DOKUMENTACJA WYKONAWCZA

TEMAT	**DOKUMENTACJA WYKONAWCZA.** **INSTALACJA SYSTEMU SYGNALIZACJI**
OPRACOWANIA:	**WŁAMANIA I NAPADU, INSTALACJA KONTROLI DOSTĘPU**
INWESTOR:	**KOMENDA WOJEWÓDZKA POLICJI W SZCZECINIE** **UL. MAŁOPOLSKA 47**
PROJEKT:	**ELTECH INSTALACJE PROJEKTOWANIE** **ANDRZEJ PILECKI** **70-781 SZCZECIN** **BRĄZOWA 79/3** **UPR. SA1- SA4 PISA NR 442/P/2005**
OBIEKT:	**KOMENDA POLICJI SZCZECIN DĄBIE** **UL. POMORSKA 15**

Dokumentacja	*Imię i nazwisko*	*Podpis*
Opracował:	*Andrzej Pilecki*	
Kreślił:	*Andrzej Pilecki*	

SZCZECIN – Wrzesień 2009 r.

SPIS TREŚCI:

1. Dane ogólne

1.1 Podstawa prawna opracowania projektu:

Zlecenie

1.2 Podstawa techniczna opracowania projektu:

* *koncepcja ochrony technicznej*
* *podkłady architektoniczne*
* *uzgodnienia ze zleceniodawcą*

1.3 Wytyczne do projektowania:

- *Warunki techniczne wykonania i odbioru robót budowlano - montażowych cz. V Instalacje elektryczne*
- *Zasady projektowania elektronicznych systemów alarmowych włamaniowych i napadowych - skrypt TECHOM 1992*
- *Karty katalogowe urządzeń*
- *PN-93E-08390/14 „Systemy alarmowe"*
- *Ustawa z dn.3.04.93r o badaniach i certyfikacji Dz. U. nr 55 poz. 250*
- *Ustawa z dn.3.04.93r o normalizacji Dz. U. nr 55 poz. 251*
- *Rozporządzenie ministra Spraw Wewnętrznych z dn. 28.03.94r w sprawie wprowadzenia obowiązku stosowania Polskich Norm i norm branżowych Dz. U. nr 44 poz. 174*
- *Rozporządzenie ministra Przemysłu z dn. 08.10.90r w sprawie warunków technicznych, jakim powinny odpowiadać urządzenia elektroenergetyczne Dz. U. nr 44 poz. 174*
- *Rozporządzenie ministra Spraw Wewnętrznych z dn. 15.09.93r zmieniające rozporządzenie w sprawie wyłączenia niektórych rodzajów działalności gospodarczej z obowiązku uzyskiwania koncesji Dz. U. nr 88 poz. 406*
- *Projekt normy PN-EN 50132-7, „Systemy alarmowe. Systemy dozorowe CCTV w zastosowaniach dotyczących zabezpieczania".*
- *Przewodnik rzeczoznawcy, zeszyty 1-8, 1994r,*
- *Karty katalogowe*

1.4 Przedmiot i zakres projektu

Zakres rzeczowy projektu obejmuje:

1. *Przyjęte rozwiązania techniczne z uwzględnieniem specyficznych cech obiektu*
2. *Koncepcja ochrony obiektu*
3. *Dobór urządzeń*
4. *Rysunki z rozmieszczeniem poszczególnych elementów systemu*

2. Opis rozwiązań technicznych:

2.1 Zakres i sposób ochrony obiektu

2.1.1 Opis obiektu:

Obiekt Komendy Policji Szczecin Dąbie przy ulicy Pomorskiej jest kompleksem budynków pełniących funkcje administracyjne oraz penitencjarne wraz z niezbędną infrastrukturą (garaże, magazyny, parkingi). Budynek główny posiada cztery kondygnacje.

