**Załącznik nr 2 do OPZ**

**Tabela parametrów funkcjonalnych**

|  |
| --- |
| **CCTV**  |
| System powinien posiadać funkcjonalność integracji z pozostałymi elektronicznymi systemami zabezpieczeń w zakresie dozorowanego obszaru; |
| System powinien umożliwiać zarządzanie poprzez platformę integrującą; |
| Przesyłanie danych w systemie powinno odbywać się w trybie ciągłym za pomocą odpowiedniej infrastruktury rejestratorów nagrywających materiał lokalnie, umożliwiających zdalne zarządzanie i podgląd materiału w centrach nadzoru bezpieczeństwa (CNB); |
| Zapewnienie transmisji strumieni wideo w trybie Multicast, zapewniającym możliwość przekazywania pakietów telekomunikacyjnych IP do grupy zainteresowanych odbiorców; |
| System będzie posiadał funkcjonalność dekodowania sprzętowego strumienia z kamer wideo poprzez wykorzystanie zasobów karty graficznej stacji operatorskiej; |
| System będzie posiadał właściwość redundancji opartej np. na macierzach RAID (Redundant Array of Independent Disks); |
| System powinien posiadać redundantne serwery odpowiedzialne za zarzadzanie całością systemu w szczególności: |
| ·     kontami użytkowników, |
| ·     zdarzeniami alarmowymi, |
| ·     analitykami wideo, |
| ·     konfiguracją systemu, |
| ·     konfiguracją rejestratorów. |
| System będzie posiadał możliwość obsługi poprzez klienta mobilnego, oraz zarządzanie poprzez przeglądarkę internetową. Wspiera urządzenia mobilne iPhone & iPad, Android (od wersji V2.x ) oraz aktualne przeglądarki; |
| System powinien umożliwić wykonywanie analityk wideo na dowolnym strumieniu wideo w systemie, poprzez obliczenia wykonywane na rejestratorach; |
| System zapewniał będzie funkcjonalność polegającą na rozpoznawaniu tablic rejestracyjnych (LPR – License Plate Recognition) w oparciu o analitykę wideo; |
| System powinien posiadać centralne zarządzanie synchronizacją czasu; |
| System powinien zapewnić łączny czas zapisu ze wszystkich kamer zlokalizowanych na obiektach nie mniejszy niż 30 dni przy rejestracji w trybie ciągłym;  |
| Wybór kamery do podglądu archiwalnego przez przeciągniecie ikony kamery z mapy synoptycznej; |
| Odtwarzanie ostatnich kilkunastu sekund nagrania bezpośrednio z widoku kamery będącej aktualnie w trybie podglądu bieżącego obrazu;  |
| Wskazanie materiału blokowanego przed nadpisaniem; |
| Wybór kamery do aktualnego podglądu przez przeciągniecie ikony kamery z mapy synoptycznej; |
| Zbliżenie cyfrowe wybranego fragmentu obrazu bez utraty podglądu na pierwotny zakres obserwowanej sceny; |
| Oparty o bezpłatne licencje, lub dodatkowo płatne urządzenia tryb videowall – tworzenie wspólnej przestrzeń roboczej z monitorów wielu stacji operatorskich;  |
| Natychmiastowy dostęp do podglądu obrazu oraz do odtwarzania materiału już zarejestrowanego. |
| **SSWiN** |
| System musi być zintegrowany z systemem kontroli dostępu (SKD) oraz systemem dozorowym (CCTV); |
| System musi być zarządzany przez łatwy w użyciu interfejs graficzno – tekstowy; |
| Wszystkie zdarzenia systemowe, muszą mieć swoje odzwierciedlenie na interaktywnych mapach, wyświetlanych na monitorze operatora i powinny być zapisywane w logach zdarzeń; |
| System powinien w pełni współpracować z projektowanym rozwiązaniem (PSIM – Physical Security Information Managment) integrującym wszystkie projektowane systemy zabezpieczeń; |
| Obsługa poszczególnych stref systemu, powinna odbywać się również lokalnie z manipulatorów szyfrowych, pozwalających na uzbrajanie/rozbrajanie danej strefy, przez osobę do tego upoważnioną; |
