PHU Paweł Iwanicki *tel. 660 482 486*
ul. Marszałkowsk 1a/3, 16-020 Czarna Białostocka *email: iwanickipawel@wp.pl*

PROJEKT WYKONAWCZY
CZĘŚĆ SSWIN, CCTV

Montażu Systemu Sygnalizacji Włamania i Napadu (SSWiN)
oraz
Telewizji Dozorowej (CCTV)

Zadanie:
"Budowa świetlicy wiejskiej w Perlejewie"

Nazwa obiektu budowlanego:
Świetlica w Perlejewie

Numery ewidencyjne działek na których obiekt jest usytuowany:
działka nr: 113/2 obręb Perlejewo

Adres obiektu budowlanego:
Woj.: podlaskie , gmina Perlejewo,

Nazwa i adres Inwestora:
Gmina Perlejewo,
Urząd Gminy Perlejewo
17-322 Perlejewo
woj. podlaskie

Projektanci:

Funkcja	Imię i Nazwisko	Data	Podpis
Projektant	inż. Paweł Piłkowski	26.06.2010r.	
Współpraca	mgr. inż. Paweł Iwanicki	26.06.2010r.	

Data opracowania: 26.06.2010r.

PHU Paweł Iwanicki *tel. 660 482 486*
ul. Marszałkowsk 1a/3, 16-020 Czarna Białostocka *email: iwanickipawel@wp.pl*

Spis zawartości projektu

I- Opis projektu

II- Rysunki

1. Rysunek nr1 – Schemat rozmieszczenia urządzeń SSWiN i CCTV
2. Rysunek nr 2 – Schemat blokowy instalacji SSWiN
3. Rysunek nr 3 – Schemat blokowy systemu CCTV

1. PODSTAWY OPRACOWANIA DOKUMENTACJI

Podstawę opracowania stanowi umowa pomiędzy firmą PHU Paweł Iwanicki, ul. Marszałkowska 1a/3, 16-020 Czarna Białostocka oraz Gminą Perlejewo na wykonanie dokumentacji projektowej branży elektrycznej Świetlicy wiejskiej w Perlejewie.

2. PRZEDMIOT OPRACOWANIA

Projekt SSWiN i CCTV wraz z przedmiarem robót, kosztorysem inwestorskim, specyfikacją techniczną wykonania i odbioru "Budowa świetlicy wiejskiej w Perlejewie".

3. ZAKRES OPRACOWANIA

W zakres opracowania wchodzą instalacje Systemu Sygnalizacji Włamania i Napadu oraz telewizji dozorowanej CCTV.

4. MATERIAŁY WYKORZYSTANE PRZY OPRACOWANIU

- obowiązujące normy i przepisy,
- katalogi aparatury zastosowanej w projekcie,
- uzgodnienia z Zamawiającym,
- wizja lokalna na obiekcie,
- Polska Norma PN-93/E-08390/12 (Systemy alarmowe).

5. OGÓLNY OPIS ZASTOSOWANEGO SYSTEMU INTEGRA

5.1. Właściwości Systemu

- do 32 wejść
  - wybór konfiguracji: NO, NC, EOL, 2EOL/NO i 2EOL/NC
  - szeroki wybór typów reakcji
  - kontrola obecności i poprawności działania czujek
- 32 wyjść
- do 16 stref
  - strefy mogą być sterowane przez użytkowników, timery, wejścia sterujące lub ich stan może zależeć od stanu innych stref
  - możliwość grupowania stref i utworzenia 1 partycji
  - czasowa blokada strefy
- współpraca z wieloma dodatkowymi modułami, wspólnymi z centralą

- sterowanie systemem
  - manipulator LCD
  - komputer użytkownika (przez port RS-232, linię telefoniczną lub sieć komputerową)
  - klawiatura strefowa
- program centrali
  - oprogramowanie zapisane w pamięci typu FLASH
  - aktualizacja oprogramowania bez konieczności demontażu centrali
- programowanie ustawień centrali
  - lokalnie przy pomocy manipulatora LCD
  - lokalnie przy pomocy komputera podłączonego do portu RS-232
  - zdalnie przy pomocy komputera łączącego się z centralą za pomocą modemu
  - pamięć FLASH zachowująca ustawienia centrali nawet po odłączeniu zasilania
- hasła do 64 haseł użytkowników
  - do 1 hasła administratora (1 hasło dla każdej partycji)
  - 1 hasło serwisowe
- kilkanaście typów haseł użytkownika z możliwością definiowania dodatkowych uprawnień określających zakres dostępu do systemu
  - menu funkcji w manipulatorze zależne od typu hasła i uprawnień użytkownika
  - określanie dostępu do klawiatur, zamków szyfrowych i czytników kart zbliżeniowych
  - okresowa zmiana haseł przy pomocy prefiksów, zapewniających lepszą ochronę przed nieuprawnionym dostępem do obiektu
  - definiowanie stref chronionych dwoma hasłami
- edycja nazw: użytkowników, stref, wejść, wyjść i modułów, co ułatwia sterowanie systemem i jego nadzór
- timery
  - do 32 timerów systemowych definiowanych przez serwis
  - timery strefowe definiowane przez użytkowników
- pamięć zdarzeń
  - możliwość zapamiętania do zdarzeń
  - rejestrowanie zdarzeń: załączenie/wyłączenie czuwania,

- kontrola dostępu
  - kontrola stanu drzwi i sterowanie ryglami przy pomocy klawiatur strefowych, zamków szyfrowych, czytników kart zbliżeniowych i pastylek
  - kontrola stanu drzwi nie wpływa na liczbę dostępnych wejść dozorowych centrali
  - sterowanie zamkiem elektromagnetycznym nie zmniejsza ilości dostępnych wyjść centrali

- monitoring telefoniczny
  - 4 numery stacji monitorujących (2+2 numery rezerwowe)
  - 9 identyfikatorów
  - formaty transmisji: podstawowe 4/2,
- powiadamianie
  - od 4 do 16 numerów telefonów
  - od 16 do 32 komunikatów głosowych
  - od 16 do 64 komunikatów tekstowych
  - potwierdzenie odbioru komunikatu hasłem z klawiatury telefonu (DTMF)
- odpowiadanie na telefon
  - rejestrowane w pamięci zdarzeń
  - sprawdzenie stanu stref centrali
  - sterowanie odpowiednio zaprogramowane

6. ANALIZA ZAGROŻEŃ

Ogólna charakterystyka przestępczości w Polsce oraz ich sprawców

W ostatnich latach obserwujemy systematyczny wzrost zagrożenia przestępczością. Jednocześnie występuje stała tendencja do profesjonalizacji przestępczości, stosowania broni palnej i przedmiotów niebezpiecznych oraz umiędzynarodowienie przestępczości.

