OPISU ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO

|  |  |
| --- | --- |
| **Tytuł projektu** | **BUDOWA CHMURY OBLICZENIOWEJ POLICJI JAKO INKUBATORA INNOWACYJNOŚCI I BEZPIECZEŃSTWA** |
| **Wnioskodawca** | Minister Spraw Wewnętrznych i Administracji |
| **Beneficjent** | **Komendant Główny Policji**Puławska 148/150, 02-624 WarszawaLider projektu odpowiedzialny za przeprowadzenie całości projektu, przygotowanie całości koncepcji i architektury systemu w tym identyfikacja elementów zależnych oraz wdrożenie nowych usług. |
| **Partnerzy** | **Ministerstwo Cyfryzacji**Królewska 27, 00-060 WarszawaDostarczenie systemów zależnych, wsparcie merytoryczne projektu w zakresie formalnym, technologii i rozwiązań.**Komenda Główna Państwowej Straży Pożarnej** ul. Podchorążych 38, 00-463 Warszawa**Lotnicze Pogotowie Ratunkowe**ul. Księżycowa 5, 01-934 Warszawa. |
| **Źródło finansowania** | Wszystkie wydatki kwalifikowane w 84,63% zostaną pokryte ze środków UE, a pozostałe 15,37% zostanie zagwarantowane ze środków budżetu państwa.Działanie 2.1 „Wysoka dostępność i jakość e-usług publicznych”typ II Tworzenie lub rozwój e-usług wewnątrzadministracyjnych (A2A) niezbędnych dla funkcjonowania e-usług publicznych (A2B, A2C)Finansowanie planowane jest z 42 części budżetowej, zgodnie z §1 rozporządzenia Ministra Finansów z dnia 4 grudnia 2009 r. *w sprawie klasyfikacji części budżetowej oraz określenia ich dysponentów* (Dz. U. z 2018 r. poz. 1177, z późn. zm.). |
| **Całkowity koszt projektu** | 95 mln PLN brutto |
| Planowany okres realizacji projektu | 08-2019 do 08-2022 |
| Osoba kontaktowa | Andrzej Pastuszka | andrzej.pastuszka@policja.gov.pl | +48 22 60 137 39 |

# POWODY PODJĘCIA PROJEKTU

Każda organizacja narażona jest na wiele zagrożeń, obejmujących swoim obszarem infrastrukturę teleinformatyczną, na której posadowione są systemy krytyczne lub systemy wspierające realizację procesów kluczowych. Ochrona obywateli oraz utrzymywanie bezpieczeństwa i porządku publicznego, należy do ustawowych zadań Policji.

Istnieje społeczna konieczność realizacji projektu, ponieważ w sposób bezpośredni odpowiada on na artykułowane przez obywateli jak i funkcjonariuszy Policji problemy i potrzeby. Dotyczy to przede wszystkim: podniesienia skuteczności i efektywności wykrywania sprawców przestępstw i wykroczeń, szczególnie drobnych najbardziej uciążliwych dla obywateli oraz ujawniania ich z wykorzystaniem środków technicznych.

Podczas przeprowadzonego na zlecenie Ministerstwa Cyfryzacji w marcu 2017 r. badania „mDokumenty – identyfikacja postaw, potrzeb i opinii obywateli” zidentyfikowano potrzebę wprowadzenia możliwości skorzystania z e-usługi będącej alternatywą dla tradycyjnego okazywania dokumentu tożsamości. Zaproponowane podejście nie zastępuje dokumentów tradycyjnych oraz nie umniejsza ich roli, jednak posiada istotną wartość, która umożliwia uzupełnienie wypowiedzi ustnej osoby (w przypadku, gdy nie dysponuje dokumentami), wobec której funkcjonariusz podejmuje czynności, a w przypadku osób z zaburzeniami głosu i mowy, wręcz pozwalając na kontakt i ustalenie tożsamości, co może być czynnikiem wymaganym do sprawnego udzielenia pomocy. Zdecydowana większość badanych (67 proc.) uznała, że w Polsce warto wdrożyć takie rozwiązanie.

W czasie aktualnie definiowanych zagrożeń hybrydowych, będących poważnym wyzwaniem dla systemu cyberbezpieczeństwa, ochrona obywateli oraz utrzymywanie bezpieczeństwa i porządku publicznego stawia szczególne wyzwania dla Policji i administracji publicznej. Zapewnienie niezagrożonego funkcjonowania kraju w przestrzeni informacyjnej, z uwzględnieniem bezpieczeństwa informacyjnego struktur państwowych (zwłaszcza administracji publicznej i służb porządku publicznego) jest celem strategicznym państwa. Projekt "Budowa chmury obliczeniowej Policji jako inkubatora innowacyjności i  bezpieczeństwa" bezpośrednio wynika z konieczności tworzenia i optymalizacji funkcjonowania stosownych, fizycznych elementów systemu informatycznego. Proponowane rozwiązania, prywatnej chmury obliczeniowej z usługą Disaster Recovery Center w rzeczywisty sposób wpłynie na poprawę bezpieczeństwa systemów wykorzystywanych przez Policję oraz służby odpowiedzialne za utrzymywanie bezpieczeństwa i porządku publicznego.

## Identyfikacja problemu i potrzeb

Policja w ramach ustawowych zadań odpowiada za ochronę bezpieczeństwa i porządku publicznego. W związku z nałożonymi obowiązkami w systemie bezpieczeństwa państwa spełnia szczególną rolę. Usprawnienie jej struktury organizacyjnej, wykonywanie działań przy użyciu nowoczesnych metod i środków, profesjonalna obsada kadrowa, przejrzystość przepisów prawnych czy wreszcie współpraca Policji z podmiotami zewnętrznymi ma ogromny wpływ na realizację jej ustawowych zadań związanych ze wspomnianym zapewnieniem bezpieczeństwa i porządku publicznego państwa. W obecnych czasach, elementem silnie wspomagającym skuteczną i efektywną pracę Policji są technologie informacyjno - komunikacyjne. Dzięki wykorzystaniu rozwiązań teleinformatycznych w działaniach realizowanych dotychczas w tradycyjny sposób możliwe jest skuteczne gromadzenie, analiza oraz definiowanie kierunków działania Policji, a tym samym skuteczne dbanie o bezpieczeństwo obywateli.

