

**BIURO PROJEKTOWE  
TECHNOLOGII I ARCHITEKTURY**

71-524 Szczecin, ul. Kadłubka 41/23, tel/fax:+48914230413, kom. 601730938, e-mail: [tear4123@gmail.com](mailto:tear4123@gmail.com)

FAZA: **PROJEKT BUDOWLANO-WYKONAWCZY**

TEMAT: PRZEBUDOWA BUDYNKU NA POSTERUNEK POLICJI W MIĘDZYDROJACH

BRANŻA: ELEKTRYCZNA SSWIN

OBIEKT: **BUDYNEK POSTERUNKU POLICJI W MIĘDZYDROJACH.**

ADRES: 72-500 MIĘDZYDROJE, UL. KOPERNIKA 2, DZ. NR 190, OBR. 20

INWESTOR: Komenda Wojewódzka Policji w Szczecinie,  
ul. Małopolska 47, 70-515 Szczecin

OŚWIADCZENIE

Zgodnie z art. 20. ust. 2. Ustawy z dnia 16.04.2004 r. o zmianie ustawy – Prawo Budowlane  
niniejszym oświadczamy, że projekt budowlany został sporządzony zgodnie z obowiązującymi przepisami oraz zasadami wiedzy technicznej.

Autor	Imię i Nazwisko	Nr uprawnień	Podpis
BRANŻA ELEK.	mgr inż.	ZAP/0199/PWOE/08	
Projektant:	ZBIGNIEW KOZAK		_____.
	inż.		
Opracował:	PIOTR ŚWIGOŃ		_____.
	mgr inż.	ZAP/0146/POOE/07	
Sprawdził:	MAREK MIELCZAREK		_____.
Dyr.Jedn.Proj.	mgr inż.	85/64	
	JAN KISIELEWICZ		

Szczecin, maj 2014 r.

## **SPIS TREŚCI:**

<b>Dane ogólne .....</b>	<b>3</b>
<i>Podstawa techniczna opracowania projektu: .....</i>	<i>3</i>
<i>Wytyczne do projektowania: .....</i>	<i>3</i>
<i>Przedmiot i zakres projektu.....</i>	<i>3</i>
<b>Opis rozwiązań technicznych: .....</b>	<b>4</b>
<i>Zakres i sposób ochrony obiektu .....</i>	<i>4</i>
<i>Opis obiektu: .....</i>	<i>4</i>
<i>Zakres ochrony .....</i>	<i>4</i>
<i>Ochrona antysabotażowa urządzeń .....</i>	<i>8</i>
<i>Zasilanie systemu.....</i>	<i>8</i>
<b>Sposób prowadzenia instalacji wewnętrznej.....</b>	<b>9</b>
<b>Uwagi dla inwestora (użytkownika) systemu antywłamaniowego.....</b>	<b>10</b>

## **Dane ogólne**

### **Podstawa techniczna opracowania projektu:**

- koncepcja ochrony technicznej
- podkłady architektoniczne
- uzgodnienia ze zleceniodawcą

### **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 dozоровe CCTV w zastosowaniach dotyczących zabezpieczania”.
- Przewodnik rzeczoznawcy, zeszyty 1-8, 1994r,
- Karty katalogowe

### **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

## **Opis rozwiązań technicznych:**

### **Zakres i sposób ochrony obiektu**

#### **Opis obiektu:**

*Projekt obejmuje opracowanie instalacji systemu sygnalizacji włamania i napadu (SSWiN) oraz kontroli dostępu (SKD) dla budynku Komisariatu Policji przy ulicy Kopernika 2 w Międzyzdrojach.*

*Obiekt stanowi kompleks budynków o charakterze administracyjnym wraz z niezbędną infrastrukturą. Występują specyficzne pomieszczenia typu: magazyn broni, magazyn NPP.*