| Instalowane urządzenia powinny być dopasowane kolorystycznie do pomieszczeń. |
| **SKD** |
| Możliwość powiązania materiału wideo ze zdarzeniami z systemu kontroli dostępu i systemu alarmowego; |
| Możliwość dowolnego konfigurowania wewnętrznych stref dostępu i stref czasowych; |
| Sterowanie elementami wykonawczymi (rygle, zwory), ze stanowiska operatora systemu;  |
| Wielopoziomowy dostęp do jego obsługi; |
| Interfejs graficzny z wizualizacją zdarzeń na mapach; |
| Powiązanie zdarzeń kontroli dostępu z nagranym materiałem w CCTV; |
| Powiązanie SKD z systemem rozpoznawania tablic rejestracyjnych LPR; |
| Wewnętrzną bazę danych, przechowywaną w kontrolerach systemu, zapewniającą niezależną pracę systemu po ewentualnej utracie komunikacji z systemem zarządzającym; |
| Zasilanie awaryjne minimum 4 godziny, obejmujące wszystkie jego elementy składowe, umożliwiając jego pracę w przypadku braku zasilania zewnętrznego; |
| Pracę w sieci TCP/IP; |
| Generowanie wydruków i raportów; |
| Zastosowanie czytników bezprzewodowych; |
| Możliwość zastosowania czytników biometrycznych; |
| Dodawanie zdjęcia użytkownika z kamery, która zostanie podłączona do systemu; |
| Dodawanie zdjęcia użytkowników z pliku; |
| Tworzenie komentarzy do zdarzeń systemowych i użytkowników; |
| Zarządzanie alarmami; |
| Możliwość projektowania kart kontroli dostępu; |
| Praca w klasie rozpoznania 2 i w klasie dostępu B z pełną rejestracją zdarzeń; |
| Praca w klasie rozpoznania 3 i w klasie dostępu B z pełną rejestracją zdarzeń; |
| Możliwość ustawienia funkcji alarmowej „wyważenie” drzwi do każdego czytnika indywidualnie;  |
| Możliwość ustawienia funkcji alarmowej w przypadku zbyt długo otwartych drzwi dla każdego czytnika indywidualnie;  |
| Możliwość ustawienia funkcji antypassback dla każdego czytnika indywidualnie; |
| Rozwiązanie plug-play, wymiana uszkodzonego kontrolera, jest automatyczna, konfiguracja pobierana jest z serwera. |
| **LPR** |
| Zapewnia 95% detekcję tablic rejestracyjnych pojazdów nieruchomych i będących w ruchu; |
| Zapewnia czas identyfikacji numerów nie krótszy niż 200 ms.; |
| Zapewnia bezpośrednią konfigurację poziomu interfejsu użytkownika; |
| Zapewnia tworzenie harmonogramów praw dostępu; |
| Zapewnia definiowanie scenariuszy działania wyzwalane wykryciem określonego numeru rejestracyjnego; |
| Pozwala na sterowanie bramami i szlabanami; |
| Zapewnia odtwarzanie odpowiednich sekwencji powiązanych z określonymi numerami rejestracyjnymi; |
| Umożliwia import oraz eksport poszeregowanych list zapisanych w systemie tablic rejestracyjnych; |
| Zapewnia archiwizacje zdjęć pojazdów w formacie JPEG; |
| Pozwala na zdalne wysyłanie informacji poprzez wiadomość email z obrazem po wykryciu określonych numerów rejestracyjnych; |
| Pozwala na przeszukiwanie danych według szczegółowych kryteriów; |
| Umożliwia odczytu wszystkich europejskich numerów rejestracyjnych; |
| Zapewnia lokalną oraz zdalną możliwość zarządzania poprzez platformę integrującą, projektowany Zintegrowany System Zarządzania Bezpieczeństwem (ZSZB). |
| **ZSZB** |
| Zarządzanie elementami sprzętowymi i logicznymi poszczególnych podsystemów; |
| Pełna wizualizacji stanu elementów sprzętowych i logicznymi poszczególnych podsystemów; |
| Konfiguracja parametrów urządzeń wchodzących w skład poszczególnych podsystemów; |
| Korelacja zdarzeń występujących w kilku podsystemach w oparciu o funkcje logiczne; |