Główne braki w zakresie aktualnie posiadanej infrastruktury i rozwiązań programowych to:

* brak rozwiązań umożliwiających automatyzację procesu weryfikacji tożsamości. Czasochłonne uzupełnianie odpowiednich pól w aplikacji stosowanej w terminalach mobilnych jest uciążliwe dla osób legitymowanych, jak i dla funkcjonariuszy;
* brak posiadania i wykorzystywania przez Policję powszechnie stosowanych systemów do przetwarzania i szeroko rozumianej analizy obrazów cyfrowych, do rozpoznawania sytuacji i zachowań będących w zainteresowaniu służb porządku publicznego w celu przeciwdziałania powstawaniu negatywnych zdarzeń w przestrzeni publicznej;
* brak usługi Disaster Recovery Center – dla systemów newralgicznych dla bezpieczeństwa i porządku publicznego (SWD Policji, SWD Państwowej Straży Pożarnej i SWD Państwowego Ratownictw Medycznego), która zapewniałaby odpowiedni poziom bezpieczeństwa jest rzeczywistym zagrożeniem. Mając na uwadze nieustany rozwój technologiczny, systemy bezpieczeństwa wymagają ciągłego skanowania wszystkich portów, natychmiastowego rozpoznawania każdego typu ataków czy wykrywania anomalii. Budowa prywatnej chmury obliczeniowej z modułem Disaster Recovery Center pozwoli na zastosowanie najnowocześniejszych rozwiązań w zakresie ochrony w tym odseparowanie i szyfrowanie danych, wieloczynnikowe uwierzytelnianie. Sprzęt, monitory instancji wirtualnych i systemy operacyjne zostaną objęte systemem zaawansowanych zabezpieczeń na wyższych poziomach zabezpieczeń w stosunku do aktualnych rozwiązań.

W ramach zniwelowania wymienionych powyżej deficytów zakłada się budowę/modernizację:

* usługi automatycznego transferu danych wymaganych do ustalenia tożsamości przez Policję z aplikacji mObywatel, wizualizującej dane osobowe obywatela. Umożliwi ona automatyzację procesu uzupełnienia danych w obowiązkowych polach na formularzach dostępnych w aplikacji stosowanej na terminalach mobilnych, które są konieczne do weryfikacji tożsamości i posiadanych uprawnień. Funkcjonariusz wykorzystując mobilny terminal, zaczyta np. z okazanego przez obywatela dokumentu alfanumeryczny, dwuwymiarowy kod graficzny (QR-kod);
* stworzenie systemu wspomagającego gromadzenie, przetwarzanie w tym zaawansowaną analizę i wykorzystanie w codziennej służbie materiałów wizualnych w postaci cyfrowej.

Działanie systemu powinno skupiać się w następujących obszarach:

1) Szybka identyfikacja osób i ujawnionych zwłok ludzkich na podstawie ich wizerunków lub/i tatuaży na ciele w tym:

a) osób legitymowanych

b) osób o nieustalonej tożsamości

c) ujawnionych zwłok ludzkich

d) osób obserwowanych w ramach czynności operacyjno-rozpoznawczych

2) Analiza materiałów foto i wideo w trybie offline (post factum) pochodzących z różnych źródeł w tym:

a) szeroko rozumiana analiza materiałów foto i wideo (indeksacja i korekta materiału, jego skracanie, wybór elementów będących w zainteresowaniu, stosowanie filtrów itp.)

b) ręczna i automatyczna detekcja obiektów na zaindeksowanym materiale

3) Analiza materiałów foto i wideo w trybie online w tym:

a) Automatyczna detekcja i identyfikacja obiektów na przekazie onlinie

4) Porównywanie i typowanie obiektów celem ich identyfikacji w tym:

a) porównywanie wykrytych obiektów ze zbiorem referencyjnym

b) porównywanie wykrytych obiektów z wizerunkami innych niezidentyfikowanych obiektów

c) typowanie obiektów w oparciu o ich wizerunek, portret pamięciowy, tatuaż, numer w tym numer rejestracyjny, napis lub znak graficzny na nich występujący

d) porównywanie wykrytych obiektów z wizerunkami osób będących w zainteresowaniu Policji

5) Stosowanie analizy kryminalnej w oparciu o:

a) utworzone relacje między obiektami w tym obiektami niezidentyfikowanymi

b) informacje o danym obiekcie oraz czasie i miejscu jego rejestracji

6) Przeszukiwanie sieci Internet w celu poszerzenia wiedzy o obiekcie lub/i jego identyfikacji

-

Można stwierdzić, że posiadanie i wykorzystanie w czynnościach służbowych takiego systemu stanowiłoby prawdziwy przełom w pracy Policji. W znaczny sposób przyczyniłoby się to do przyspieszenia, ułatwienia i zwiększenia skuteczności podejmowanych działań. Pozwoliłoby również na wydajniejsze i skuteczniejsze wykorzystanie posiadanych sił i środków służby prewencyjnej, kryminalnej jak i śledczej.

* posiadanej infrastruktury teleinformatycznej, na której posadowione są systemy krytyczne lub systemy wspierające realizację procesów kluczowych;
* sieci teleinformatycznej OST112 ukierunkowaną na niezakłóconą i bezpieczną wymianę danych pomiędzy systemami IT wykorzystywanymi przez funkcjonariuszy Policji z terenu całego kraju.

|  |  |  |
| --- | --- | --- |
| **Interesariusz** | **Zidentyfikowany problem** | **Szacowana wielkość grupy** |
| Obywatele  | Przy realizacji codziennych zadań funkcjonariusze Policji realizując swoje podstawowe uprawnienie jakim jest legitymowanie są zmuszeni do czasochłonnego uzupełniania odpowiednich pól w aplikacji stosowanej w terminalach mobilnych. Jest to uciążliwe dla osób legitymowanych.  | Każdego dnia średnio 1100 funkcjonariuszy wykonuje ok. 28500 legitymowań. Z uwagi na powyższe można stwierdzić, że ok. 28 tys. obywateli dziennie odczuje poprawę sprawności działania służb. |
| Obywatele | Brak usługi bieżącego raportowania stanu bezpieczeństwa przestrzeni publicznej. | Każda zainteresowana osoba, mająca dostęp do sieci Internet. |
| Służby porządku publicznego  | Aktualnie służby porządku publicznego nie posiadają narzędzi do przetwarzania szeroko rozumianej analizy obrazów cyfrowych, do rozpoznawanie sytuacji i zachowań będących w ich zainteresowaniu.  | Społeczeństwo, poprzez doposażenie organów państwowych posiadających określone uprawnienia i obowiązki, we współczesne narzędzia analizy audio/wideo umożliwiające podjęcie działań zmierzających do wykrycia i ujawnienia przestępstw, osądzenia przestępców i wykonania wyroków. |
| Służby porządku publicznego | Zapewnienie niezagrożonego funkcjonowania kraju w przestrzeni informacyjnej, z uwzględnieniem bezpieczeństwa informacyjnego struktur państwowych. Brak usługi Disaster Recovery Center – dla newralgicznych systemów dla bezpieczeństwa i porządku publicznego (SWD Policji, SWD PSP i SWD PRM).  | Społeczeństwo, poprzez poprawienie bezpieczeństwa przetwarzania i gromadzenia danych wykorzystywanych w systemach obsługujących zgłoszenia alarmowe.  |

## Opis stanu obecnego

Obecnie brak jest rozwiązań umożliwiających automatyzację procesu weryfikacji tożsamości i posiadanych uprawnień. W ramach codziennych rutynowych czynności podejmowanych przez funkcjonariuszy Policji, niezbędne jest czasochłonne uzupełnianie odpowiednich pól w aplikacji stosowanych w terminalach mobilnych. Wykonywanie tych czynności jest niekomfortowe dla osób wobec których są podejmowane działania ze strony Policji, ale również dla funkcjonariuszy. Należy pamiętać, że przedmiotowe zadania są wykonywane w różnych warunkach atmosferycznych, przez całą dobę.