Bezpieczeństwo zależne jest od bardzo wielu czynników, które powinny stanowić całość. Poszczególne sposoby oraz środki zabezpieczenia i ochrony muszą się wzajemnie uzupełniać i tworzyć szczelny system bezpieczeństwa. Jak uczy doświadczenie bezpieczeństwo osób i mienia może być tworzone tylko przez kompleks specjalnych środków, których generalnym celem jest ograniczenie możliwości powstawania zagrożeń, zaś w przypadku zaistnienia, pełna ich neutralizacja. Nasuwa się więc wniosek, że system zabezpieczający nie może dobrze funkcjonować bez odpowiedniego powiązania środków technicznych, i zasad organizacyjnych odpowiednich służb. Widzimy więc, że na nic się nie zda nowoczesny system alarmowy bez skutecznych zabezpieczeń mechanicznych oraz adekwatnie szybkiej interwencji odpowiednich służb.

Aby wykonać właściwy system zabezpieczeń przeciwdziałający skutecznie istniejącym zagrożeniom oraz posiadający optymalną wielkość (choćby ze względów ekonomicznych), koniecznym staje się dokładne określenie podstawowego zbioru zagrożeń mogących potencjalnie wystąpić w badanym obiekcie. Kolejnym istotnym krokiem będzie określenie funkcji realizowanych przez analizowany obiekt mające istotny wpływ na występowanie wcześniej określonego podstawowego zbioru zagrożeń. Istotą sprawy jest wyszukanie zależności pomiędzy określonymi zagrożeniami a funkcjami realizowanymi w obiekcie.

6.1.Klasyfikacja występujących na obiekcie zagrożeń:

6.1.1.Klasyfikacja w/g przyczyn.

- zagrożenia **losowe** - to te które wynikają z aktywności sił przyrody inaczej mówiąc żywiołów, nie mające bezpośredniego związku z zamierzonym działaniem człowieka. Oczywiście w pewnych wypadkach ta granica między zagrożeniami losowymi a zagrożeniami wynikającymi z działania człowieka jest mało precyzyjna. Może się na przykład zdarzyć, że to człowiek w sposób świadomy lub nieświadomy wyzwoli siły żywiołów. Losowość tych zdarzeń można też próbować ująć w pewne ramy przy pomocy statystyk, a nawet rachunku prawdopodobieństwa uwzględniając w danych wejściowych zjawiska przyrody występujące na danym obszarze (szkody górnicze , powodzie, susze, gwałtowne burze i huragany). Najczęściej występującym zagrożeniem z tej grupy jest pożar. Jest to zagrożenie losowe mimo, że zazwyczaj wynikające z nieprzestrzegania przez człowieka określonych przepisów.

- zagrożenia **zamierzone** - czyli te gdzie siłą sprawczą jest człowiek. Podstawową cechą tej grupy jest fakt, że źródłem zagrożenia jest **działanie lub zaniechanie działania przez człowieka**. Różnorodność tych zagrożeń jest tak wielka jak nieograniczona jest ludzka fantazja. W praktyce jednak zależy od złożoności funkcji jaką reprezentuje przedmiot zagrożenia. W naszym wypadku tym przedmiotem jest sąd z całą gamą swoich funkcji zatem ilość zagrożeń jest tu dość znaczna. Drugą charakterystyczną cechą opisywanego typu zagrożeń jest **bezprawność działań.** Czyli innymi słowy zagrożenia zamierzone są spowodowane działaniem bezprawnym. Trzecią charakterystyczną cechą opisywanego rodzaju jest ich rzeczywisty charakter. Innymi słowy są to zagrożenia prawdziwe i realne.

6.1.2.Klasyfikacja w/g czasu:

1. Zagrożenia występujące **w czasie godzin pracy obiektu**
2. Zagrożenia występujące **poza godzinami pracy obiektu**

6.1.3.Klasyfikacja w/g miejsca:

1. Zagrożenia **zewnętrzne** - *są to takie zagrożenia gdzie miejscem ich powstania jest otoczenie zewnętrzne obiektu.*
2. Zagrożenia **wewnętrzne** - *są to takie zagrożenia gdzie miejscem ich powstania jest wewnętrzna struktura obiektu.*

6.1.4.Klasyfikacja w/g charakteru przestępstw:

1. Zagrożenia wynikłe z przestępstw o **charakterze kryminalnym.**
2. Zagrożenia wynikłe z przestępstw o **charakterze ekonomiczno - finansowym**
3. Zagrożenia wynikłe z przestępstw o **charakterze komputerowo - informatycznym**

6.2.Wyszczególnienie potencjalnych zagrożeń

1. Kradzież zwykła - *(rozumiana jako zabór cudzego mienia w celu przywłaszczenia)*

2. Kradzież z włamaniem - *(ma miejsce wówczas kiedy zabór mienia następuje w następstwie usunięcia przeszkody materialnej będącą częścią konstrukcji lub zamknięcia)*

3. Przestępstwo rozbójnicze - *ma miejsce wówczas kiedy występuje przemoc i skierowana jest ona na osobę, a nie na rzecz.*

4. Zagrożenie kradzieżą rozbójniczą - *występuje wówczas kiedy bezpośrednio po zaborze mienia następuje gwałt na osobie w celu utrzymania się w posiadaniu mienia.*

5. Kradzież szczególnie zuchwała - *wykorzystanie przez sprawcę kradzieży postawy obliczonej na zastraszenie lub zaskoczenie. Przemoc sprawcy skierowana jest na rzecz, a nie na osobę.*

6. Rozbój - *występuje wówczas, kiedy zabór mienia ma miejsce w następstwie użycia gwałtu lub przemocy na osobie, której mienie skradziono.*
7. Wymuszenie rozbójnicze - *występuje wówczas kiedy sprawca poprzez groźbę użycia gwałtu na osobie zmusza tę osobę do wydania należącego do niej mienia, przy czym wydanie mienia następuje w przyszłości.*

8. Zagrożenie ujawnieniem tajemnicy służbowej - - *nie wymaga komentarza*

9. Przywłaszczenie - *rozumie się przez nieuprawnione wejście w posiadanie dokumentów, informacji stanowiących własność innej osoby*
10. Zagrożenie oszustwem poprzez wprowadzenie w błąd - *np. umyślne przekazanie błędnych i nieprawdziwych informacji w celu uzyskania korzyści.*

11. Zagrożenie oszustwem poprzez wyzyskanie błędu - *np. wykorzystanie informacji o nieświadomie popełnionym błędzie w celu osiągnięcia korzyści.*

12. Zniszczenie mienia - *celowe działanie powodujące np. trwałe uszkodzenie urządzenia lub pozbawienie cech charakterystycznych dokumentu np. czytelność, widzialność, słyszalność itp.*

13. Uszkodzenie mienia - *celowe działanie powodujące np. czasową niesprawność urządzenia lub częściową nieczytelność nośnika informacji.*

14. Fałszerstwo - *świadome działanie polegające nadaniu np. dokumentowi wszystkich cech autentyczności bez wiedzy i zgody właściciela czy twórcy dokumentu. Również przekazanie informacji zawierającej nieprawdziwe dane stanowi fałszerstwo.*

15. Wymuszenie (szantaż) - *np. zmuszanie osoby trzeciej do działania przestępczego lub na niekorzyść firmy z wykorzystaniem prywatnych informacji o tej osobie lub też o osobach*

bliskich.