| Współdziałanie poniższych podsystemów za pomocą interfejsów programowych: |
| ·     Kontroli Dostępu,  |
| ·     Sygnalizacji Włamania i Napadu,  |
| ·     Monitoringu Wizyjnego CCTV IP,  |
| ·     Interkomowego SOS/INFO,  |
| ·     Rejestracji Czasu Pracy, |
| ·     Monitoringu środowiskowego, |
| ·     Obsługi gości. |
| Integrację systemów zewnętrznych: |
| ·     Systemu Dystrybucji Kluczy, |
| ·     Systemu Kontroli Wartowników, |
| ·     Sygnalizacji Pożarowej, |
| ·     Automatyki. |
| Oparty na strukturze sieci IP z centralnym serwerem oraz rozproszoną strukturą elementów sterujących, wykorzystującą standardowe łącza okablowania strukturalnego, zarówno miedzianego jak i światłowodowego; |
| Oparta na technologii Web i umożliwiać dostęp użytkownikom do interfejsu systemu za pomocą przeglądarek internetowych; |
| Inteligencja systemu rozproszona do poziomu lokalnych sterowników; |
| Moduły pamięci pozwalające na buforowanie transakcji w przypadku braku komunikacji z serwerem centralnym; |
| Umożliwia dodanie do systemu co najmniej 2 000 użytkowników przypisanych do odpowiedniej grupy użytkowników; |
| Pozwala na zapisanie w systemie co najmniej 7 000 000 zdarzeń; |
| Umożliwia dodanie co najmniej 3200 map synoptycznych ; |
| Umożliwia dodanie co najmniej 32 000 obiektów; |
| Umożliwia podłączenie co najmniej 64 jednocześnie zalogowanych operatorów; |
| Horyzontalny podział bazy danych w ramach jednego serwera na kilka odseparowanych od siebie części logicznych; |
| Operator będzie miał dostęp do zdarzeń, map synoptycznych i użytkowników tylko w zakresie ograniczonej części chronionego obiektu; |
| Zarządzanie uprawnieniami i personalizacja stanowiska pracy musi być przypisywana poszczególnym profilom użytkownika; |
| Wbudowana mapa synoptyczna (wizualizacja) za pomocą, której będzie istnieć możliwość pełnej wizualizacji stanu i zarządzania wszystkimi podsystemami. |
| Funkcje, które muszą być realizowane przez system wizualizacji: |
| ·     System Kontroli dostępu – wizualizacja stanów czytnika, kontaktronu, elektrorygla i wszystkich elementów dodatkowych. Po kliknięciu ikony czytnika powinna zostać wyjustowana lista wyboru trybów pracy czytnika (m.in. stan otwarty, stan normalny, stan z potwierdzeniem operatora), |
| ·     System Sygnalizacji Włamania i Napadu – wizualizacja stanów poszczególnych elementów detekcyjnych (np. czujek ruchu PIR). Zazbrajanie i rozbrajanie poszczególnych stref SSWiN, |
| ·     System Monitoringu wizyjnego – kliknięcie ikony kamery ma spowodować wyświetlenie obrazu z danej kamery. Dla kamer PTZ, pełna możliwość sterowania kamerą z poziomu mapy synoptycznej. Możliwość umiejscowienia na mapie synoptycznej przycisków, wymuszających obrót kamery PTZ w konkretne miejsce (preset). |
| Mapa synoptyczna musi wspierać system widgetów, który umożliwia umieszczenie na niej dowolnych elementów w tym: |
| ·     listę osób znajdujących się w danej strefie kontroli dostępu, |
| ·     wykresy zawierające liczby osób przechodzących przez dane przejście, |
| ·     listę stref SSWiN z informacją o ich stanie, umożliwiającą zazbrajanie i rozbrajanie poszczególnych stref, |
| ·     skróty do konkretnych pozycji w menu, szczególnie często używanych przez operatora, |
| ·     listę urządzeń z informacją o ich stanie połączenia z serwerem. |
| Zarządzanie platformą CCTV z poziomu ZSZB: |