W odczuciu społeczeństwa zarejestrowanie sprawcy zdarzenia i przesłanie jego obrazu do jednostki Policji jest wystarczające do tego by doprowadzić do jego ustalenia, zatrzymania i ukarania. Posiadanie zarejestrowanego obrazu cyfrowego nie jest jednak tożsame z identyfikacją obiektów na nim się znajdujących. W przypadku zdarzeń drogowych podjęcie czynności jest możliwe już po odczytaniu numeru rejestracyjnego pojazdu, jednak nie skutkuje to automatyczną identyfikacją sprawcy nawet w przypadku nagrania jego wizerunku. Takie problemy związane z analizą zarejestrowanych danych cyfrowych pojawiają się nie tylko w przypadku zdarzeń drogowych.

Analogiczna sytuacja występuje w przypadku zarejestrowania przez monitoring sklepowy osoby dokonującej kradzieży lub kamery umieszczonej w bankomacie rejestrującej osobę montującą nakładkę do skanowania kart płatniczych. W sytuacji, gdy sprawca oddala się z miejsca zdarzenia często jedynym śladem potencjalnie umożliwiającym ustalenie jego tożsamości jest zarejestrowany obraz jego wizerunku. Gdy policjanci z jednostki prowadzącej sprawę nie zidentyfikują sprawcy zdarzenia, a ogłoszenie w mediach czy na stronie internetowej jednostki Policji oraz inne działania nie doprowadzą do ustalenia sprawcy, sprawę umarza się z braku możliwości wykrywczych.

Osobnym złożonym problemem jest analiza zarejestrowanego materiału w przypadku zdarzeń, w których bierze udział wiele osób. Podczas zakłócania porządku przez dużą grupę osób np. na stadionie, czy podczas demonstracji występowanie dziesiątek, setek a czasami nawet tysięcy osób na jednym materiale w znacznym stopniu ogranicza możliwości identyfikacji poszczególnych osób. W przypadku nagrań trwających wiele minut ustalenie zachowania tej samej osoby lub wielu osób w tłumie na przestrzeni wielu minut, zmieniających swoje położenie a czasem i elementy ubioru jest bardzo trudne lub wręcz często niemożliwe.

Kolejnym z problemów jest analiza wielogodzinnych nagrań zabezpieczonych materiałów wideo. Przeglądanie materiału wideo w celu zaobserwowania konkretnego zdarzenia, jakim jest np. przejście osoby przez kadr, wymusza często konieczność wielogodzinnej obserwacji. Przeglądanie materiału z nagrania zarejestrowanego w nocy, kiedy przez wiele godzin kamera nie rejestruje żadnego zdarzenia i wychwycenie na nim kilku sekundowego ujęcia jest dla oglądającego bardzo trudne. Wynika to ze zmęczenia i znużenia operatora przeglądającego tak długi materiał. Sprawa jest jeszcze trudniejsza, gdy do przejrzenia jest wielogodzinny materiał z kilku kamer, których tzw. pola widzenia nie nakładają się na siebie.

W przypadku analizy nawet niedługich nagrań brak jest narzędzi, a zarazem możliwości indeksowania zarejestrowanego materiału pozwalającego następnie na filtrowanie występujących na nim obiektów, kierunku ich poruszania, trasy przejazdu lub przemarszu, czasu, w jakim pojawiają się w kadrze, ich zachowania. Możliwość użycia wielu filtrów i nałożenie ich na siebie w celu wybrania tylko interesujących informacji z całego pakietu zarejestrowanych danych znacznie przyspieszyłoby wykonywanie czynności związanych z analizą tak obszernego materiału. Brak takich narzędzi skutkuje koniecznością przeglądania całości nagrania wideo oraz ograniczeń postrzegania i identyfikacji wynikających z percepcji operatora.

Wdrażane aktualnie na wyposażenie Policji kamery nasobne dla policjantów poza rejestracją czynności prowadzonych przez policjanta, nie przynoszą dodatkowej wartości pozwalającej na analizę zarejestrowanych danych. W sytuacji, kiedy sprawca zdarzenia został nagrany przez kamerę policjanta, a następnie zbiegł z miejsca zdarzenia pojawia się wyżej opisywany problem z jego identyfikacją. Gromadzenie olbrzymich ilości danych pochodzących z nagrań kamer nasobnych (aktualnie jest wykorzystywane ok 2 tys. sztuk docelowo zgłaszane zapotrzebowanie to ok. 15 tys. sztuk w okresie trzech lat) nie przekłada się na możliwości dodatkowego efektywnego wykorzystania danych jakie rejestrują.

Kolejnym czynnikiem zmniejszającym skuteczne działanie Policji, związanym z wykorzystaniem technik foto i wideo jest brak możliwości bieżącej identyfikacji osób podczas imprez masowych ze szczególnym uwzględnieniem imprez podwyższonego ryzyka. Obecnie przed lub w czasie trwania imprezy nie ma możliwości technicznych na identyfikację osób posiadających zakaz wstępu na imprezę masową, a w wyniku tego ich odizolowania od innych uczestników tej imprezy.

Osobnym aspektem jest brak możliwości identyfikacji obserwowanych lub zarejestrowanych w danym miejscu osób podczas wykonywania czynności operacyjno- rozpoznawczych.

Kolejnym problemem, z jakim spotykają się policjanci jest brak możliwości typowana sprawców na podstawie wykonanych portretów pamięciowych. Zaawansowane techniki umożliwiające obecnie wykonywanie bardzo realistycznych portretów pamięciowych przez biegłych z zakresu antropometrii z Laboratorium Kryminalistycznego Komendy Wojewódzkiej/Stołecznej Policji (LK KWP/KSP) i CLKP stanowią potencjalnie doskonały materiał do skutecznego typowania sprawców przestępstw. Analogicznie jak w innych przypadkach brak jest narzędzi pozwalających na automatyzację tego procesu. Skutkuje to zaangażowaniem wyspecjalizowanych sił i środków po stronie Policji z ograniczoną szansą na pozytywny efekt w postaci identyfikacji sprawcy.

Projekt "Budowa chmury obliczeniowej Policji jako inkubatora innowacyjności i bezpieczeństwa" bezpośrednio wynika z konieczności tworzenia i optymalizacji funkcjonowania stosownych fizycznych elementów systemu bezpieczeństwa. Policja narażona jest na wiele różnych zagrożeń obejmujących swoim obszarem posiadaną infrastrukturę teleinformatyczną, na której posadowione są systemy krytyczne lub systemy wspierające realizację procesów kluczowych. W jej posiadaniu są narzędzia mogące zapobiec wystąpieniu awarii systemu, zminimalizowaniu skutków oraz powrotu do stanu poprzedniego. Brak jest jednak usługi Disaster Recovery Center – dla systemu SWD Policji, która zapewniałaby odpowiedni poziom bezpieczeństwa. W ramach współpracy międzyresortowej przygotowana infrastruktura będzie też wykorzystana dla poprawy bezpieczeństwa systemów SWD Państwowej Straży Pożarnej i SWD Państwowego Ratownictwa Medycznego.