16. Podsłuch bezpośredni - *podsłuch prowadzony bezpośrednio przez osobę zainteresowaną pozyskaniem wiadomości np. z sąsiedniego pokoju lub ukrycia.*

17. Podsłuch zdalny (elektroniczny) - *instalacja urządzeń podsłuchowych w pomieszczeniach, urządzeniach łączności, itp. bezpośrednio użytkowanych przez podsłuchiwaną osobę lub grupę osób. Również podsłuch z użyciem oddalonych mikrofonów kierunkowych itp.*

18. Sabotaż inspirowany od wewnątrz - *uczynienie mienia w postaci urządzenia, dokumentu lub też inaczej zachowanej informacji, niezdatnym do użytku na zlecenie osoby mającej stały dostęp do tych dokumentów lub urządzeń. Fizyczna obecność sabotażysty organizowana jest w zasadzie przez tę właśnie osobę.*

19. Sabotaż inspirowany od zewnątrz - - *uczynienie mienia w postaci urządzenia, dokumentu lub też inaczej zachowanej informacji, niezdatnym do użytku na zlecenie osoby nie mającej stałego dostępu do tych dokumentów lub urządzeń. Fizyczna obecność sabotażysty organizowana jest raczej z zewnątrz z wykorzystaniem przeważnie nieświadomości, naiwności lub lekkomyślności osób/osoby mającej stały dostęp do tych dokumentów.*

20. Nieuprawnione kopiowanie - *ma miejsce wówczas kiedy zaistnieją warunki do kopiowania dokumentów bez wiedzy i zgody osób zarządzającymi tymi dokumentami.*

21. Przekupstwo - *wejście w posiadanie interesujących materiałów w drodze przekazania korzyści majątkowych osobie mającej dostęp do tych materiałów.*

22. Zmowa przestępcza - *zorganizowanie grupy osób, która w celu uzyskania korzyści organizuje się do przestępczych działań.*

23. Zagrożenie podglądem - *sytuacja w której możliwy jest do prowadzenia podgląd zachowania osób, przebiegu np. poufnych rozmów, podglądu w celu identyfikacji osób uczestniczących z zamiarem późniejszego wykorzystania tej wiedzy. Często samej operacji podglądu towarzyszy rejestracja .*

24. Zagrożenie pozorowanymi działaniami przestępczymi - *ma miejsce wówczas kiedy dla odwrócenia uwagi działania przestępcze inicjowane są w innym miejscu.*

25. Zagrożenie działaniem przestępczym z ukrycia - *ma miejsce wówczas kiedy potencjalny przestępca ukrył się w strefie chronionego obiektu w celu dokonania przestępstwa w czasie najbardziej odpowiednim.*

26. Zagrożenie uszkodzeniem infrastruktury technicznej - *ma miejsce wówczas kiedy istnieje realne prawdopodobieństwo celowym działaniem powodującym dysfunkcję urządzeń*

technicznych zapewniających niezakłócony tok pracy w obiekcie.

27. Zagrożenie celowym wywołaniem pożaru - *rozumiane jest jako podpalenie w celu np. odwrócenia uwagi, zatarcia śladów innego działania przestępczego lub dezorganizacji pracy obiektu.*

28. Zagrożenie osobiste dla osób z kierownictwa - *należy tu rozumieć zespół różnorakich zagrożeń np. porwanie, celowe spowodowanie wypadku, szantaż, sprowadzających się do tego, że osoba taka zmuszona jest postępować wbrew interesom swojej instytucji.*

29. Zagrożenie nielojalnością pracowników - *ma miejsce wówczas kiedy zespół pracowników czuje się niedowartościowany, a atmosfera pracy w zespole jest stresogenna. To niedowartościowanie może dotyczyć np. wynagrodzenia, pozycji w zespole, formalnego stanowiska służbowego, nagród i wyróżnień itp.*

30. Zagrożenie krótkotrwałą destabilizacją pracy komórki organizacyjnej - *ma miejsce wówczas kiedy występuje realne prawdopodobieństwo zakłócenia na krótki okres czasu pracy komórki poprzez np. celowe wyłączenie zasilania, spowodowanie zawieszenia sprzętu informatycznego, krótkotrwały zabór dokumentów, blokada systemów łączności itp.*

31. Zagrożenie długotrwałą destabilizacją pracy komórki organizacyjnej - *jw. lecz to prawdopodobieństwo dotyczy dłuższego czasu.*

W terminologii prawniczej jako przestępstwo określamy czyn, który posiada trzy cechy:
- jest to czyn człowieka
- jest to czyn bezprawny
- ma on charakter rzeczywisty
Niektórzy kryminolodzy, patrząc z punktu widzenia sprawcy wyróżniają przestępstwa agresywne oraz intelektualne. Patrząc z punktu widzenia skąd pochodzi sprawca można wyróżnić trzy rodzaje zagrożeń

1. Przestępstwa popełniane przez sprawcę który jest w obiekcie nieproszonym gościem
2. Przestępstwa pracownicze - dokonywane przez sprawcę, który jest w obiekcie na podstawie stosunku pracy.
3. Przestępstwa kontrahenckie - popełniane przez osobę która pozostaje z obiektem w określonym stosunku prawnym. Zaliczyć do nich można również przekupstwo, wyłudzenia mienia, fałszerstwa dokumentów.

Można również przeprowadzić klasyfikację zagrożeń w/g czasu w którym one powstają i występują one w szkole w czasie godzin pracy obiektu, i poza godzinami pracy.

Sklasyfikować można przestępstwa także według miejsca gdzie one powstają i wyróżnić

tu możemy zagrożenia zewnętrzne i wewnętrzne.

Wśród wielu przestępstw kryminalnych przeważają zagrożenia przestępcze przeciwko mieniu i życiu czyli kradzieże, z włamaniem, rozboje i wymuszenia rozbójnicze. Ich udział w ogólnej ilości stwierdzonych przestępstw wynosi blisko 60 %.

Spośród przestępstw przeciwko mieniu szczególnie niebezpieczne są te, w których sprawca używa przemocy. Są to przestępstwa o charakterze rozbójniczym. Znajomość podstawowych cech osobowościowych przestępców powinna ułatwić rozpoznawanie zagrożeń i odpowiednio na nie reagować.

W ostatnich latach przestępstwa przeciwko mieniu i życiu skierowane były przede wszystkim na:

- środki transportu 30%
- obiekty gospodarstwa domowego 23,5%
- obiektom handlowym 14%

Należy się liczyć z faktem że, przestępcy profesjonalni rezygnować będą z siłowego frontalnego ataku na obiekt, a stosować będą inne środki które zapewnią im określony cel, bez zbędnego narażania się. W związku z tym dokonują w miejscach potencjalnych przestępstw szeroko zakrojone rozpoznania sytuacji. Dlatego konieczne jest zachowanie w tajemnicy wszelkich informacji, które mają związek z bezpieczeństwem osób i mienia.

