego przez operatora, po uprzednim sprawdzeniu danych personalnych osoby posiadającej stosowne uprawnienia,
 - 3) monitorowanie i identyfikację osób przebywających w obszarze chronionym obiektu,
 - 4) logowanie kart dostępu przez operatora w obiekcie,
 - 5) szybkie odblokowanie wszystkich przejść kontrolowanych przez system kontroli dostępu w razie pożaru, ewakuacji, alarmu lub sytuacji kryzysowej,
 - 6) lokalne odblokowanie przejść kontrolowanych w chwili awarii systemu,
 - 7) alarmowe blokowanie uprawnień karty dostępu lub ich zmianę,
 - 8) prowadzenie ewidencji osób, które są obsługiwane przez system,
 - 9) rejestrowanie i wydruk, w czasie rzeczywistym wszystkich zdarzeń zaistniałych w systemie z podaniem typu zdarzenia, daty i czasu jego zajścia z opóźnieniem nie dłuższym niż 60 s,

- 10) lokalizację ostatniego użycia karty dostępu przez podanie danych dotyczących czytnika, dnia i czasu jej użycia,
 - 11) możliwość identyfikacji osób w obszarze chronionym obiektem,
 - 12) wykonywanie przez operatora raportów wejścia (wjazdu) lub wyjścia (wyjazdu) z poszczególnych kontrolowanych przez ten system obszarów, rejonów, terenów, obiektów, pomieszczeń lub stref oraz kontroli liczby pracowników i interesantów przebywających w nich i czasie ich pobytu,
 - 13) poprawną pracę modułów systemu kontroli dostępu w przypadku chwilowego zaniku połączenia z komputerem,
 - 14) przydzielanie, blokowanie i zmianę poziomu dostępu przez obsługę dla użytkowników systemu kontroli dostępu,
 - 15) możliwość ustawienia terminu ważności dla karty, po którym wejście przy jej użyciu nie będzie możliwe i będzie rejestrowane w systemie jako sytuacja alarmowa.
8. System kontroli dostępu i jego elementy składowe powinny charakteryzować się:
- 1) odpornością na zakłócenia elektromagnetyczne,
 - 2) odpornością na wyładowania elektryczności statycznej, w tym na wyładowania atmosferyczne,
 - 3) możliwością przeprowadzenia kontroli sprawności systemu lub poszczególnych jego elementów i urządzeń przez administratora.
9. System kontroli dostępu powinien sygnalizować:
- 1) wykryte uszkodzenia w systemie w czasie nie dłuższym niż 5 s,
 - 2) sabotaż ze wskazaniem jego lokalizacji,
10. Nowoprojektowane SKD zaleca się integrować z systemem depozytorów kluczowych. Wymagania dla depozytorów kluczowych przedstawiono w **załączniku nr 5**.

3.2.3.1. Wymagania techniczno – użytkowe dla SKD

1. System kontroli dostępu powinien posiadać:
 - 1) wbudowany zegar czasu rzeczywistego o maksymalnym błędzie wskazania nie większym niż 5s na dobę oraz powinien być zsynchronizowany z zegarami z innych systemów alarmowych w obiekcie,
 - 2) pamięć pozwalającą na zarejestrowanie zdarzeń, z co najmniej 30 ostatnich dni,
 - 3) pojemność umożliwiającą zarejestrowanie danych personalnych wszystkich osób uprawnionych do wejścia lub wjazdu do chronionego obszaru, rejonu, terenu, obiektu lub pomieszczenia wraz z 20% rezerwą,
 - 4) możliwość automatycznego anulowania ważności kart dostępu po minięciu okresu ich ważności,
 - 5) możliwość rozbudowy systemu,
 - 6) zabezpieczenia antysabotażowe i przeciwprzebieciowe oraz uniemożliwiające nieuprawnionym osobom ingerencję w oprogramowanie,
 - 7) rozproszoną inteligencję, tzn. każdy z kontrolerów powinien posiadać własną bazę danych niezbędną do jego samodzielnego funkcjonowania w przypadku awarii łączy lub innych kontrolerów,
 - 8) możliwość logowania kartą oraz opcjonalnie kartą + kodem lub samym kodem,
 - 9) możliwość korzystania z niego równocześnie przez wielu użytkowników,
 - 10) w razie potrzeby można zainstalować tablicę synoptyczną na ekranie monitora z zaznaczeniem i sygnalizacją naruszenia przejść kontrolowanych.