W ostatnich latach na rynku IT odnotowywany jest gwałtowny wzrost wykorzystania chmur obliczeniowych (ang. cloud computing). Duże korporacje, ale też średni i mały biznes korzystają z usług chmur w zakresie: gromadzenia danych, oprogramowania lub mocy obliczeniowej. Wpływa to na poprawę bezpieczeństwa oraz daje możliwość bez konieczności inwestowania w sprzęt, skorzystania z maksymalnej mocy obliczeniowych i pojemności baz danych w przypadku szczególnych potrzeb. Z uwagi na to, że liczba wdrożeń tego typu rozwiązań (wirtualne systemy operacyjne, programy online np. do edycji tekstu, arkusze kalkulacyjne, bazy danych) rośnie lawinowo, analitycy IT przewidują ograniczenie dostępności rozwiązań stacjonarnych instalowanych w infrastrukturze firmowej. Policja, z uwagi na rodzaj gromadzonych danych, nie może korzystać z rozwiązań dostępnych w chmurach publicznych. Z uwagi na powyższe, realizacja projektu „Budowa chmury obliczeniowej Policji jako inkubatora innowacyjności i bezpieczeństwa" w bieżącej rzeczywistości jest konieczna. W sposób bezpośredni przyczyni się do poprawy bezpieczeństwa przetwarzanych danych. Ma to szczególne znaczenie przy aktualnie definiowanych zagrożeniach hybrydowych, które są poważnym wyzwaniem dla systemu cyberbezpieczeństwa.

# EFEKTY PROJEKTU

## Cele i korzyści wynikające z projektu

Celem projektu jest zwiększenie skuteczności i efektywności zwalczania przestępczości, wykroczeń, rozpoznawania negatywnych sytuacji i zachowań oraz zdarzeń w przestrzeni publicznej. Realizacja rozwiązania w postaci prywatnej chmury obliczeniowej dla wybranych systemów centralnych Policji z przyjętymi standardami umożliwiającymi udostępnienie jej zasobów innym podmiotom administracji publicznej, pozwoli na aktywne dostosowywanie się do warunków i aktualnych zagrożeń w dynamicznie zmieniającej się rzeczywistości i związanego z tym trudnego do zdefiniowania zagrożenia cyberbezpieczeństwa Państwa. Projekt wpisuje się w Strategię na rzecz Odpowiedzialnego Rozwoju w obszarze e-państwo – „Budowa i rozwój e-administracji - orientacja administracji państwa na usługi cyfrowe”. Zintegrowanie infrastruktury przetwarzania danych e‑administracji i rozwój Systemu Rejestrów Państwowych (SRP). Produktami projektu będą udostępnione e-usługi publiczne dedykowane dla obywateli w kontaktach z Policją. Usługa automatycznego transferu danych wymaganych do ustalenia tożsamości przez Policję z aplikacji mObywatel, wizualizującej dane osobowe obywatela. Umożliwi ona automatyzację procesu uzupełnienia danych w obowiązkowych polach na formularzach dostępnych w aplikacji stosowanej na terminalach mobilnych, które są konieczne do weryfikacji tożsamości i posiadanych uprawnień. Funkcjonariusz wykorzystując mobilny terminal, zaczyta np. z okazanego przez obywatela dokumentu alfanumeryczny, dwuwymiarowy kod graficzny (QR-kod).

Dzięki systemowi i przygotowanej platformie zostanie dla obywateli wprowadzona usługa wizualizacji i publikowania raportów o stanie bezpieczeństwa przestrzeni publicznej. Udostępnianie danych obywatelom, dla informacji z odniesieniami przestrzennymi będzie możliwe z wykorzystaniem interaktywnych map cyfrowych. Nowoczesne rozwiązania mogą zapewnić infrastrukturę dla nowych projektów, których realizacja aktualnie nie byłaby możliwa, np. bieżąca kontrola dostępności ciągów komunikacyjnych według danych systemu monitoringu co jest istotne w przypadku działań ratowniczych podejmowanych przez służby Ministerstwa Spraw Wewnętrzych i Administracji, Ministerstwa Zdrowia czy też Ministerstwa Sprawiedliwości. Dostęp do przygotowanej platformy będzie miał charakter ponadresortowy, jego celem jest zapewnienie odpowiednich warunków do współpracy, efektywnej wymiany danych oraz udostępniania informacji przy zapewnieniu odpowiedniego poziomu bezpieczeństwa. Realizacja projektu docelowo ma umożliwić świadczenie w optymalny sposób e-usług dla obywateli przez podmioty publiczne wchodzące w skład administracji rządowej.

Usługi oparte na innowacyjnych technologiach informatyczno-analitycznych, umożliwiać będą korzystanie z  materiałów wideo/audio gromadzonych na podstawie odrębnych przepisów, a także poprzez wykorzystanie Systemu Poszukiwawczego Policji, który będzie umożliwiał sprawdzenia danych osób i pojazdów oraz danych z wszystkich innych systemów informacyjnych udostępnionych dla potrzeb Policji. Na etapie projektu, który w oparciu prywatną chmurę obliczeniową, zakłada dużą skalowalność i możliwość rozbudowy nie jest możliwe wskazanie całego potencjału jaki można będzie dzięki niemu realizować. W stanie początkowym będą to w szczególności:

– System do automatycznej analizy obrazów cyfrowych, do rozpoznawania sytuacji i zachowań będących w zainteresowaniu służb porządku publicznego w celu przeciwdziałania powstawaniu negatywnych zdarzeń w przestrzeni publicznej w zakresie detekcji:

* + wizerunku osób poszukiwanych w ramach działania Child Alert,
	+ numerów tablic rejestracyjnych (obszary wyłączone z ruchu, obszary dostępne dla określonych podmiotów czy osób, optymalizacja działań po ogłoszeniu alarmu Child Alert, wsparcie dla odzyskiwania pojazdów utraconych, definicja pojazdów pozostających w zainteresowaniu służb, weryfikacja w zbiorach),
	+ traffic (kolizje, wypadki, utrudnienia w ruchu, informacja o ruchu transportu publicznego itp.),
	+ przyczyn (wyszukiwanie zdarzenia inicjującego na osi czasu).
	+ kodów ADR (monitorowanie przemieszczania się pojazdów przewożących ładunki niebezpieczne),
	+ liczba uczestników imprez masowych, zgromadzeń publicznych,
* niebezpiecznych zachowań w trakcie imprez masowych w tym na obiektach sportowych,
* treści transparentów w trakcie imprez masowych czy zgromadzeń publicznych.