6.3.ROZPATRYWANY ZBIÓR ZAGROŻEŃ

Biorąc pod uwagę specyfikę obiektu jakim jest świetlica wiejska strukturę i rodzaj przechowywanych walorów należy spodziewać się szerokiego wachlarza zagrożeń.

Analizując funkcje realizowane przez obiekt możemy rozróżnić:

1. Praca obiektu w czasie pracy personelu
2. Obiekt po godzinach pracy

Do miejsc szczególnie narażonych na zagrożenia możemy zaliczyć:

1. Pracownia komputerowa (POM. NR. 6)
2. Pomieszczenie gospodarcze (POM. NR. 8)
3. Świetlica (POM. NR. 7)

Zależność między potencjalnymi zagrożeniami a miejscami ich występowania przedstawia tabela 1

MIEJSCE → **ZAGROŻENIE ↓**	Pracownia komputerowa	Pomieszczenie gospodarcze	Świetlica
Kradzież zwykła	X	X	X
Kradzież z włamaniem	X	X	X
Przest. rozbójnicze	X	X	X
Zagrożenie kradzieżą rozbójniczą	X	X	X
Kradzież szczególnie zuchwała	X	X	X
rozbój			
Wymuszenie rozbójnicze			
Atak terrorystyczny	X	X	X
Ujawnienie tajemnicy państwowej			
Ujawnienie tajemnicy służbowej			
przywłaszczenie	X	X	X
Oszustwo przez wprowadzanie w błąd	X	X	X
Oszustwo przez wyzyskanie błędu			
Zniszczenie mienia	X	X	X
fałszerstwo			
wymuszenie	X	X	X
Podsłuch bezpośredni	X	X	X
Podsłuch zdalny	X	X	X
Sabotaż od wewnątrz	X	X	X
Sabotaż od zewnątrz	x	x	x
Bezprawne kopiowanie			
Porwanie dla wymuszenia			
przekupstwo			
Zmowa przestępcza	X	X	X

6.4.OCENA STOPNIA RYZYKA

Na podstawie przeprowadzonej analizy zagrożeń określiłem kategorię zagrożonej wartości jako Z 4. Na tej podstawie dobrano klasę systemu alarmowego, i przyjęto klasę urządzeń alarmowych. Ponieważ obiekt charakteryzuje się średnim ryzykiem szkód oraz nie zachodzi konieczność stosowania czujników przystosowanych do pracy w ekstremalnych warunkach atmosferycznych system alarmowy został zaklasyfikowany do **klasy SA – 3.**

6.5.CZYNNOŚCI MAJĄCE NA CELU PRZECIWDZIAŁANIE ZAGROŻENIOM

Ogólnie środki neutralizacji zagrożeń dzielimy na:

1.Prawne a wśród nich

- kompetencje instytucji i organizacji powołanych dla zwalczania zagrożeń.
- wymagania wobec środków neutralizacji zagrożeń i ich kontroli.
- określanie podmiotów uprawnionych do zapewnienia bezpieczeństwa osobom i mieniu oraz ich kompetencji.
- ustalanie wymagań techniczno - eksploatacyjnych dla wyrobów oraz świadczonych usług, a także w zakresie zachowań się ludzi.
- zapewnienie naprawiania szkód powstałych w wyniku zamachu.

2. Architektoniczno budowlane

- lokalizacja obiektu{ położenie, dojazd, oświetlenie }oraz jego kształt
- konstrukcja obiektu {otwory, umocnienia, pomieszczenia } i użyte materiały
- wewnętrzne funkcje { podział na strefy ochronne }

3. Mechaniczne

- zamki, okucia, kraty, szyby
- środki przechowywania wartości {szafy, kasy, skarbce }
- środki transportowania wartości { samochody }

4. Elektroniczne

- urządzenia i systemy alarmowe
- urządzenia i systemy wspomagające {kontrola dostępu, podgląd i rejestracja obrazu }
- urządzenia i systemy przekazywania informacji o zagrożeniach

5. Fizyczne

- dozór lub ochrona fizyczna - dozorcy
- interwencja Policji

Możemy stwierdzić, że bezpieczeństwo osób i mienia będzie zapewniona w przypadku, kiedy czas na odparcie zamachu oraz ujęcia sprawcy będzie krótszy lub równy sumie czasów niezbędnych dla:

- pokonania przez sprawcę zabezpieczeń budowlanych i mechanicznych
- rozpoznawania przyczyny i sygnalizowania faktu naruszenia strefy chronionej
- realizacji zamiaru sprawcy

Niektóre z tych środków mają na celu odstraszenie potencjalnego przestępcę poprzez manifestowanie swego istnienia i działania a wszystkie w/w mają ochraniać dobra poprzez stwarzanie warunków dla skutecznej reakcji na występujące zagrożenia.

6.6.PODZIAŁ OBIEKTU NA STREFY OCHRONY

W systemie zostały wydzielone strefy:

1. Świetlica i pracownia komputerowa (obsługiwane przez użytkowników)
2. Pomieszczenie Gospodarcze (obsługiwane przez użytkowników)

6.7.OPIS FUNKCJONALNY SYSTEMU.

System został podzielony na 2 niezależnych stref. Podział taki umożliwia wyłączenie z dozoru 1 części systemu alarmowego bez przerywania ochrony pozostałych części obiektu

Każdemu z użytkowników zostanie przydzielony indywidualny kod, przez co możliwa będzie identyfikacja osób obsługujących system alarmowy.

6.8.OKABLOWANIE

Zasilanie główne 230V urządzeń zainstalowanych w budynku odbywać się będzie z wydzielonego obwodu z głównej tablicy zasilającej w budynku RG. Okablowanie z tablicy do centrali należy wykonać kablem YDYp 3*1,5.

Połączenia czujników wewnątrz budynku z centralą wykonać kablem YTDY 10*0,5mm, kabel ułożyć w listwach instalacyjnych.

Magistralę cyfrową – szynę szyfratorów LCD – ułożyć w listwach instalacyjnych kablem YTDY 6*0,5.

Schematy rozmieszczenia okablowania oraz urządzeń wraz ze schematem blokowym systemu SSWiN przedstawione zostały na dołączonych rysunkach nr 1 – nr 2.

6.9.MONTAŻ URZĄDZEŃ

Płyta główna centrali zawiera elementy elektroniczne wrażliwe na wyładowania elektrostatyczne. Przed montażem należy rozładować ładunki elektrostatyczne, a w czasie montażu unikać dotykania elementów na płycie centrali.

Centrala i inne elementy systemu alarmowego powinny być montowane w ramach obszaru chronionego. W pomieszczeniu tym powinien być dostępny stały (nie odłączany) obwód zasilania 230V z uziemieniem ochronnym.