| ·     aktywacja predefiniowanych ustawień kamer obrotowych kamer PTZ w wyniku otrzymania przez system ZSZB informacji alarmowej z systemu SSWiN, KD lub innych, |
| ·     zdalne kontrolowanie funkcji PTZ z poziomu mapy synoptycznej systemu, |
| ·     generowanie zdarzeń w bazie danych systemu ZSZB z przypisaniem powiązanego obrazu, |
| ·     import zdarzeń będących wynikiem działania algorytmów analizy obrazu, |
| ·     podgląd obrazu z kamer CCTV w trybie "na żywo", |
| ·     odtwarzanie fragmentu zapisanego materiału wideo, przypisanego do konkretnego, odnotowanego zdarzenia w systemie, |
| ·     sterowanie kamerami PTZ (Pan Tilt Zoom) z poziomu wizualizacji, przy pomocy myszki. |
| Zarządzanie platformą KD z poziomu ZSZB: |
| ·     otwarcie/zamknięcie przejścia objętego systemem KD, z poziomu mapy synoptycznej przy pomocy myszki, |
| ·     rozbrajanie/zazbrajanie stref objętych jednocześnie systemem SSWiN oraz KD,  |
| ·     nadawanie/edycja uprawnień dla wszystkich/wybranych użytkowników systemu KD, |
| ·     wprowadzanie nowych użytkowników, |
| ·     edycja i wydruk kart użytkowników wraz z przygotowanymi informacjami oraz ze zdjęciem , przy pomocy drukarki termosublimacyjnej i preintstalowanego modułu programowego, |
| ·     przygotowanie/edycja harmonogramu pracy systemu KD (kalendarz), |
| ·     nadanie wybranym użytkownikom znacznika "osoba upośledzona ruchowo", umożliwi wydłużenie czasu otwarcia przejścia, |
| ·     generowanie szczegółowych raportów użytkownika,  |
| ·     pełna edycja uprawnień przypisanych do każdego użytkownika systemu KD, |
| ·     konfiguracja systemu śluzowości dla wybranych przejść objętych kontrolą dostępu, |
| ·     wprowadzenia numerów tablic rejestracyjnych ze integrowanego systemu CCTV, jako wirtualnych kart KD,  |
| ·     ustawienie funkcji alarmowej „wyważenie” drzwi do każdego czytnika indywidualnie,  |
| ·     ustawienie funkcji alarmowej w przypadku zbyt długo otwartych drzwi dla każdego czytnika indywidualnie,  |
| ·     ustawienie funkcji antypassback dla każdego czytnika indywidualnie, |
| ·     konfiguracja kodów PIN dla czytników wyposażonych w klawiaturę PIN. |
| Odtwarzanie fragmentów nagrań zawierających zdarzenie zawierające odczyt tablicy rejestracyjnej w LPR bezpośrednio z poziomu ZSZB; |
| Zarządzania elementami sprzętowymi systemów podrzędnych: |
| ·     otwarcie/zamknięcie przejścia/szlabanu/furty objętego systemem KD, z poziomu mapy synoptycznej przy pomocy myszki, |
| ·     wysterowanie kamery PTZ z poziomu mapy synoptycznej ZSZB, |
| ·     rozbrajanie/zazbrajanie stref objętych systemem SSWiN. |
| Wizualizacja stanu elementów sprzętowych i logicznych: |
| ·     pokazanie na mapach synoptycznych ZSZB za pomocą widgetów (ikon), aktualnego stanu urządzeń, np. czytnika KD, Kontaktronu, czujki Pir, Kamery, |
| ·     pokazanie na mapach synoptycznych ZSZB za pomocą widgetów (ikon), lub zaznaczonych dowolnym kolorem stref - stanu tych stref, np. zazbrojona/rozbrojona strefa SSWiN; stan alarmowy,  |
| ·     sygnalizacja graficzna, na mapie synoptycznej, zaniku sygnału wizyjnego z podłączonych do ZSZB kamer. |
| Otwarty interfejs umożliwiający przyszłą integrację z systemami automatyki; |
| Pojawienie się okna dialogowego z podpowiedziami procedur postępowania dla obsługi systemu , w przypadku pojawienia się, konkretnego zdarzenia/alarmu w systemie;  |
| Możliwość wprowadzenie numerów tablic rejestracyjnych ze integrowanego systemu ZSZB jako wirtualnych kart i nadawania im uprawnień dla przejść. |