– Infrastruktura do gromadzenia i przetwarzania oraz przygotowania materiału dowodowego dla potrzeb postępowań prowadzonych w trybie kodeksu wykroczeń czy kodeksu postępowania karnego w tym:

* + - przygotowanie analiz stanu bezpieczeństwa,
		- typowanie obszarów zagrożonych,
		- typowanie miejsc budowy/posadowienia stacjonarnych punktów monitoringu (punkty kamerowe).

– Disaster Recovery Center – dla systemów należących do Policji oraz partnerów projektu (SWD Policji, SWD PSP i SWD PRM), która zapewniałaby odpowiedni poziom bezpieczeństwa.

Na aktualnym etapie rozwoju współczesnych narzędzi informatycznych infrastruktura prywatnej chmury obliczeniowej jest niezbędna dla wytworzenia, wdrożenia i funkcjonowania e-usług publicznych. W ramach tego projektu zostaną zastosowane rozwiązania oraz usługi wykorzystujące wirtualizację środowisk sprzętowych i aplikacyjnych, umożliwiające docelowo ich integrację w ramach prywatnej chmury obliczeniowej całej administracji publicznej. Projekt nie wprowadza w swym założeniu jedynie usług A2C lub A2B, ale tworzy dla nich warunki, m.in. dzięki modernizacji, zapewnieniu interoperacyjności oraz rzeczywistej poprawy bezpieczeństwa systemów teleinformatycznych gromadzących i przetwarzających dane wrażliwe, które nie mogą być dostępne w sieci Internet. W ramach projektów realizowane będą również szkolenia podnoszące kompetencje pracowników obsługujących usługi świadczone drogą elektroniczną, z akcentem na bezpieczeństwo teleinformatycznego systemów i przechowywanych danych.

|  |  |
| --- | --- |
| **Cel** | Poprawa efektywności służb w zapewnieniu bezpieczeństwa obywatelom, poprzez budowę infrastruktury dostosowanej do aktualnych wymagań współczesnych narzędzi informatycznych i udostępnienie e-usług publicznych dedykowanych dla obywateli |
| **Cel strategiczny** | 1. Zgodny z założeniami Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 przyjętego uchwała Rady Ministrów z dnia 8 stycznia 2014 r. i zaakceptowanego w dniu 5 grudnia 2014 r. przez Komisję Europejską, w szczególności z pkt. 2.2 dotyczącym Celu szczegółowego tj. Podniesienie dostępności i jakości e-usług publicznych.2. Zgodny z Priorytetami Komendanta Głównego Policji na lata 2016 – 2018 (których okres obowiązywania został przedłużony do 2020 r.)tj.:* Wzrost skuteczności działań policji w zwalczaniu przestępczości najbardziej uciążliwej społecznie.
* Działania Policji ukierunkowane na poprawę bezpieczeństwa w ruchu drogowym.
* Optymalizacja działań Policji na rzecz zapewnienia bezpieczeństwa imprez masowych.
* Doskonalenie jakości zadań realizowanych przez policjantów i pracowników Policji poprzez zapewnienie optymalnych warunków pełnienia służby/pracy.
 |
| **Korzyść:** | 1. Zmniejszenie uciążliwości dla obywatela podczas kontaktu z Policją w trakcie wykonywania czynności legitymowanie.
2. Skrócenie czasu obsługi realizowanych przez Policję zadań.
3. Zmniejszenie w skali kraju liczby funkcjonariuszy zaangażowanych w realizację procesu.
4. Zwiększenie niezawodności systemu w przypadku wystąpienia nieprzewidywalnych zdarzeń w obrębie objętej projektem infrastruktury IT.
5. Powiększenie przestrzeni serwerowej i zlokalizowanie jej w zachodniej części kraju.
 |
| **KPI:** | 1. Średni czas realizacji czynności: legitymowania, potwierdzenia tożsamości i sprawdzenia osoby w wymaganych bazach danych
2. Liczba zrealizowanych spraw poprzez udostępne on-line usługi publiczne polegające na analizie obrazów cyfrowych, do rozpoznawanie sytuacji i zachowań będących w zainteresowaniu podmiotów realizujących zadania w zakresie bezpieczeństwa i porządku publicznego.
3. Wielkość przestrzeni serwerowni wykorzystywanej przez Policję i inne podmioty.
 |
| **Wartość aktualna i docelowa KPI:** | 1. Aktualnie brak narzędzia umożliwiającego automatyzację procesu weryfikacji tożsamości, docelowo opracowanie i udostępnienie aplikacji spełniającej tą funkcję.
2. Aktualnie brak narzędzia do automatycznego przetwarzania szeroko rozumianej analizy obrazów cyfrowych, do rozpoznawanie sytuacji i zachowań będących w zainteresowaniu podmiotów realizujących zadania w zakresie bezpieczeństwa i porządku publicznego. Przewiduje się wzrost skuteczności Policji w porównaniu do lat poprzednich. Wartością satysfakcjonującą będzie wzrost wspomnianego wskaźnika w stosunku do roku poprzedniego.
3. Wartość o jaką zwiększy się przestrzeń serwerowni po zakończeniu projektu.
 |
| **Metoda pomiaru KPI** | 1. Badanie opinii społecznej Polskie Badanie Przestępczości przeprowadzane cyklicznie od stycznia 2007 roku.
2. Pomiar, miernik ilościowy wykryć z użyciem narzędzia do automatycznej analizy audio-wideo.
 |

## Udostępnione e-usługi

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa e-usługi**  | **Typ** | **Zakres oddziaływania** | **Poziom dojrzałości e-usługi[[1]](#footnote-1)** |
| 1. | Usługa ustalenia tożsamości poprzez automatyczny transfer, wymaganych danych z aplikacji mObywatel do systemów Policyjnych. | -A2C | Policja - Obywatele | 3 |
| 2. | Usługa wizualizacji i publikowania raportów o bieżącym stanie bezpieczeństwa przestrzeni publicznej. Wykorzystanie interaktywnych map cyfrowych dla informacji z odniesieniami przestrzennymi. | -A2C | Policja - Obywatele | 2 |
| 3. | Usługa analizy on-line strumienia audio-wideo. System automatycznej analizy obrazów cyfrowych, do rozpoznawanie sytuacji i zachowań będących w zainteresowaniu służb porządku publicznego w celu przeciwdziałania powstawaniu negatywnych zdarzeń w przestrzeni publicznej m. in. automatyczna klasyfikacja zdarzenia i przygotowanie materiału do podjęcia dalszej decyzji przez funkcjonariusza. | -A2A | Policja i podmioty realizujące zadania w zakresie bezpieczeństwa i porządku publicznego. [wykorzystanie do A2C] | - |
| 4. | Usługa analizy offline materiałów audio-wideo z wykorzystaniem chmury prywatnej. Gotowe środowisko PaaS (Platform as a Service, czyli platforma jako usługa) do uruchomienia aplikacji w zakresie detekcji, gromadzenie i przetwarzania oraz przygotowanie materiału dowodowego dla potrzeb postępowań prowadzonych w trybie kodeksu postępowania karnego oraz udostępnienie jej zasobów innym podmiotom administracji publicznej (w szczególności Sądom i Prokuraturom).  | -A2A | Policja i podmioty realizujące zadania w zakresie bezpieczeństwa i porządku publicznego. Policja —administracja | - |
| 5. | Usługa Disaster Recovery Center dla wybranych systemów centralnych Policji oraz udostępnienie jej zasobów innym podmiotom administracji publicznej. | -A2A | Policja - administracja | - |

## Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Czy wszystkie zdigitalizowane zasoby objęte projektem będą udostępniane bezpłatnie?