3.2.3.2. Wymagania dla kart dostępu

1. W systemach kontroli dostępu obiektów należy stosować zbliżeniowe pasywne karty dostępu. Karty dostępu powinny być trwałe, czytane przez czytnik z odległości nie większej niż 10 cm oraz powinny uniemożliwiać zeskanowanie (odczyt) zapisanej w nich informacji. Czas reakcji urządzenia zezwalającego na wejście/wyjście po użyciu karty nie powinien przekraczać 3 s.
2. Karty dostępu, które są wykorzystywane w SKD powinny umożliwiać również otwarcie zainstalowanych w obiekcie depozytorów kluczowych.
3. Nie zaleca się stosowania kart dostępu z paskiem magnetycznym, kodem kreskowym i innych o podobnej zasadzie działania.

3.2.3.3. Wymagania dla czytników kart dostępu

1. W zależności od wymagań użytkownika można stosować czytniki wyposażone w zintegrowaną klawiaturę do wprowadzania kodu PIN.
2. Czytniki zewnętrzne powinny być odporne na trudne warunki atmosferyczne i akty wandalizmu.
3. Czytniki instalowane na metalowych elementach bramek, tripodów itp. powinny być w miarę możliwości wykonane w technologii nie powodującej zmniejszenia zasięgu ich działania ze względu na podłoże, na jakim zostały zainstalowane.
4. Maksymalna odległość czytników kart dostępu od kontrolera nie powinna być większa niż 150 m. Należy montować je na wejściu (wjeździe) i wyjściu (wyjeździe) z chronionego obszaru, rejonu, terenu lub pomieszczenia obiektu.
5. Powinny one być wyposażone w wizualny wskaźnik stanu, np.: dwukolorową diodę LED, oraz akustyczny wskaźnik zadziałania. Powinny być przystosowane do instalowania w strefie ochrony wewnętrznej i zewnętrznej obiektów.

3.2.3.4. Przepustowość

1. Przepustowość systemu kontroli dostępu powinna być dostosowana do liczby osób pracujących w danym obiekcie oraz osób posiadających uprawnienia do wejścia do pomieszczeń podlegających szczególnej ochronie.
2. Na przejściach kontrolowanych objętych kontrolą dostępu dla ruchu pieszego osobowego należy stosować mechaniczne urządzenia blokujące typu:
 - 1) drzwi,
 - 2) drzwi obrotowe,
 - 3) bramki obrotowe (tripody),
 - 4) furty,
 - 5) kołowroty.
3. Mechaniczne urządzenia blokujące powinny umożliwiać przejście tylko jednej osobie w określonym programowo czasie.
4. Na przejściach w ogrodzeniach obiektów przeznaczonych dla pojazdów mechanicznych należy stosować:
 - 1) łańcuchy,
 - 2) szlabany,
 - 3) szlabany z kolczatką,
 - 4) bramy,
 - 5) ruchome bariery zaporowe.

5. Szlabany i bramy zamykane automatycznie należy wyposażać w pomarańczowe światła ostrzegawcze i blokady uniemożliwiające zamknięcie ich w czasie trwania ruchu osobowego lub samochodowego.
6. Ruchome bariery zaporowe należy instalować za bramami wjazdowymi na terenie wewnętrznym obiektów w sposób uniemożliwiający ich ominięcie. Ponadto powinny być one wyposażone w optyczną sygnalizację stanu bariery (otwarcie, zamknięcie).

3.2.3.5. Wymagania dla drzwi

1. W systemie kontroli dostępu można stosować jedno lub dwu skrzydłowe drzwi drewniane, plastikowe, metalowe oraz specjalne:
 - 1) dźwiękoszczelne,
 - 2) przeciwwłamaniowe,
 - 3) przeciwpożarowe,
 - 4) inne otwierane w jedną lub dwie strony.
2. W razie potrzeby drzwi objęte SKD mogą być nadzorowane przez system telewizji dozorowej. Powinny one być wyposażone w samozamykacz z regulatorem szybkości zamykania, szybkości zatraskiwania i ogranicznikiem wychylenia oraz urządzenie nadzoru nad stanem drzwi (otwarcie i zamknięcie).