2.1.2 Zakres ochrony

Ochrona obiektu powinna spełniać dwa warunki, po pierwsze zapewnić bezpieczeństwo obiektu oraz możliwie wczesne wykrycie intruza po godzinach pracy (w nocy), po drugie maksymalnie zneutralizować okoliczności sprzyjające powstawaniu przestępstw w godzinach pracy (w dzień).

Celem oceny niebezpieczeństwa jest:

- *analiza i uświadomienie istniejących zagrożeń dla wszystkich funkcji rozpatrywanego obiektu, (analiza funkcji jakie obiekt realizuje w powiązaniu z rodzajami dóbr podlegających ochronie karnoprawnej oraz poszczególnymi rodzajami przestępstw),*
- *znalezienie czynników sprzyjających powstawaniu w/w zagrożeń,*
- *unormowania prawne,*
- *procesy techniczne świadczenia usług,*
- *stwarzanie warunków prawidłowego funkcjonowania obiektu,*
- *procesy organizacji, zarządzania ludźmi i czynnikami materialnymi,*
- *rozwiązania budowlane, infrastruktura techniczna,*
- *zabezpieczenia mechaniczne,*
- *zabezpieczenia elektroniczne,*
- *ochrona fizyczna*
- *wskazanie środków neutralizacji zagrożeń,*
- *analiza kosztów wdrożenia proponowanych rozwiązań.*

Dyskusja nad bezpieczeństwem rozważanego obiektu, z uwagi na bardzo szeroki wachlarz zagadnień z tym związanych, może się skupić jedynie na:

- *bezpieczeństwie pracowników przebywających w strefie strzeżonej obiektu,*
- *bezpieczeństwie przechowywanej broni i amunicji*
- *bezpieczeństwie przechowywanych i gromadzonych danych komputerowych,*
- *bezpieczeństwie gromadzonych dokumentów archiwalnych,*
- *bezpieczeństwa wyposażenia obiektu (głównie sprzęt komputerowy).*

Zagrożenia z punktu widzenia osoby sprawcy należy rozważać w wielu kategoriach, chociaż z uwagi na zawężenie kryteriów bezpieczeństwa podmiotowego, analiza zagrożeń

przedmiotowych wyszczególnień niżej musi siłą rzeczy też zostać ograniczona. Lista możliwych do rozważania kryteriów jest bardzo długa:

- *siła wyższa: awarie zasilania elektrycznego, awaria zasilania gazowego, awaria wodociągu, katastrofy wywołane siłami natury, zamieszki uliczne*
- *intruz: usiłowanie zabójstwa, uszkodzenie ciała, kradzież mienia ruchomego, kradzież z włamaniem, kradzież rozbójnicza, kradzież zuchwała, rabunek, wymuszenie rozbójnicze, podpalenie, niszczenie mienia,*
- *pracownik: nieumyślne spowodowanie śmierci, spowodowanie niebezpieczeństwa pożaru lub kradzieży, łapownictwo, zabór mienia, nadużycie uprawnień, przestępstwa komputerowe, naruszenie tajemnicy służbowej i państwowej,*
- *interesant: przekupstwo, wyłudzenia mienia, fałszerstwo dokumentów, oszustwo.*

Ponieważ szczegółowe rozważania prowadzące do gotowych rozwiązań techniczno – organizacyjnych stanowią bardzo szerokie zagadnienia wykraczające znacznie poza ramy niniejszego opracowania problem badania zagrożeń musi być mocno zawężony. Analiza zwraca uwagę na tylko niektóre, najważniejsze kryteria, których przewidywane i możliwe w danym momencie do zastosowania środki neutralizacji odniosą największy skutek.