 TAK/~~NIE~~ [[2]](#footnote-2)

|  |  |  |
| --- | --- | --- |
| **Rodzaj** **informacji / zasobów** | **Planowana data udostępnienia** | **Szacowana liczba obiektów objętych digitalizacją (udostępnianiem informacji)** |
| Usługa wizualizacji i publikowania raportów o bieżącym stanie bezpieczeństwa przestrzeni publicznej. Nowoczesne rozwiązania zapewnią infrastrukturę dla nowych projektów, ale również umożliwią na połączenie środowisk bazodanowych z systemami informacyjnymi. Pozwoli to na rozszerzenie zakresu prezentowanych danych statystycznych (np. wizualizujących miejsca szczególnie niebezpieczne dla pieszych na Krajowej Mapie Zagrożeń Bezpieczeństwa czy też integrację Krajowego Systemu Informacyjnego Policji z Uniwersalnym Modułem Mapowym). | sierpień 2022 | Rocznie odnotowanych jest ok. 750 tys. przestępstw w analizowanych statystycznie kategoriach. |

## Produkty końcowe projektu

|  |  |
| --- | --- |
| **Nazwa produktu** | **Planowana data wdrożenia** |
| Zmodernizowanie sieci OST 112 poprzez zwiększenie przepustowości łączy podstawowych do 40 Gb/s w celu zapewnienia wymiany danych pomiędzy interesariuszami, zniwelowanie istniejących wąskich gardeł i uzyskanie odpowiedniego poziomu przepływu danych. | grudzień 2021 |
| Budowa data center wraz z osprzętem technicznym. | grudzień 2021 |
| Usługa ustalenia tożsamości poprzez automatyczny transfer danych z aplikacji mObywatel do systemów Policyjnych. | marzec 2022 |
| Uruchomienie Disaster Recovery Center | sierpień 2022 |
| Uruchomienie chmurowych usług IaaS i PaaS, ( np. infrastruktura dla udostępnianych obywatelom usług umożliwiających wizualizację i publikowanie raportów o bieżącym stanie bezpieczeństwa w przestrzeni publicznej oraz przyjmowania i analizy materiału wideo przekazywanego przez obywateli). | sierpień 2022 |

# KAMIENIE MILOWE

|  |  |
| --- | --- |
| **Kamienie milowe** | **Planowany termin osiągnięcia** |
| Zakończenie dialogu technicznego  | 2019-04-30 |
| Złożenie wniosku o dofinansowanie | 2019-10-01 |
| Uzyskanie dokumentacji i projektu architektonicznego serwerowni. | 2019-11-01 |
| Uzyskanie pozwolenia na budowę serwerowni. | 2020-02-01 |
| Wdrożenie zmodernizowanej sieci OST 112 o zwiększonej przepustowości łączy podstawowych do 40 Gb/s. | 2021-12-31 |
| Uruchomienie przestrzeni sprzętowej i zwiększenie mocy obliczeniowej serwerów. | 2022-01-31 |
| Uruchomienie środowiska chmury obliczeniowej wraz z oprogramowaniem sieciowym (ACI, Dashboard). | 2022-06-30 |
| Zakończenie testów systemu w zakresie możliwych scenariuszy zakłócenia działania zarówno przez czynniki wewnętrzne jak i zewnętrze ze szczególny akcentem na bezpieczeństwo danych i odporność na cyberataki. | 2022-07-31 |
| Wdrożenie aplikacji na mobilne terminale noszone umożliwiające automatyzację procesu weryfikacji tożsamości. | 2022-07-01 |
| Uruchomienie Disaster Recovery Center. | 2022-09-01 |
| Uruchomienie systemu automatycznej analizy obrazów cyfrowych, do rozpoznawanie sytuacji i zachowań będących w zainteresowaniu służb porządku publicznego. | 2022-10-31 |

# KOSZTY

## Koszty ogólne projektu wraz ze sposobem finansowania

|  |  |
| --- | --- |
| **Całkowity koszt projektu (netto oraz brutto), w tym:** | **95 000 000,00 zł brutto,****77 235 00,00 zł netto;** |
| **Procent dofinansowania ze środków UE (brutto)**  | **85 %** |
| **Procent środków z budżetu państwa (brutto)** | **15%** |
| **Podział całkowitego kosztu projektu na poszczególna lata (netto oraz brutto)** | *Rok 2019* | **brutto: 48 268 160,00 zł / netto: 39 242 014,08 zł** |
| *Rok 2020* | **brutto: 30 871 640,00 / netto: 25 098 643,32 zł** |
| *Rok 2021* | **brutto: 15 860 200,00 zł / netto: 12 894 342,60 zł** |

## Wykaz poszczególnych pozycji kosztowych

|  |  |  |
| --- | --- | --- |
| **Nazwa pozycji kosztowej:** | Przewidywany koszt brutto: | Uzasadnienie pozycji kosztowej (przeznaczenie): |
| Oprogramowanie |  20 607 800,00 zł  | Organizacja środowiska do:- automatyzacji procesu uzupełnienia danych w aplikacjach mobilnych służb; - automatycznej analizy obrazów cyfrowych pod kątem rozpoznawania sytuacji i zachowań zagrażających porządkowi publicznemu;- obsługi zapasowego centrum przetwarzania danych (ang. Disaster Recovery Center) umożliwiającego odtworzenie w zadanym czasie, kluczowych dla bezpieczeństwa usług i danych, wybranych zasobów systemów centralnych Policji udostępnianych także innym podmiotom administracji publicznej. |
| Infrastruktura  | 67 788 900,00 zł  | Zakup infrastruktury techniczno-sprzętowej. Realizacja budowy obiektu klasy „Data Center” wraz z systemami zabezpieczeń, zasilania prądowego, systemów środowiskowych i p.poż. |
| Koszty UX i grafiki | 120 000,00 zł  | Testowanie uruchomionego systemu w zakresie wszystkich możliwych scenariuszy zakłócenia działania zarówno przez czynniki wewnętrzne jak i zewnętrze ze szczególny akcentem na bezpieczeństwo danych i odporność na cyberataki. |
| Bezpieczeństwo |  1 426 400,00 zł  | Ochrona systemu przetwarzającego dane istotne dla bezpieczeństwa centralnych systemów informatycznych Policji oraz infrastruktury teleinformatycznej w warunkach aktualnie definiowanych zagrożeń hybrydowych dla systemów cyberbezpieczeństwa. |
| Wydajność rozwiązania | 120 000,00 zł  | Podniesienie jakości produktu i zapobiega generowaniu dużej ilości błędów. |
| Szkolenia | 164 400,00 zł  | Celem jest podniesienie wiedzy oraz kwalifikacji administratorów zarządzających komponentami zrealizowanego projektu. |
| Działania informacyjno-promocyjne | 23 700,00 zł  | Promocja jest przewidziana w postaci konferencji podsumowujących projekt oraz minimalnymi wymaganiami wynikającymi z realizacji projektów unijnych.  |
| Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego) | 4 748 800,00 zł  | Usługi wspomagające będą realizowane w celu spełnienia wszystkich wymogów formalnych |