3.2.3.6. Wymagania dla bramek obrotowych (tripodów)

1. Bramki obrotowe należy montować w kontrolowanych, zadaszonych i oświetlonych wejściach/wyjściach do/z obszaru chronionego rozmieszczonych w ich ogrodzeniach zewnętrznych lub w korytarzach wewnątrz obiektów i budynków.
2. Bramki obrotowe powinny być tak skonstruowane, aby ramiona bramki obracając się, wymuszały przejście tylko jednej uprawnionej osoby. Ruch ramion bramki powinien być zainicjowany po przybliżeniu karty dostępu do czytnika zbliżeniowych kart dostępu oraz po wygenerowaniu i przesłaniu do bramki sygnału otwarcia przez system kontroli dostępu.
3. Bramki obrotowe powinny mieć możliwość automatycznego, otwarcia w razie zagrożeń (np. pożaru) i ewakuacji, mechanicznego złożenia ramion bramki lub swobodnego obrotu ramion po zaniku zasilania lub awarii bramki, a ponadto powinny mieć:
 - 1) mechanizm otwarcia działający w kierunku przechodzenia osób od strony czytnika kart zbliżeniowych,
 - 2) blokadę otwarcia bramki przez obsługę,
 - 3) przycisk wyjścia awaryjnego.

3.2.3.7. Wymagania dla obudów

1. Obudowy urządzeń składowych systemu kontroli dostępu powinny zabezpieczać elementy elektroniczne i elektryczne przed zabrudzeniem i chronić je wraz z przewodami sygnałowymi i zasilającymi przed mechanicznym uszkodzeniem.
2. Obudowy urządzeń instalowanych na zewnątrz i w nieogrzewanych pomieszczeniach powinny być hermetyczne i odporne na działanie skrajnych warunków klimatycznych typu: wilgoć, opady śniegu, deszczu, duże wahania temperatury i inne.

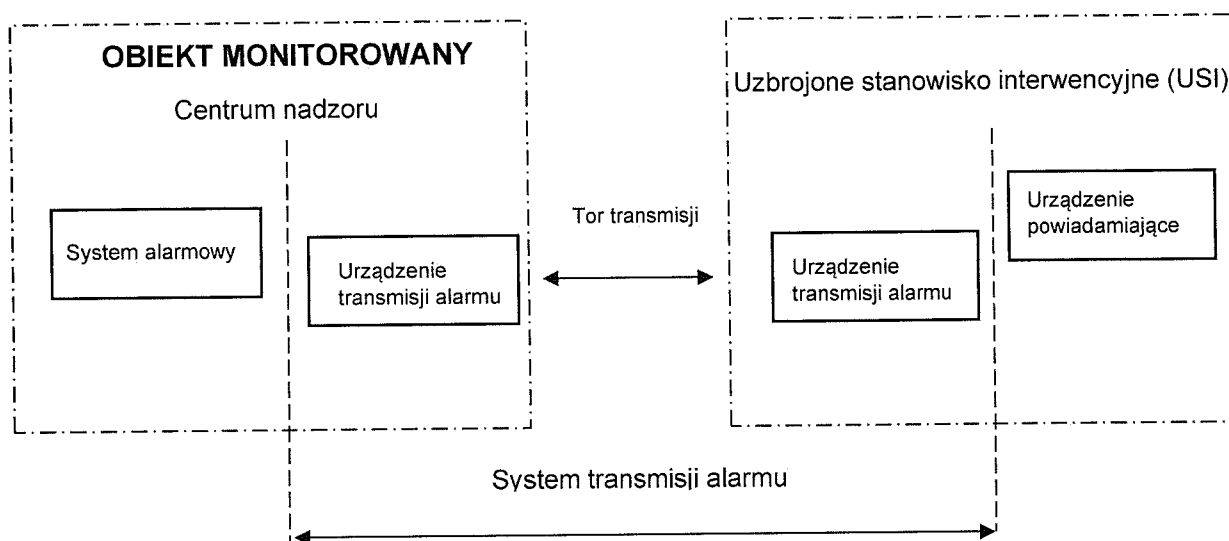
3.2.3.8. Sygnalizowanie stanów systemu kontroli dostępu