Koncepcja ochrony:

a) Pomieszczenia w budynku chroni system składający się z czujników :
   - *magnetycznych zamontowanych na drzwiach skrzydłowych i oknach*
   - *czujników przestrzennych ruchu dozorujących pomieszczenie magazynu broni oraz serwerowni.*

b) Centralę włamaniową projektuje się umieścić w pomieszczeniu oficera dyżurnego na parterze.
c) Manipulatory do obsługi systemu będą zamontowane w pomieszczeniu oficera dyżurnego, przy magazynie broni oraz przy serwerowni.
d) Manipulatory będą pełnić funkcję lokalnej sygnalizacji włamania.
e) Kontrola dostępu ograniczająca dostęp do pomieszczeń tylko dla uprawnionych osób.
f) Nadzór nad systemem KD poprzez dedykowany komputer z odpowiednim oprogramowaniem, umożliwiającym bieżącą obserwację ruchu osobowego na obiekcie oraz nadawanie odpowiednich uprawnień dla użytkowników.
g) Sygnalizacja naruszenia dostępu lokalnie przy przejściach oraz u oficera dyżurnego.
h) Możliwość blokowania dostępu w przypadku strefy podlegającej dozorowi systemu SSWiN oraz KD (brak dostępu w przypadku uzbrojenia strefy).
i) ochrona przeciwpożarowa pomieszczeń (oddzielne opracowanie)
j) system telewizji dozorowej (oddzielne opracowanie)

2.1.3 Centrala INTEGRA 128

*System sygnalizacji włamania i napadu oparty został centrali **Integra 128** produkcji firmy SATEL, która wykorzystuje najnowsze osiągnięcia techniki mikroprocesorowej. Niezawodność i pewność działania tego urządzenia jest równa najnowocześniejszym systemom mikrokomputerowym. System oparty na centrali Integra 128 jest to system procesorowy z oprogramowaniem w pamięci FLASH, umożliwiający unowocześnienie*

programowania centrali i rozbudowę o nowe funkcje. Nowa wersja oprogramowania wpisywana jest przez port RS-232 centrali. Możliwość zachowania parametrów programowanych przez serwis w pamięci FLASH, dzięki czemu nawet po odłączeniu akumulatorka podtrzymującego pamięć ustawień, centrala wraca do ustawień zaprogramowanych przez serwis. Możliwość dzielenia systemu na 8 partycji i 32 strefy (strefa = grupa wejść). Strefy mogą być sterowane przez użytkownika, przez timery, przez wejścia sterujące lub ich stan może zależeć od stanu innych stref. Możliwe jest czasowe ograniczanie dostępu do stref. Możliwość rozbudowy poprzez dodanie modułów rozszerzających. Możliwość zapamiętania w systemie 240 haseł, które mogą być przeznaczone dla użytkowników lub też można przypisać im funkcje sterujące. Rozbudowane funkcje jednoczesnego sterowania systemem poprzez manipulatory LCD i podłączone do nich komputery użytkowników. Dodatkowo serwis ma możliwość sterowania centralą przez port RS-232 lub przez łącze telefoniczne. Możliwe jest też sterowanie pojedynczymi strefami poprzez przydzielone do nich klawiatury strefowe. Możliwość definiowania nazw użytkowników i większości elementów systemu (stref, wejść, wyjść, modułów), dzięki którym ułatwione jest sterowanie i kontrola systemu oraz przeglądanie pamięci zdarzeń. Rozbudowana funkcja bieżącego wydruku zdarzeń, umożliwiająca selekcję zdarzeń. Opisy zdarzeń są zgodne z listą zdarzeń formatu Ademco Contact ID, przez co wydruk z centrali jest zbieżny z wydrukiem ze stacji monitorującej. Oprócz tego nazwy wejść, modułów i użytkowników drukowane są tak, jak je zdefiniowano w systemie Możliwe sterowanie w oparciu o czas, dzięki 64 timerom uwzględniającym tygodniowy rytm pracy oraz definiowane okresy wyjątków. Dodatkowo każda strefa ma swój timer (dzienny lub tygodniowy), programowany przez administratora, zapewniający automatyczne uzbrajanie i rozbrajanie. Ułatwione realizowanie niestandardowych funkcji sterowania dzięki możliwość realizowania złożonych operacji logicznych na wyjściach Pojemna pamięć zdarzeń (22000), w której oprócz zdarzeń monitorowanych zapamiętywane są też: dostęp użytkownika, użyte funkcje i inne. Magistrale komunikacyjne umożliwiające dołączanie modułów zwiększają możliwości sprzętowe - pozwalają rozbudować system o nowe elementy, które zostaną opracowane w przyszłości. Centrala posiada atest w ZRTOM TECHOM w klasie S, oraz Świadectwo homologacji Ministerstwa Łączności.
Płyta główna jednostki centralnej posiada:

- *16 wejść indywidualnie oprogramowanych, obsługujących konfigurację NO,NC,EOL,2EOL/NO i 2EOL/NC z kontrolą poprawności działania każdego czujnika.*
- *16 wyjść o programowanym sposobie działania z możliwością wybrania jednej z kilkudziesięciu funkcji (w tym: 4 wyjścia wysokoprądowe z bezpiecznikami elektronicznymi, 2 wyjścia realizują „funkcje zasilające")*
- *12 wyjść niskoprądowych przystosowanych do sterowania przekaźnikami*
- *2 złącza do podłączenia syntezerów mowy*
- *magistrala komunikacyjna a do podłączenia manipulatorów LCD, do której można podłączyć 8 manipulatorów kodu i tablicę synoptyczną*
- *2 magistrale do modułów dodatkowych (ekspanderów), dzięki którym można centralę rozbudować do 64 wejść i 64 wyjść*
- *komunikator telefoniczny wyposażony w układ detekcji DTMF, umożliwiający odbieranie poleceń przez telefon, realizujący funkcje monitoringu*
- *Zasilacz impulsowy o wydajności 3A, wyposażony w układ kontroli stanu akumulatora i odłączenie akumulatora rozładowanego*
- *niezależny, podtrzymywany własnym akumulatorkiem zegar czasu rzeczywistego i komunikatora telefonicznego*
- *zabezpieczenie wszystkich wejść, wyjść i magistral komunikacyjnych*

Manipulator INT KLCD R

- *wyświetlacz LCD*
  - 2x16 znaków
  - odczyt pamięci zdarzeń
  - stan wejść centrali
  - stan stref
  - zegar systemu i data
  - notatki z serwisu
  - notatki serwisowe to wygodny sposób przypomnienia użytkownikowi m.in. o okresowej konserwacji systemu

- *podświetlenie klawiatury i wyświetlacza*
  - stałe
  - czasowe po naciśnięciu klawisza
  - uaktywniane dowolnym wejściem centrali lub czasem na wejście

- *alarmy NAPAD, POŻAR, POMOC wywoływane z klawiatury*

- *6 diod LED*
  - stan stref - ALARM, czas na wejście lub wyjście
  - stan systemu - AWARIA

- *sygnalizacja dźwiękowa*
  - alarm
  - awaria
  - czas na wejście
  - czas na wyjście
  - czas autouzbrojenia
  - naruszenie wejść (gong)
  - potwierdzenie operacji klawiatury

- *2 wejścia*
  - obsługa konfiguracji NO, NC, EOL, 2EOL/NO i EOL/NC
  - kilkadziesiąt rodzajów reakcji
  - wykrywanie awarii czujki
  - wykrywanie zamaskowania czujki

- *mikroprzełącznik wykrywający sabotaż manipulatora*

- *sygnalizacja utraty łączności z centralą*

- *łącze RS-232 do współpracy z GUARDX*
  - pełna kontrola stanu systemu
  - manipulator wirtualny w komputerze
  - ułatwione zarządzanie użytkownikami

Czujka dualna PIR+MV

tor PIR i mikrofalowy
poczwórny pyrolelement
funkcja antymaskingu realizowana przez tor mikrofalowy
cyfrowy algorytm detekcji
wymienne soczewki Fresnela

DANE TECHNICZNE:

Pyroelement poczwórny
Mikrofala 10,525 GHz
Antymasking tak
Soczewka EWA
Cyfrowa kompensacja temperatury tak
Regulacja czułości toru podczerwieni zworkami
Regulacja czułości toru mikrofalowego płynna
Autodiagnostyka podstawowa
Znamionowe napięcie zasilania (±15%) 12 V DC
Średni pobór prądu (±10%) 24 mA
Wymiary obudowy (mm) 63 x 136 x 49
Regulowany uchwyt do montażu tak
Klasa środowiskowa II
Zakres temperatur pracy -10°C…+55°C

Czujki kontaktronowe DC108 i MC470

Czujki kontaktronowe stosowane do ochrony drzwi i okien posiadają zabezpieczenie przed przyłożeniem zewnętrznego pola magnetycznego.
Przełącznik kontaktronowy typu A, styki normalnie zamknięte (NC)
Obciążenie: max. 200 V DC/szczytowo AC/500 mA/10 VA
Odległość zamknięcia - 20 mm
Standardowe długości kabla: 2 i 5 m
4-żyłowy biały kabel, atest VdS
Materiał magnesu: Alnico 5
Pętla sabotażowa
Zatwierdzony przez Techom, VdS, ANPI/NVBB i inne europejskie biura certyfikacyjne
Plastikowa obudowa ABS
Przełącznik kontaktronowy typu A, styki normalnie zamknięte
Odległość: stal – 13/0 mm, 25/2 mm
Obciążenie: max. 200 V DC/szczytowo AC/500 mA/10 VA
6 przyłączy na śruby z zabezpieczeniem przewodów
Przełącznik antysabotażowy
Wyposażony w podkładki dystansowe i wkręty
Biały lub brązowy plastik
Zatwierdzony przez Techom, ANPI/NVBB i inne europejskie biura certyfikacyjne

CENTRALA KD CPR 32 ROGER SYSTEM RACS 4

RACS 4 to sieciowy system kontroli dostępu oparty o kontrolery dostępu serii PR, czytniki serii PRT, moduły rozszerzeń XM-2/XM-8, kontrolery sieciowe (centrale) CPR oraz oprogramowanie zarządzające PR Master. Funkcjonalność systemu zależy od rodzaju sprzętu użytego w danej instalacji. System RACS może zostać podzielony na osobne gałęzie zwane podsystemami kontroli dostępu, przy czym w obrębie jednego systemu KD można zintegrować do dwustu pięćdziesięciu podsystemów. W każdym podsystemie może funkcjonować do 32 kontrolerów dostępu połączonych za pomocą magistrali komunikacyjnej RS485 o maksymalnej długości 1200m. Program PR Master wymienia dane z podsystemami za pośrednictwem portów szeregowych (COM lub USB) lub poprzez sieć komputerową (WAN/LAN). System RACS 4 jest dedykowany do małych oraz średnich instalacji kontroli dostępu i może obsługiwać do 1000 kontrolerów oraz do 4000 użytkowników (kontrolery serii PRxx2) lub do 1000 użytkowników (kontrolery serii PRxx1).

Centrala CPR32-SE jest opcjonalnym elementem systemu kontroli dostępu RACS. Zastosowanie centrali w systemie rozszerza jego funkcjonalność o pewne dodatkowe cechy. W odniesieniu do kontrolerów serii PRxx1 zastosowanie centrali umożliwia

rejestrację zdarzeń oraz definiowanie czasowych praw dostępu. W przypadku kontrolerów serii PRxx2 centrala CPR32-SE umożliwia wykorzystanie funkcji globalnego anti-passback oraz grupowanie kontrolerów w tzw. Strefy Alarmowe.
Możliwość podłączenia do 32 kontrolerów serii PR w ramach jednej sieci (podsystemu)
Wyjście przekaźnikowe dla celów sygnalizacji stanów alarmowych
Zegar czasu rzeczywistego z podtrzymaniem bateryjnym Możliwość aktualizacji oprogramowania firmowego (fleszowanie)
Nieulotny bufor 250.000 zdarzeń Zasilacz buforowy o wydajności 1.5A
Programowalne linie wejściowe i wyjściowe Zasilanie 18-22 VAC
Interfejs komunikacyjny RS485 (dowolna topologia)

Kontroler PR 302.