Uwagi:

- *Przed zamontowaniem obudowy centrali, należy zainstalować kołki mocujące płytę główną.*
- *Należy zastosować większą niż standardową obudowę ze względu na umieszczenie 2 ekspanderów.*
- *Podczas mocowania obudowy należy zwrócić uwagę by nie uszkodzić przewodów, które przełożone będą przez otwory w tylnej ściance centrali.*
- *Podczas dołączania manipulatorów LCD, modułów i pozostałych elementów pobierających zasilanie z wyjść centrali należy wyłączyć zasilanie sieciowe i akumulator.*

UWAGA !

Ponieważ centrala zasilana jest z sieci ~230V, nieostrożność podczas podłączania lub błędne podłączenie może grozić porażeniem i stanowić zagrożenie życia! W związku z tym, przy podłączaniu centrali należy zachować szczególną ostrożność. Przewód, którym podłączone będzie zasilanie sieciowe, w trakcie montażu i podłączania centrali nie może być pod napięciem !

6.9.1. Podłączenie manipulatora LCD

Centrala umożliwia podłączenie ośmiu niezależnych manipulatorów LCD, przeznaczonych do sterowania i programowania systemu alarmowego. Wszystkie manipulatory LCD dedykowane do centrali alarmowej zapewniają jej pełną obsługę i mogą być instalowane w jednym systemie alarmowym. Jeśli do centrali podłącza się kilka manipulatorów, wszystkie łączy się równolegle. Ponieważ dane na szynie manipulatorów są adresowane, wszystkie manipulatory działają niezależnie. Manipulatory podłącza się do złącz centrali. Wyjście umożliwia zasilenie wszystkich manipulatorów (wyjście ma bezpiecznik elektroniczny). Każdy manipulator powinien być podłączony osobnym kablem (zalecamy używanie typowego nieekranowanego przewodu). Odległość manipulatora od centrali może wynosić do **300m**. Dla zapewnienia poprawnego działania manipulatorów istotne jest zapewnienie jak najmniejszej rezystancji kabli. Przykładowo: w zależności od odległości manipulatora od centrali, przy kablu DY8x0,5 dla poszczególnych sygnałów należy zapewnić odpowiednie ilości połączonych równolegle żył.

6.9.2. Podłączenie czujników

Montaż czujki PIR/MW

Czujka przystosowana jest do montażu wewnątrz pomieszczeń. Można ją zamocować bezpośrednio do ściany lub na dołączonym uchwycie. Przed zamontowaniem obudowy należy wyjąć płytkę z elektroniką i wyłamać odpowiednie przepusty pod wkręty i kabel w tylnej ściance obudowy.

Montaż czujki PIR

Czujka przystosowana jest do montażu wewnątrz pomieszczeń. Można ją zamocować bezpośrednio do ściany lub na dołączonym uchwycie. Przed zamontowaniem obudowy należy wyjąć płytkę z elektroniką i wykonać odpowiednie przepusty pod wkręty i kabel w tylnej ściance obudowy.

Podziałka zaznaczona na płytce czujki służy do prawidłowego ustawienia piroelementu względem soczewki zainstalowanej w obudowie. Płytkę, w przypadku montażu czujki na wysokości **2,1m**, należy ustawić środkową kreską naprzeciw wskaźnika umieszczonego na obudowie obok podziałki. Takie ustawienie zapewnia uzyskanie deklarowanego przez producenta zasięgu. W przypadku montażu na innej wysokości należy

przeprowadzić regulację ustawienia piroelementu przesuwając płytkę w górę. Rezystory należy montować wewnątrz obudowy czujki.

Sygnalizator należy montować na płaskim podłożu i w możliwie niedostępnym miejscu tak, aby zminimalizować ryzyko sabotażu. Montaż sygnalizatora do podłoża wykonuje się za pomocą wkrętów i kołków rozporowych (wkręty i kołki rozporowe są w komplecie z sygnalizatorem).

Montaż sygnalizatora wewnętrznego

Sygnalizator należy montować na płaskim podłożu i w możliwie niedostępnym miejscu tak, aby zminimalizować ryzyko sabotażu. Montaż sygnalizatora do podłoża wykonuje się za pomocą wkrętów i kołków rozporowych (wkręty i kołki rozporowe są w komplecie z sygnalizatorem).

6.10. OBLICZENIE POJEMNOŚCI AKUMULATORA I PRĄDÓW ZASILACZA W JEDNOSTCE CENTRALNEJ SYSTEMU

6.11. Pojemność akumulatora i zalecenia wynikające z Polskiej Normy

Zgodnie z obowiązującą Polską Normą PN-93/E-08390/12 (Systemy alarmowe, Wymagania ogólne, Zasilacze - Parametry funkcjonalne i metody badań) konfiguracja zasilania systemu alarmowego powinna być uzależniona od dostępnych źródeł zasilania oraz wymagań stawianym odpowiednim klasom systemów alarmowych i zawierać jedno lub więcej źródeł takich jak baterie akumulatorów. W systemach sygnalizacji włamania i napadu najczęściej występują zasilacze połączone z siecią zasilającą 230 V napięcia przemiennego zawierające transformator bezpieczeństwa i baterię akumulatorów pełniącą funkcję źródła rezerwowego. Występujący w zespole zasilacza układ do ładowania baterii akumulatorów zapewnia utrzymywanie stanu pełnego naładowania akumulatorów w warunkach normalnej pracy systemu alarmowego. Zasilacze są urządzeniami występującymi oddzielnie lub stanowią integralną część centrali alarmowej.

Jeżeli w systemie alarmowym występuje zasilacz zawierający baterię akumulatorów i urządzenie ładujące, wyżej wymieniona norma definiuje sposób określania minimalnej pojemności akumulatora Q_{min} (w Ah) jako:

$$Q = 1{,}25(I_1t_1 + I_2t_2)\ [Ah]$$

gdzie:

I_1 - całkowity prąd pobierany przy zaniku zasilania podstawowego w stanie dozoru,

t_1 - wymagany czas dozoru,

I_2 - całkowity prąd pobierany w stanie alarmowania,
t_2 - wymagany czas alarmowania.

Źródło rezerwowe musi gwarantować czas co najmniej 15 minut alarmu (zasilanie sygnalizatorów) oraz dozorowanie systemu w czasie: 48h. Przełączanie zasilania systemu powinno odbywać się automatycznie i nie powodować zakłóceń pracy systemu.