## Koszty ogólne utrzymania wraz ze sposobem finansowania (okres 5 lat)

|  |  |  |
| --- | --- | --- |
| **Całkowity koszt utrzymania trwałości projektu (brutto)** | 150 000 000,00 zł | Źródło finansowania |
| **Podział całkowitego kosztu utrzymania trwałości projektu na poszczególna lata (netto oraz brutto)** | 2022 rok | **brutto: 30 000 000,00 zł****netto: 24 390 000,00 zł** | budżet państwa |
| 2023 rok | **brutto: 30 000 000,00 zł**netto: 24 390 000,00 zł | budżet państwa |
| 2024 rok | **brutto: 30 000 000,00 zł**netto: 24 390 000,00 zł | budżet państwa |
| 2025 rok | **brutto: 30 000 000,00 zł**netto: 24 390 000,00 zł | budżet państwa |
| 2026 rok | **brutto: 30 000 000,00 zł****netto: 24 390 000,00 zł** | budżet państwa |

# 4.4 Planowane koszty ogólne realizacji (w przypadku projektu współfinansowanego – wkład krajowy z budżetu państwa) oraz koszty utrzymania projektu:

# ~~zostaną pokryte w ramach budżetów odpowiednich dysponentów części budżetowych bez konieczności występowania o dodatkowe środki z budżetu państwa~~,

# będą powodować konieczność przyznania dodatkowych kwot.[[3]](#footnote-3)

# GŁÓWNE RYZYKA

## Ryzyka wpływające na realizację projektu

|  |  |  |  |
| --- | --- | --- | --- |
| **Nazwa ryzyka** | Siła oddziaływania | Prawdopodobieństwo wystąpienia ryzyka | Sposób zarzadzania ryzykiem |
| Długotrwałe, przeciągające się procedury przetargowe, ograniczone zasoby kadrowe | duża | wysokie | - Korzystanie z doświadczeń innych projektów w zakresie odwołań - Stałe monitorowanie harmonogramu zamówienia |
| Fluktuacja kadr, odejście z pracy kluczowych dla realizacji projektu osób  | duża | wysokie | - Systematyczne prowadzenie uporządkowanego repozytorium projektu.- Określanie zastępstw- Komunikacja w projekcie ( bieżąca wymiana wiedzy, doświadczeń) |
| Nieprecyzyjnie lub niepełnie określone wymagania w opisie przedmiotu zamówienia | duża | średnie | - Kompetentna analiza przygotowująca opis przedmiotu zamówienia.- Wykorzystywanie wsparcia zewnętrznego do analizy i przygotowania przedmiotu zamówienia i kryteriów oceny ofert |
| Niekorzystne zmiany kursów walut, wahania cen materiałów | średnia | małe | - Planowanie kwoty do przetargu z racjonalnym zapasem |
| Nieskuteczna komunikacja pomiędzy uczestnikami Projektu | średnia | średnie | - Na etapie realizacji projektu, wypracowany zostanie system komunikacji określający zasady powszechnego stosowania przez wszystkich uczestników projektu. |
| Niedostateczna jakość wymagań technicznych w dokumentacji przetargowej dla zaawansowanej technologicznie infrastruktury technicznej | duża | małe | - Przeprowadzenie analiz potrzeb wydajnościowych podczas przygotowywania dokumentacji przetargowej. Wsparcie zewnętrzne podczas przygotowania i realizacji przetargu. |
| Nierzetelny lub niedoświadczony Wykonawca systemu nie będący w stanie zrealizować zamówienia w sposób należyty | duża  | średnie | - Analiza na etapie przygotowania postępowania i adekwatne do skali i charakteru zamówienia warunki udziału w postępowaniu-Mechanizmy kontrolne w umowie - Racjonalne harmonogramy |
| Opóźnienia w procedurze uzyskania pozwolenia na budowę i użytkowanie serwerowni.  | średnia | duże | Kompetentna analiza wszystkich warunków, które mogą wydłużać procedurę uzyskania pozwoleń.  |

## Ryzyka wpływające na utrzymanie efektów

|  |  |  |  |
| --- | --- | --- | --- |
| **Nazwa ryzyka** | Siła oddziaływania | Prawdopodobieństwo wystąpienia ryzyka | Sposób zarzadzania ryzykiem |
| Fluktuacja kadr, odejście z pracy kluczowych dla realizacji projektu osób  | duża | duże | Systematyczne prowadzenie uporządkowanego repozytorium projektu.- Określanie zastępstw- Komunikacja w projekcie ( bieżąca wymiana wiedzy, doświadczeń) |
| Zapewnienie finansowania | duża | średnie | Monitorowanie zmian budżetu |

# OTOCZENIE PRAWNE

Nie jest wymagana zmiana przepisów prawa.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp** | Tytuł aktu prawnego | Czy wymaga zmian? | Opis zmian (jeśli dotyczy) | Etap prac legislacyjnych (jeśli dotyczy) |
|  |  | ~~TAK~~/NIE[[4]](#footnote-4) |  |  |

# ARCHITEKTURA

## Widok kooperacji aplikacji



Diagram kooperacji, przedstawia umiejscowienie prywatniej chmury obliczeniowej Policji, która ma pełnić również funkcję Disaster Recovery Center dla wybranych systemów centralnych Policji, oraz udostępnianie jej zasobów innym podmiotom administracji publicznej.

| Status | Opis |
| --- | --- |
| Planowany | Prywatna chmura obliczeniowa Policji z usługą udostępniania wirtualnego środowiska pracy (PaaS) i DRC. |
| Istniejące | Działające systemy: SI CPR i dwa środowiska CPD Policji.  |
| W budowie | System CPD PSP na etapie budowy. |