Zewnętrzny kontroler dostępu, wbudowany czytnik zbliżeniowy EM 125 kHz, , Obustronna kontrola jednego przejścia (wejście/wyjście). Rejestracja zdarzeń dla celów RCP.
Praca w trybie autonomicznym lub w zintegrowanym systemie sieciowym Wbudowany czytnik zbliżeniowy EM 125 kHz
1000 użytkowników Możliwość dołączenia dodatkowego czytnika serii PRT (kontrola wejścia/wyjścia)
250 grup dostępuProgramowalne linie wejściowe i wyjściowe
32 harmonogramy czasowe Wbudowane wyjście przekaźnikowe
128 stref czasowych w obrębie jednego harmonogramu
Interfejs komunikacyjny RS485 (dowolna topologia)
Harmonogramy świąteczne
Oprogramowanie zarządzające (Windows XP/Vista)
Automatyczna zmiana czasu lato-zima

Wyłącznik awaryjny.

Przy każdym przejściu objętym kontrolą dostępu zainstalować przycisk awaryjny wyjścia (zielony, typu zbij szybkę). Otwarcie drzwi nastąpi również w przypadku alarmu pożarowego drugiego stopnia. Zasilanie elektrozaczepów i zwór elektromagnetycznych należy podłączyć do styków normalnie zwartych modułów EKS4001.

Okablowanie.

Zasilanie centralki i zasilaczy włączyć do lokalnych rozdzielnic na kondygnacjach, zabezpieczyć szybkim bezpiecznikiem nadprądowym B6.
Przewody magistralne wykonać kablem UTP kat5e.

2.1.4 Ochrona antysabotażowa urządzeń

Wszystkie urządzenia systemu wykrywania włamania i napadu wyposażone są w elementy chroniące je przed nieautoryzowanym dostępem. Centrala alarmowa reaguje

na każde naruszenie ochrony antysabotażowej poprzez zgłoszenie odpowiedniego komunikatu na odpowiednich manipulatorach.

Zastosowane elementy antysabotażowe:

- *czujki dualne mają wbudowane elementy chroniące przed mechanicznym otwarciem i oderwaniem od podłoża,*
- *centrala alarmowa i manipulatory - wbudowane czujniki krańcowe działające na otwarcie i oderwanie od podłoża, sabotaż ilości wprowadzonych błędnych kodów,*
- *czujki magnetyczne – posiadają budowę reagującą na każdą próbę przyłożenia obcego, zewnętrznego pola magnetycznego, podłączenie np. kilku kontaktronów do jednego przewodu należy wykonać poprzez puszkę łączeniową ze stykiem antysabotażowym.*

2.2 Zasilanie systemu

Zasilanie płyty głównej centrali odbywa się z dwóch źródeł:

- zasilanie podstawowe 230 V A.C.

- zasilanie awaryjne 12 V DC z akumulatora bezobsługowego 12 V o pojemności 18 Ah.

Zasilanie ekspanderów i klawiatur należy wyprowadzić z zewnętrznego zasilacza 12V/65Ah i włączyć w przewody magistralne. Minus zasilacza połączyć z minusem zasilania płyty głównej Integraf 128.

Zasilanie podstawowe SSWiN należy doprowadzić z wydzielonego obwodu 230V AC,

zabezpieczenie typu B6 należy oznaczyć i opisać w rozdzielnicy elektrycznej.

Analogicznie doprowadzić zasilanie podstawowe do centrali KD ROGER.