6.12. Zasilanie rezerwowe w systemach alarmowych

Korzystając z zaleceń Inwestora dokonajmy doboru zasilaczy i akumulatorów dla systemu alarmowego składającego się z elementów opisanych w tablicy 1 zaprojektowanego z uwzględnieniem poniższych założeń:
- czas gotowości t_1 - 48 h,
- czas trwania stanu alarmu t_2 - 1/4 h w ciągu 48 h,
- czas ładowania akumulatorów $t_ł$ - 12 h

Elementy systemu alarmowego i ich pobór prądu [A]
W systemie wykorzystany został zasilacz 4,8A dla zasilania centrali

L.p.	*Urządzenie*	*Prąd znamionowy*	*Ilość*	*Pobór prądu*
1	Centrala	0,12	1	0,12
2	Klawiatura LCD	0,15	1	0,15
3	Klawiatura strefowa	0,1	1	0,1
4	Czujka PIR/MW	0,024	6	0,144
5	Podcentrala	0,02	2	0,04
				RAZEM 0,554 A

W systemie zainstalowano ponadto 8 czujników magnetycznych. Urządzenia te nie wymagają zasilania.

Wykorzystując wzór (1) do obliczenia minimalnej pojemności akumulatora otrzymujemy:

$Q = 1{,}25(I_1t_1 + I_2t_2)$ [Ah]

$Q = 1{,}25(0{,}554*48 + 0{,}479*0{,}25) = 1{,}25(26{,}592+0{,}1198) = 26{,}74$Ah

Zastosować należy akumulator 34 Ah jako wystarczający do zabezpieczenia zakładanego czasu podtrzymania.

6.13. Obliczenia dla zasilacza

Aby można było naładować akumulator w ciągu 12 h należy sprawdzić czy nie będzie przekroczona wartość prądu znamionowego zasilacza podcentrali w czasie ładowania akumulatora prądem I_Q 0,1 In przy jednoczesnym poborze prądu przez przyłączone elementy systemu.

$I = 4{,}8\ A > I_{Q0,1In} + I_{1\ B23} = 3{,}295 + 0{,}729 = 4{,}024\ A$

Ponieważ nierówność jest spełniona wydajność zastosowanego zasilacza 4,8 A jest odpowiednia.

7. Wykaz zastosowanych urządzeń

L.p.	Nazwa urządzenia	klasa	Ilość
1	Centrala	S	1
2	Szyfrator LCD	S	1
3	Szyfrator strefowy LED	S	1
4	Obudowa szyfratora z zamkiem		1
5	Podcentrala	S	2
6	Obudowa centrali z transformatorem	-	1
7	Sygnalizator zewnętrzny	C	1
8	Sygnalizator wewnętrzny	C	1
9	Czujnik magnetyczny	S	8
10	Czujnik PIR	C	0
11	Czujnik PIR/MW	S	6
12	Akumulator 36 Ah	-	1

8. SYSTEM TELEWIZJI DOZOROWEJ (CCTV)

Systemem dozorowym CCTV zostaną objęte wyznaczone przez inwestora obszary terenu wokół budynków. System CCTV jest systemem niezależnym od innych sieci teletechnicznych, posiada własne zasilanie, podłączone do niezależnego pola w tablicy rozdzielczej, własne okablowanie oraz wydzielone trasy kablowe.

8.1. OPIS TECHNICZNY

Zastosowane w wykonanym systemie rozwiązania techniczno-funkcjonalne są typowymi rozwiązaniami dla tego typu systemów. Projektuje się system oparty jest na kamerach zewnętrznych zamontowanych w klimatyzowanych obudowach, wyposażonych w grzałki. Projektuje się zastosować kamery tzw. dzienno/nocne zbudowane na przetwornikach w obudowach klimatyzowanych, odpornych na zniszczenie.

Kamery zostaną wyposażone w obiektywy super jasne, asferyczne o zmiennej ogniskowej z zakresu 3-8mm, z przesłonami automatycznymi sterowanymi DC.

Transmisja sygnałów wizji z kamer do rejestratora odbywać się będzie po łączach bezpośrednich w transmisji standard PAL łączem 75 ohm, standardowy sygnał video 1Vpp. Przewidziano możliwość podłączenia do rejestratora wirtualnych stanowisk podglądu z transmisją po lokalnej sieci IP.

Zastosowano najbardziej optymalne rozwiązanie rejestracji wizji na stanowisku monitorującym poprzez montaż 1 rejestratora wyposażonego w twardy dysk o pojemności gwarantującej archiwizację materiału wizyjnego przez okres nie mniejszy niż 14 dni oraz gniazda USB do zgrywania materiału zapisanego na twardym dysku w formie pojedynczych zdjęć lub sekwencji filmowych.

Prędkość odświeżania zapisu (poklatkowość) wynosić będzie min. 6 klatek/sek. Taka poklatkowość zapewnia dobrą jakość obrazu przy zachowaniu optymalnych warunków sprzętowych w sferze wymagań dotyczących rejestracji, tzn. brak konieczności inwestowania w obszerne archiwa dyskowe.

Do zainstalowanego rejestratora przewidziano podłączenie monitora LCD VGA o przekątnej 19 cali.

8.2. OPIS INSTALACJI ZASILAJĄCEJ I SYGNAŁOWEJ

Od rejestratora do poszczególnych kamer należy doprowadzić indywidualne przewody wizyjne koncentryczne. Na końcach każdego łącza wizyjnego zarobić końcówkę BNC75.Po stronie rejestratora poszczególne przewody podłączyć do odpowiednich wejść wizyjnych, a po stronie kamer - do wyjść sygnałowych 75 Ohm. Do kamer zewnętrznych wraz z obudowami wyposażonymi w podgrzewacze termostatyczne, doprowadzić zasilanie 230 V AC. Połączenie to należy wykonać kablem OMY 3x1,5. Kabel wprowadzić do wnętrza obudowy i odłączyć pod zaciski rozdzielacza zasilania (integralna część obudowy). Kamera zasilana jest napięciem 12V DC z zasilacza zamontowanego wewnątrz obudowy kamery . Grzałki są zasilane napięciem 230V.

Po stronie rejestratora przewody zasilające należy podłączyć do zasilacza UPS.

Zasilanie 230V doprowadzić należy do zasilacza UPS i innych urządzeń CCTV w szafie RACK19" zlokalizowanej wewnątrz budynku.

8.3. LOKALIZACJA KLUCZOWYCH ELEMENTÓW SYSTEMU

Lokalizacja kamer przedstawiona jest na rysunku nr. 1.

Szafa RACK 19” w której należy zainstalować:

1. Rejestrator cyfrowy,
2. Zasilacz awaryjny UPS 1600 VA

8.4.SPOSÓB UKŁADANIA INSTALACJI W BUDYNKU

Okablowanie instalacji wewnętrzne należy ułożyć podtynkowo jeśli to niemożliwe w listwach elektroinstalacyjnych PCV montowanych na wysokości około 2,5m wewnątrz budynku. Trasy kablowe pokazane są na rysunkach, w przypadku konieczności zmiany trasy należy to uzgodnić z przedstawicielem Inwestora, dotyczy to przede wszystkim konieczności ominięcia kolizji z istniejącymi instalacjami, ujawnionymi po rozpoczęciu robót.