### **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:*

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

*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 dozoru pomieszczenie wymagające szczególnej ochrony.*
- 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 magazynie NPP.*
- d) *Manipulatory będą pełnić funkcję lokalnej sygnalizacji włamania.*
- e) *Kontrola dostępu ograniczająca dostęp do pomieszczeń tylko dla uprawnionych osób.*
- f) *Nadzór nad systemem KD i SSWiN poprzez dedykowany komputer z oprogramowaniem TITAN oraz programem wizualizacji stanu obiektu ALLIANCE 8300, umożliwiającym bieżącą obserwację ruchu osobowego w 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)*

*Powyższe systemy projektuje się w oparciu o urządzenia UTC serii ATS MASTER. Jest to zintegrowany system sygnalizacji włamania i napadu oraz kontroli dostępu, zapewniający najwyższy stopień bezpieczeństwa. Spełnia wymogi klasy SA4.*

### **Centrala alarmowa ATS 4018**

- 16 linii na płycie, możliwość rozszerzenia do 32 linii (dwoma modułami ATS 1202)
- 3 wyjścia wysokoprądowe (na syreny i lampę)
- 1 wyjście typu NC/NO (programowane)
- 8 wyjść typu OC (na złączu), możliwość zwiększenia liczby wyjść poprzez:
  - moduły 16 wyjść typu OC ATS 1820

- moduły 8 wyjść typu NC/NO ATS 1811 (liczba modułów ograniczona tylko miejscem w obudowie)
- Dialer telefoniczny na płycie (protokół Contact ID)
- Złącze serwisowe RS 232 (tymczasowe podłączenie komputera)
- Miejsce na 1 lub 2 akumulatory 12 V 7,2 Ah

### **ATS 1105 - podstawowy manipulator systemu**

ATS, stosowany jako interfejs użytkownika. Daje dostęp do wszystkich funkcji systemu, łącznie z otwieraniem drzwi (za pomocą kodu). Ma wyświetlacz LCD 2 x 16 znaków oraz 8 diod wskazujących stan obszarów (1-8 lub 9-16). ATS 1100 ma jedno wejście (przycisk otwarcia drzwi) oraz jedno wyjście typu OC (otwieranie drzwi przez dodatkowy przekaźnik)

### **ATS 1190 – czytnik kart zbliżeniowych**

Czytnik kart zbliżeniowych ATS 1470/1471. Może pracować jako urządzenie typu ZAZ (dołączane do magistrali systemowej centrali lub kontrolera), bądź w trybie off-line jako czytnik z wyjściem w standardzie Wieganda. W zależności od trybu pracy, wymaga podłączenia przewodem 4...8 żyłowym. Maksymalne odległości przy pracy jako ZAZ: tak jak dla innych urządzeń tego typu (do 1500 m). ATS 1190 ma własne menu programowania i może być konfigurowany z manipulatora centrali lub przez programator kart (ATS 1620) i tzw. kartę konfiguracyjną. Może służyć do zazbrajania/rozbrajania kartą grup alarmowych lub do otwierania drzwi. Dwie diody wskazujące stan zazbrojenia obszarów (czerwona) oraz otwarcie drzwi (niebieska).

### **ATS 1250 Kontroler dostępu dla 4 drzwi**

Urządzenie typu MZD, służące do tworzenia złożonych systemów kontroli dostępu. Dzięki jego zastosowaniu stają się dostępne zaawansowane funkcje, nieosiągalne przy stosowaniu tylko samych czytników dołączonych do centrali ATS 4018. Są to m. in:

- dołączanie linii czujek otwarcia drzwi,
- rozbudowane tryby zazbrajania i rozbrajania grup alarmowych kartą,
- strefy anti-pass back,
- różne tryby pracy (np. karta+ kod) w oknach czasowych,
- alarm „drzwi otwarte za długo”,
- alarm „wymuszone otwarcie”,
- karty „wizytowe”,
- zliczanie wejść i wyjść,
- funkcja „dwie karty” (dwa kody),
- czytanie 7 różnych formatów kart (Wiegand 26-bit, Wiegand 30-bit itp.),
- możliwość dołączenia czytników innych firm (z wyjściem Wieganda).