3. Zbiorcze zestawienie urządzeń

lp	SSWiN	Typ	Ilość
1	Centrala SSWiN z obudową	SATEL Integra	1
2	Klawiatura	INT KLCD R	7
3	Ekspander wejść w obudowie	CA 64 E	11
4	Sygnalizator akustyczny	Satel	5
5	Czujka PIR		20
6	Czujka dualna	RK410	1
7	Akumulator 18 Ah	EUROPOWER	1
8	Czujka kontaktronowa MC 370	ALARMTECH	50
	Czujka kontaktronowa MC 470		13
9	Zasilacz buforowy 65 Ah		1
10	Akumulator 65Ah		1

lp	KD	Typ	Ilość
1	Centrala KD z obudową	ROGER CPR32	1
2	Kontroler	PR302	15
3	Zasilacz buforowy	AWZ 300	4
4	Interfejs komunikacyjny	UT4 ROGER	1
5	Akumulator 18 Ah	EUROPOWER	4
6	Kontaktron	SATEL S4	
7	Elektrozaczep rewersyjny		9
8	Szyld elektrozaczepu		
9	Przycisk awaryjny otwarcia	D 110	7
10	Przycisk otwarcia		3
11	Komputer z systemem Windows XP PRO i oprogramowaniem Inpro BMS		1

4. Sposób prowadzenia instalacji wnętrzowej.

Instalację prowadzić natynkowo w korytach instalacyjnych. Do czujek doprowadzić przewody typu YTKSY 3x2x0.5, magistrale do manipulatorów i ekspanderów wykonać przewodem UTP kat 5e, zasilanie centrali Integra oraz Roger wykonać przewodem YDY 3x2.5.

Docelowy montaż urządzeń należy uzgodnić z inwestorem po uwzględnieniu wyposażenia pomieszczeń.

Sposób prowadzenia instalacji powinien uwzględniać dalszą rozbudowę systemu (podłączenie do centrali SSWiN oraz KD magistral z innych budynków).

Dopuszcza się zastosowanie innych urządzeń niż wymienione o równoważnych parametrach i posiadających odpowiednie certyfikaty.

5. Uwagi dla inwestora (użytkownika) systemu antywłamaniowego.

- *Po zainstalowaniu całego wyposażenia wnętrz lub przy zmianie w wykorzystaniu przestrzeni należy przeprowadzić weryfikacje projektu, pod względem sprawności dozorowania obiektu.*
- *Wykonawstwo i konserwację projektowanego systemu należy zlecić wyspecjalizowanej firmie, która posiada odpowiednio przeszkolonych pracowników.*
- *Użytkownik systemu jest odpowiedzialny za prowadzenie zeszytu kontrolnego (dziennika operacyjnego), w którym należy zamieszczać wszystkie uwagi dotyczące pracy systemu :*

- regularne kontrole instalacji i urządzeń
- dokonywane naprawy, zmiany i uzupełnienia w instalacji
- wszystkie alarmy : rzeczywiste, pozorowane, fałszywe i uszkodzenia (w przypadku centralki z drukarką wystarczy taśma z wydrukiem)

- *Osoby, którym powierzono stałą obsługę centrali sygnalizacji włamania powinny być przeszkolone w zakresie niezbędnych czynności, które należy wykonać w przypadku pojawienia się jakiegokolwiek alarmu.*
- *Podczas prowadzenia prac (instalacyjno-montażowych) systemu należy zapewnić:*

- nadzór autorski
- nadzór inwestorski (wskazany jest inspektor posiadający wiedzę w zakresie ochrony antywłamaniowej)

- *Odbiór instalacji powinien odbywać się po wykonaniu całego systemu zgodnie z opracowaną dokumentacją techniczną i ewentualnymi zmianami wpisanymi do dziennika budowy.*
- *Odbiór instalacji powinien być połączony z przekazaniem instalacji do eksploatacji; w odbiorze powinien brać udział konserwator systemu, który sprawował będzie nadzór nad instalacją.*
- *Celowe jest dokonanie w trakcie odbioru sprawdzenia skuteczności działania systemu sygnalizacji i personelu obsługi. Dlatego też przeszkolenia personelu należy dokonać przed dniem odbioru instalacji antywłamaniowej.*

6. Spis rysunków