8.5.SPOSÓB MONTAŻU ELEMENTÓW

Wszystkie urządzenia systemu zostaną trwale zamontowane do elementów konstrukcyjnych. Dotyczy to w szczególności kamer, które muszą być zainstalowane w sposób stabilny, uniemożliwiający wszelkie przemieszczanie się urządzeń oraz zapewniający niedostępność związaną z wszelkimi próbami dewastacji lub unieszkodliwienia systemu.

Podczas instalacji systemu należy uwzględnić warunki i wymagania, co do obszaru widzenia poszczególnych kamer, warunki ekspozycji oraz uwarunkowań technicznych i technologicznych. Czynności te przeprowadzić w oparciu o wytyczne Inwestora i z udziałem jego przedstawicieli.

W miejscu lokalizacji rejestratora zainstalowana będzie szafa montażowa typu RACK19" w której zainstalowane zostaną UPS i rejestrator cyfrowy. Monitor będzie zamontowany na specjalnie do tego przystosowanym stanowisku operacyjnym.

8.6.SPECYFIKACJA URZĄDZEŃ

W trakcie przeprowadzonej wizji lokalnej, montażu w obiekcie oraz na drodze ustaleń z Inwestorem, jak również Użytkownikiem systemu, spełniono następujące podstawowe wymagania dla zrealizowanego systemu:

Kamera:

Kamera Dzień/Noc,
570 linii TV (700 linii TV w trybie cz/b),
Czułość 0.00003 Lux (w trybie cz/b),
WDR – zwiększenie dynamiki przetwornika 60dB,
Cyfrowa redukcja szumów,
przyciemnienie jasnych obszarów przy BLC,
Mechanicznie zdejmowany filtr podczerwieni,

Obiektyw:

Obiektyw asferyczny 1/3" CS;

Jasność F:1.0;
Ogniskowa 3-8mm; automatyczna przysłona sterowana stałym napięciem, korekcja aberracji dla zakresu bliskiej podczerwieni (IR)

Rejestrator:
Rejestrator cyfrowy 8 kanałowy,
Nagrywanie na dysk z kompresją JPEG-2000,
Transmisja do sieci LAN z kompresją H.264,
Zapis 100 kl./sek. przy rozdz. 720X288,
1 wyjście monitorowe BNC, wyjście monitorowe VGA, LAN, 1 kanał audio, pilot na podczerwień, mysz PS2 w komplecie, USB do archiwizacji,
Obsługa dysków SATA do 1TB ,
Komplet programów do obsługi przez sieć IP:
- program do zmiany ustawień rejestratora;
- program do podglądu obrazu na żywo z kamer;
- program do archiwizacji przez sieć;
- program do odtwarzania zarchiwizowanego materiału;

Obudowa zewnętrzna kamery emaliowana,
zasilacz wewnętrzny 12V DC 500mA
grzałka 230 V,
uchwyt.

Monitor:
Monitor LCD 19", VGA 230VAC.

Szefa RACK 19":
szafa 19" wisząca z półką
wysokość 10U,
jednosekcyjna,
drzwi przednie pełne, zamykane na kluczyk.

UPS:
Moc 1600 VA
Czas przełączania na UPS 3 ms
Filtracja napięcia wyjściowego filtr przeciwzakłóceniowy, RFI/EMI tłumik warystorowy
Napięcie wyjściowe 230 V
Częstotliwość prądu 50 Hz
Ilość gniazd wyjściowych 4 szt.

9. ZESTAWIENIE MATERIAŁOWE

Materiał	Jednostka miary	Ilość

Rejestrator	szt.	1
Dysk 1T SATA	szt.	1
Szafa RACK	szt.	1
UPS 1600 VA	szt.	1
Kamera zewnętrzna	szt.	8
Obiektyw 3-8mm	szt.	8
Obudowa do kamery z zasilaczem	szt.	6
Monitor LCD 19" VGA	szt.	1
Przewód konc. RG 59	m	160
Przewód zasilający OMY 3x1,5	m	100
Listwa instalacyjna	m	30
Puszka krosująca 230V	szt	2
Inne materiały	kpl.	1

10. ZALECENIA DLA UŻYTKOWNIKA

Zaleca się użytkownikowi systemu wyznaczenie osób do pracy przy obsłudze systemu oraz wyznaczenie jednej osoby jako administratora systemu. Osoba ta będzie posiadała większy zakres wiedzy i uprawnień odnośnie funkcjonowania systemu np. archiwizacji wybranych fragmentów nagrań na zewnętrzne pamięci USB.
Pomieszczenie z urządzeniem rejestrującym powinno by odpowiednio zabezpieczone przed dostępem osób nieupoważnionych z zewnątrz jak i nieupoważnionych do obsługi systemu pracowników.

11. NORMY I PRZEPISY

PN-93/E-08390/14 - Systemy alarmowe . Wymagania ogólne. Zasady stosowania.
PN-ICE 60364-1 - Instalacje elektryczne w obiektach budowlanych.
BN-88/8984-19 - Telekomunikacyjne sieci kablowe miejscowe. Ogólne wymagania.
Rozporządzenie Ministra Przemysłu z dnia 08-10-1990r. W sprawie warunków technicznych jakimi powinny odpowiadać urządzenia elektroenergetyczne w zakresie ochrony przeciwporażeniowej Dz.U.Nr 81 z dnia 26-11-1990r. Poz.473
Instrukcje i zalecenia producentów urządzeń.

12. UWAGI KOŃCOWE

Wszystkie roboty instalacyjne oraz uruchomieniowe związane z wykonaniem Systemu CCTV należy wykonać w oparciu o dokumentacją projektową, zalecenia producenta oraz aktualnie obowiązujące normy i przepisy.

Wykonawca powinien spełniać następujące wymaganie:
- posiadać koncesję MSWIA,
- co najmniej jeden z pracowników biorących bezpośredni udział w realizacji inwestycji powinien posiadać Licencje Pracownika Zabezpieczenia Technicznego drugiego stopnia

- Wykonawca bezwzględnie powinien posiadać Autoryzacje Techniczne i certyfikaty uprawniające do instalowania, konfigurowania urządzeń i systemów zawartych w niniejszym projekcie,
-Wykonawca powinien posiadać niezbędną wiedzę, doświadczenie techniczne poparte referencjami oraz możliwości finansowe niezbędne do realizacji zadania,
-Wykonawca musi zapewnić serwis gwarancyjny
Konfigurację programową oraz szczegóły związane z przebiegiem tras kablowych należy uzgodnić z przedstawicielem Inwestora.

Po zakończeniu wszystkich prac należy przeszkolić zespół osób wyznaczonych przez Inwestora do obsługi systemu i sporządzić z tego szkolenia odpowiedni protokół.

Dokumenty, które zobowiązany jest dostarczyć Inwestorowi Wykonawca:
- dokumentację powykonawczą,
- protokół zdawczo odbiorczy,
- protokół z przeszkolenia w obsłudze systemy wyznaczonych przez Inwestora osób,
- ważne atesty i świadectwa dopuszczenia zasadniczych elementów systemu,
-karty katalogowe zasadniczych elementów systemu.