1. Sygnalizowanie stanów systemu kontroli dostępu powinno być realizowane w sposób optyczny i akustyczny na ekranie monitora lub tablicy synoptycznej.
2. System kontroli dostępu powinien być zaprojektowany i wykonany w sposób umożliwiający jego rozbudowę i modyfikację oraz powinien zapewniać natychmiastowe odblokowanie przez obsługę centrum nadzoru wszystkich kontrolowanych przejść w obiekcie na wypadek zagrożenia.
3. Powinien umożliwiać współpracę z wewnętrznym i zewnętrznym systemem alarmowym, urządzeniami systemem telewizji dozorowej oraz systemem sygnalizacji pożarowej itp.
4. W kontrolowanych przez czytniki drzwiach należy montować zamki sterowane elektrycznie, rygły elektryczne lub zwory elektromagnetyczne.
5. W systemie kontroli dostępu należy zapewnić środki uniemożliwiające nieuprawnione dokonanie zmian w oprogramowaniu systemu. Cel ten może być realizowany poprzez wykorzystanie więcej niż jednego kodu dostępu. Możliwość zmiany kodu dostępu powinna być w dyspozycji administratora systemu.

3.2.4. Wymagania dla systemów transmisji alarmów

Sygnał alarmowy z urządzeń wykrywających zmiany w systemie ochrony obiektu (zdarzenie alarmowe) kierowany jest do:

- a) centrum nadzoru (CN) - stosuje się w przypadku rozmieszczenia takiego centrum na terenie chronionego obiektu,
- b) uzbrojone stanowisko interwencyjne (USI) – stosuje się w przypadku gdy obiekt jest monitorowany ze stacji monitorowania alarmów przedsiębiorcy.



Rysunek 1 – System transmisji alarmu poza chroniony obiekt

3.2.4.1. Wymagania dla systemów transmisji sygnałów i komunikatów do CN

Zasadniczym torem transmisji sygnałów i komunikatów w systemie alarmowym są łącza kablowe. Stosuje się je w obrębie pojedynczego kompleksu, w którym zlokalizowane jest Centrum Nadzoru.

System transmisji alarmów powinien:

- 1) posiadać przynajmniej jeden kablowy tor transmisji sygnałów do CN;
- 2) zapewniać transmisję i monitorowanie sygnałów potwierdzających sprawność monitorowanych systemów alarmowych i wykorzystywanych torów transmisji, w okresach nie większych niż 180 s,
- 3) zapewnić czas transmisji sygnału alarmowego i innych przekazywanych do CN danych i komunikatów nie dłuższy niż 20 s,
- 4) wskazywać szczegółowo występujące alarmy i komunikaty w stosunku do pojedynczych pomieszczeń podlegających ochronie w obiekcie;
- 5) wykrywać i przekazywać następujące sygnały z monitorowanego systemu:
 - a) włamania,
 - b) napadu,
 - c) sabotażu,
 - d) usterki technicznej,
 - e) awarii zasilania,
 - f) innych sygnałów wynikających z funkcjonalności systemu,
 - g) wykrywać próby manipulacji przy torach transmisji, ich modyfikacji lub próby zamiany urządzeń,
- 6) posiadać zabezpieczone przed włamaniem, sabotażem, podmianą urządzenia nadawcze oraz inne ważne urządzenia z punktu widzenia transmisji sygnałów i komunikatów;
- 7) posiadać zabezpieczenie przed nieautoryzowanym kopiowaniem danych;
- 8) posiadać możliwość archiwizacji wszystkich sygnałów i komunikatów z okresu minimum 30 dni.

3.2.4.2. Wymagania dla systemów transmisji sygnałów i komunikatów do USI

Systemy transmisji sygnałów i komunikatów kierowanych do uzbrojonego stanowiska interwencyjnego powinny:

- 1) posiadać co najmniej jeden tor transmisji sygnałów do uzbrojonego stanowiska interwencyjnego;
- 2) zapewniać transmisję i monitorowanie sygnałów potwierdzających sprawność monitorowanych systemów alarmowych i wykorzystywanych torów transmisji, w okresach nie większych niż 180 s,
- 3) posiadać czas transmisji sygnału alarmowego nie dłuższy niż 20 s;
- 4) wskazywać szczegółowo występujące alarmy i komunikaty w stosunku do pojedynczych pomieszczeń podlegających ochronie w obiekcie;
- 5) wykrywać i przekazywać następujące sygnały z monitorowanego systemu:
 - a) włamania,
 - b) napadu,
 - c) sabotażu,
 - d) usterki technicznej,
 - e) awarii zasilania,
 - f) innych sygnałów wynikających z funkcjonalności systemu,
 - g) wykrywać próby manipulacji przy torach transmisji, ich modyfikacji lub próby zamiany urządzeń,