Lista systemów wykorzystywanych w projekcie:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa systemu** | **Gestor systemu** | **Opis systemu** | **Status** | **Krótki opis ewentualnej zmiany** |
| 1 | Centrum przetwarzania Danych (CPD) i Zapasowe Centrum Przetwarzania Danych (ZCPD)  | Policja | Zapewnia optymalne warunki do eksploatacji systemu teleinformatycznych (np. SIS, VIS, KSIP, SWD, KCIK) | Istniejący | Poprawa bezpieczeństwa przetwarzanych danych. Możliwość odtworzenia infrastruktury informatycznej, przetwarzającej krytyczne systemy lub procesy. |
| 2 | System Informatyczny CPR | SI CPR | System Informatyczny CPR do obsługi OST112, integruje przekazywanie zgłoszeń do poszczególnych służb | Istniejący | Poprawa przepływu i sprawności przekazywanych danych |
| 3 | Centrum przetwarzania Danych PSP | CPD PSP | Centrum przetwarzania Danych Państwowej Straży Pożarnej | W budowie | Poprawa przepływu i sprawności przekazywanych danych pomiędzy SWD |

Lista przepływów :

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **System źródłowy** | **System docelowy** | **Zakres wymienianych danych** | **Sposób wymiany danych** | **Typ modyfikacji** | **Typ Interfejsu** |
| 1. | mObywatel,mTożsamość | SWD Policji | Wymagana ustawowo informacja o osobie | Tryb odwołań bezpośrednich  | Krytyczna | Szyna danych dla udostępnionych usług |
| 2. | Systemy monitoringu wizyjnego  | System Analizy Wideo | Materiały multimedialne  | Kopiowanie danych | Krytyczna | Szyna danych |
| 3. | SWD PolicjiSWD PSPSWD PRM | Disaster Recovery Center | Replikacja baz danych | Kopiowanie danych | Krytyczna | Szyna danych  |

## Kluczowe komponenty architektury rozwiązania



Diagram przedstawia założenia projektowe komponentów logicznych prywatniej chmury obliczeniowej Policji.

## Przyjęte założenia technologiczne

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Obszar** | **Założenie technologiczne** |
| 1. 1
 | Infrastruktura | Projekt zakłada architekturę sprzętowo-programową działającą na potrzeby hybrydowej chmury prywatnej (chmury prywatnej na potrzeby Policji oraz innych służb podległych resortowi Spraw Wewnętrznych i Administracji z opcją jej współdzielenia w zakresie wykonywania pełnej kopii bezpieczeństwa bazy w trybie OFFLINE, czyli tzw. zimnego backup-u). Jego podstawowymi założeniami są elastyczność, zarówno pod kontem wydajności jaki i pojemności środowiska. |
| 1. 2
 | Sieć i bezpieczeństwo | Zwiększenie przepustowości łączy podstawowych do 40 Gb/s. Modernizacja komponentów bezpieczeństwa CSD. |
| 1. 3
 | Standardy wymiany danych | Architektura będzie łączyć środowisko klasyczne (konwergentne) ze środowiskiem typowo chmurowym opartymi na rozwiązaniach hiperkonwergentnych i hiperskalowalnych. Umożliwi to wymianę danych niezależnych od platformy, protokołów i formatów oraz ich integrację z systemami wewnętrznymi. |
| 1. 4
 | Systemy operacyjne serwerowe | Rozwiązanie hybrydowe będzie zapewniało optymalne wykorzystanie licencji oraz specyficznych wymagań usług, które nie są dostosowane do architektury typu cloud.  |
| 1. 5
 | Bazy danych | Z uwagi, że takie środowiska nie posiadają stałej lub maksymalnej wielkości i powinny dostosowywać się do zmiennych wymagań użytkowników, jako początkowe zostały przyjęte parametry aktualnie wykorzystywanych systemów, usług i baz gromadzących dane. |
| 1. 6
 | Serwery aplikacji | Uruchomienie chmurowych usług IaaS i PaaS. |

## Opis zasobów danych przetwarzanych w planowanym rozwiązaniu

Czy nowy system będzie tworzył zasoby danych o charakterze rejestru publicznego?

~~TAK/~~NIE [[5]](#footnote-5)

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Tworzony rejestr publiczny** | **Opis**  |
| - | - | - |

Czy nowy system będzie przetwarzał (używał, zmieniał) zawartość innych rejestrów publicznych?

TAK/~~NIE~~ [[6]](#footnote-6)

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Rejestr publiczny** | **Opis**  | **Zakres przetwarzania** |
| 1 | PESEL/CEL (Centralna Ewidencja Ludności), CEPIK (Centralna Ewidencja Pojazdów i Kierowców) | W planowanym rozwiązaniu zakłada się automatyzację procesów weryfikacji tożsamości osób, posiadanych przez nie uprawnieniach. Zapasowe centrum (ang. Disaster Recovery Center) będzie replikowało zasoby bazodanowe jedynie dla danych Systemu Wspomagania Dowodzenia Policji, Systemu Wspomagania Dowodzenia Państwowej Straży Pożarnej i Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego w zakresach właściwych dla środowisk podstawowych. System Wspomagania Dowodzenia Policji w granicach wskazanych przepisami prawa, korzysta z rejestrów publicznych poprzez System Poszukiwawczy Policji (SPP). Analiza video zakłada przeszukiwanie i analizowanie materiałów multimedialnych zbiorów monitoringu wizyjnego, udostępnionego przez różne podmioty. Ponadto wprowadzone rozwiązania pozwolą na analizę materiału gromadzonego z kamer nasobnych funkcjonariuszy Policji.  | używanie |

## Bezpieczeństwo

Planowany poziom zapewnienia bezpieczeństwa (w rozumieniu przepisów §20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności […] (Dz. U. 2012, poz. 526 z późn. zm.) w zakresie dot. systemu zarządzania bezpieczeństwem informacji:

* system nie podlega rygorom KRI – należy wyjaśnić czy istnieją inne normy bezpieczeństwa, które będą spełnione przez system zgodnie z wymogami KRI,
* ~~dodatkowe zabezpieczenia powyżej wymogów KRI: należy wskazać uzasadnienie~~~~[[7]](#footnote-7)~~

System nie podlega wymogom KRI, ponieważ nie tworzy zbiorów o charakterze rejestrów publicznych.

Stosowane w Policji polityki dotyczące bezpieczeństwa przetwarzania danych są zgodne z minimalnymi wymaganiami dla systemów teleinformatycznych określonymi w rozdziale IV Rozporządzenia Rady Ministrów z dn. 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*.

1. Pięciostopniowa e-dojrzałość usług określona w badaniach „Digitizing Public Services in Europe: Putting ambition into action”, prowadzonych na zlecenie KE przez firmę Cap Gemini c.europa.eu/newsroom/document.cfm?action=display&doc\_id=747 [↑](#footnote-ref-1)
2. Niepotrzebne skreślić. [↑](#footnote-ref-2)
3. Niepotrzebne skreślić [↑](#footnote-ref-3)
4. Niepotrzebne skreślić. [↑](#footnote-ref-4)
5. Niepotrzebne skreślić. [↑](#footnote-ref-5)
6. Niepotrzebne skreślić [↑](#footnote-ref-6)
7. Niepotrzebne skreślić [↑](#footnote-ref-7)