- Wszystkie prace prowadzić zgodnie z obowiązującymi przepisami BHP oraz Polskimi Normami
- Stosować wyroby stosowane w instalacjach elektrycznych dopuszczone do obrotu i powszechnego stosowania w budownictwie
- Dopuszcza się stosowanie wyrobów innych producentów niż wymienione w projekcie pod warunkiem zachowani podstawowych parametrów technicznych i użytkowych. Podanie typu urządzenia miało na celu jedynie określenie parametrów technicznych i nie narzuca producenta.

13. Informacja BIOZ

13.1. Zakres rzeczowy robót:

- Montaż systemu sygnalizacji włamania i napadu
- Montaż systemu telewizji dozorowej

13.2. Elementy zagospodarowania działki lub terenu mogące stwarzać zagrożenie bezpieczeństwa i zdrowia ludzi

- nie występują

13.3. Przewidywane zagrożenia występujące podczas realizacji następujących robót:

- prace na wysokościach
- prace na urządzeniach elektrycznych

13.4. Sposób prowadzenia instruktażu pracowników przed przystąpieniem do realizacji robót szczególnie niebezpiecznych:

- nie występuje

13.5. Osoba odpowiedzialna za instruktaż pracowników- kierownik budowy

Kierownik budowy powinien:

- zapoznać pracowników z zakresem robót oraz określić strefy szczególnie niebezpieczne
- określić zasady postępowania w celu eliminacji zagrożeń zdrowia i życia
- określić zasady postępowania w przypadku wystąpienia tych zagrożeń
- zapoznać pracowników z przepisami BHP

13.6. Środki techniczne i organizacyjne zapobiegające niebezpieczeństwom wynikającym z wykonywania robót budowlanych w strefach szczególnego zagrożenia zdrowia lub w ich sąsiedztwie:

Instalacje rozdziału energii elektrycznej na terenie budowy powinny być zaprojektowane i wykonane oraz utrzymywane i użytkowane w taki sposób, aby nie stanowiły zagrożenia pożarowego lub wybuchowego, lecz chroniły pracowników przed porażeniem prądem elektrycznym.
Roboty związane z podłączeniem, sprawdzaniem, konserwacją i naprawą instalacji i urządzeń elektrycznych mogą być wykonywane wyłącznie przez osoby posiadające odpowiednie uprawnienia.

Żurawie samojezdne, koparki i inne urządzenia ruchome, które mogą zbliżyć się na niebezpieczną odległość do w/w napowietrznych lub kablowych linii elektroenergetycznych, powinny być wyposażone w sygnalizatory napięcia.
Rozdzielnice budowlane prądu elektrycznego znajdujące się na terenie budowy należy zabezpieczyć przed dostępem osób nieupoważnionych.
Rozdzielnice powinny być usytuowane w odległości nie większej niż 50,0 m od odbiorników energii.

Przewody elektryczne zasilające urządzenia mechaniczne powinny być zabezpieczone przed uszkodzeniami mechanicznymi, a ich połączenia z urządzeniami mechanicznymi wykonane w sposób zapewniający bezpieczeństwo pracy osób obsługujących takie urządzenia.
Okresowe kontrole stanu stacjonarnych urządzeń elektrycznych pod względem bezpieczeństwa powinny być przeprowadzane, co najmniej jeden raz w miesiącu, natomiast kontrola stanu i oporności izolacji tych urządzeń, co najmniej dwa razy w roku, a ponadto:
- przed uruchomieniem urządzenia po dokonaniu zmian i napraw części elektrycznych i mechanicznych,
- przed uruchomieniem urządzenia, jeżeli urządzenie było nieczynne przez ponad miesiąc,
- przed uruchomieniem urządzenia po jego przemieszczeniu.

W przypadkach zastosowania urządzeń ochronnych różnicowoprądowych w w/w instalacjach, należy sprawdzać ich działanie każdorazowo przed przystąpieniem do pracy.
Dokonywane naprawy i przeglądy urządzeń elektrycznych powinny być odnotowywane w książce konserwacji urządzeń.

Roboty ziemne powinny być prowadzone na podstawie projektu określającego położenie instalacji i urządzeń podziemnych, mogących znaleźć się w zasięgu prowadzonych robót.
Wykonywanie robót ziemnych w bezpośrednim sąsiedztwie sieci, takich jak:
- elektroenergetyczne,
- gazowe,
- telekomunikacyjne,
- ciepłownicze,
- wodociągowe i kanalizacyjne,

powinno być poprzedzone określeniem przez kierownika budowy bezpiecznej odległości, w jakiej mogą być one wykonywane od istniejącej sieci i sposobu wykonywania tych robót.

W czasie wykonywania robót ziemnych miejsca niebezpieczne należy ogrodzić i umieścić napisy ostrzegawcze.

W czasie wykonywania wykopów w miejscach dostępnych dla osób niezatrudnionych przy tych robotach, należy wokół wykopów pozostawionych na czas zmroku i w nocy ustawić balustrady zaopatrzone w światło ostrzegawcze koloru czerwonego.
Poręcze balustrad powinny znajdować się na wysokości 1,10 m nad terenem i w odległości nie mniejszej niż 1,0 m od krawędzi wykopu.

Wykopy o ścianach pionowych nieumocnionych, bez rozparcia lub podparcia mogą być wykonywane tylko do głębokości 1,0 m w gruntach zwartych, w przypadku, gdy teren przy wykopie nie jest obciążony w pasie o szerokości równej głębokości wykopu.

Wykopy bez umocnień o głębokości większej niż 1,0 m, lecz nie większej od 2,0 m można wykonywać, jeżeli pozwalają na to wyniki badań gruntu i dokumentacja geologiczno – inżynierska.

Ruch środków transportowych obok wykopów powinien odbywać się poza granicą klina naturalnego odłamu gruntu.

W czasie wykonywania robót ziemnych nie powinno dopuszczać się do tworzenia nawisów gruntu.

Przebywanie osób pomiędzy ścianą wykopu a koparką, nawet w czasie postoju jest zabronione.

Zakładanie obudowy lub montaż rur w uprzednio wykonanym wykopie o ścianach pionowych i na głębokości powyżej 1,0 m wymaga tymczasowego zabezpieczenia osób klatkami osłonowymi lub obudową prefabrykowaną.

14. Licencja

LICENCJA
0003305
pracownika
zabezpieczenia technicznego
drugiego stopnia

wydana Panu(i) PIŁKOWSKI
Paweł
s/c Stanisława Nr PESEL 58032104515
upoważniająca do wykonywania czynności
określonych w art. 3 pkt 2 i art. 29 ust.1
ustawy z dnia 22 sierpnia 1997 r.o ochronie
osób i mienia (Dz.U.Nr 114, poz.740)

KOMENDANT WOJEWÓDZKI
POLICJI
w Białymstoku
mł. insp. mgr Jan KULESZ