Kontroler ma na płycie 4 interfejsy Wieganda, do których można dołączyć czytniki ATS 1190 lub inne, kompatybilne (np. HID).

Dodatkowo, posiada też własną magistralę, na której może znajdować się do 16 urządzeń typu ZAZ, wykorzystywanych do otwierania drzwi lub sterowania systemem alarmowym. Mogą to być urządzenia:

- czytniki ATS 1190
- manipulatory ATS 1100 (kontrola dostępu za pomocą kodu PIN)

- manipulatory ATS 1105 (z dołączonymi czytnikami ATS 1190) – sterowanie za pomocą karty i kodu PIN
- interfejs ATS 1170: możliwość dołączenia czytników Wieganda innych firm

### **Czujka dualna PIR+MV**

tor PIR i mikrofalowy  
 poczwórny pyroelement  
 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 ( $\pm 15\%$ ) 12 V DC  
 Średni pobór prądu ( $\pm 10\%$ ) 24 mA  
 Wymiary obudowy (mm) 63 x 136 x 49  
 Regulowany uchwyt do montażu tak  
 Klasa środowiskowa II  
 Zakres temperatur pracy  $-10^{\circ}\text{C} \dots +55^{\circ}\text{C}$

### **Czujki kontaktronowe MC440 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  
 Materiał magnesu: Alnico 5  
 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  
 Białe lub brązowy plastik  
 Zatwierdzony przez Techom, ANPI/NVBB i inne europejskie biura certyfikacyjne

### **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 EWS4001 zainstalowanych przy kontrolerach.*

#### **Okablowanie.**

*Zasilanie centralki i zasilaczy włączyć do lokalnych rozdzielnic na kondygnacjach, zabezpieczyć szybkim bezpiecznikiem nadprądowym B6.*

*Przewody magistralne między urządzeniami MZD i ZAZ wykonać kablem FTP kat5e. Do podłączenia czujek użyć przewodu typu YTKSY 3x2x0,5.*

#### **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.*
- dopuszcza się łączenie przewodów kontroli dostępu (czytniki, przyciski wyjścia, czujki otwarcia) pod warunkiem zastosowania puszek łączeniowych wyposażonych w styk antysabotażowy.*

#### **Zasilanie systemu**

*Zasilanie płyty głównej centrali ATS MASTER i modułów MZD 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 podstawowe SSWiN należy doprowadzić z wydzielonego obwodu 230V AC, zabezpieczenie typu B6 należy oznaczyć i opisać w rozdzielnicy elektrycznej.*

**Sposób prowadzenia instalacji wewnętrznej.**

*Instalację prowadzić natynkowo w korytach instalacyjnych lub podtynkowo w rurach elektroinstalacyjnych RL. Instalacja nie może być układana razem z instalacją elektryczną (odstęp 20cm). Do czujek doprowadzić przewody typu YTKSY 3x2x0.5, magistrale do manipulatorów i ekspanderów wykonać przewodem UTP kat 5e, zasilanie centrali ATS 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. Zastosowanie systemów innego producenta wymaga ew. zmian w okablowaniu, co należy nanieść w dokumentacji powykonawczej.***

## **Uwagi dla inwestora (użytkownika) systemu antywłamaniowego.**

- Po zainstalowaniu całego wyposażenia wewnątrz lub przy zmianie w wykorzystaniu przestrzeni należy przeprowadzić weryfikację projektu, pod względem sprawności dozoru 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 centrali 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**

Rys. nr SSWIN1 - Rzut II-piętra – instalacja SSWIN

Rys. nr SSWIN2 - Rzut I-piętra – instalacja SSWIN

Rys. nr SSWIN3 - Rzut parteru – instalacja SSWIN

Rys. nr SSWIN4 - Rzut piwnic – instalacja SSWIN

Rys. nr SSWIN5 - Instalacja SSWIN – schemat blokowy