Załącznik 1. do SIWZ

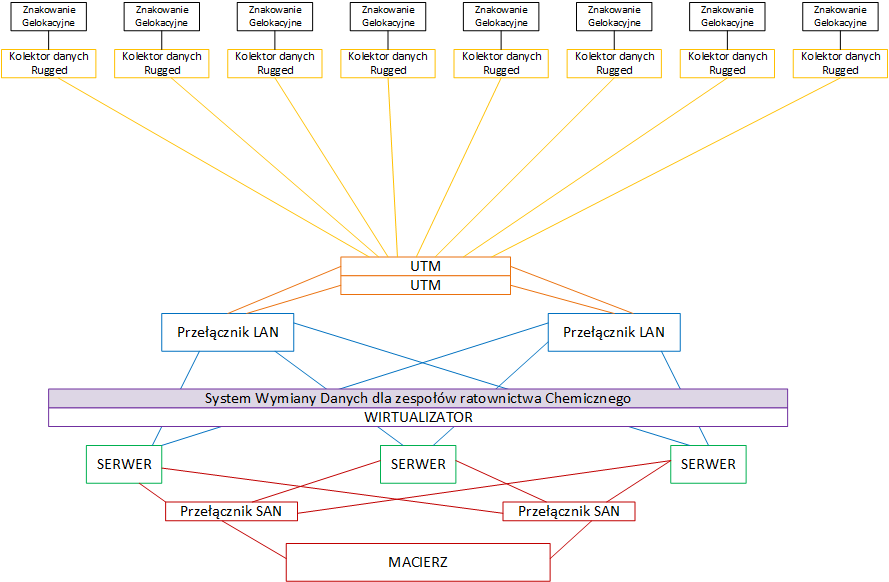
# OPIS PRZEDMIOTU ZAMÓWIENIA

# I. Część sprzętowa

# Infrastruktura IT

System musi zostać zbudowany na dedykowanym oprogramowaniu pracującym w modelu chmury prywatnej, która zostanie oparta o dwie podstawowe, centralne jednostki analityczne (KWPSP Warszawa- KWPSP Poznań) oraz o centrum awaryjne (KWPSP Warszawa – w fizycznie wydzielonej lokalizacji). W każdej z lokalizacji podstawowych musi zostać zainstalowany klaster obliczeniowy, na który składać się będą trzy serwery obliczeniowe oraz szybka macierz dyskowa. Centralne jednostki analityczne muszą wymieniać dane z mobilnymi zespołami analitycznymi (3 zespoły) i zespołami rozpoznania (4 zespoły), które stanowią specjalistyczne grupy ratownictwa chemiczno-ekologicznego PSP. Środowisko to musi zostać zabezpieczone dedykowanymi koncentratorami VPN, które muszą zestawiać kanały komunikacyjne z mobilnymi kolektorami danych za pomocą sieci publicznej przy użyciu silnych metod uwierzytelniania, w oparciu o certyfikaty generowane dla każdego z kolektorów danych. Kolektory muszą zostać wyposażone we wbudowany modem LTE/3G/WLAN i umożliwić podłączenie się do praktycznie dowolnego medium telekomunikacyjnego jak również działanie w miejscach, w których klasyczne medium (sieć LAN, Wifi) nie występuje.

Wymaganą architekturę rozwiązania dla jednego z centrów danych przedstawia poniższy rysunek:



Architektury takie muszą zostać zainstalowane w lokalizacji KWPSP – Warszawa oraz Poznań, dodatkowo w zapasowej serwerowni KW PSP Warszawa (w wydzielonej lokalizacji, innej niż siedziba KW) musi zostać zainstalowana macierz dyskowa, na którą replikowane będą kopie zapasowe tego rozwiązania.

Wykonawca dostarczy wszystkie niezbędne przewody i komponenty niezbędne do prawidłowego podłączenia i uruchomienia sprzętu oraz prawidłowego funkcjonowania systemu.

1. Macierz dyskowa do backupu - 3 szt.

| **Lp.** | **Nazwa podzespołu** | **Minimalne wymagane parametry** |
| --- | --- | --- |
| 1. | Obudowa | 1) Przez macierz dyskową Zamawiający rozumie zestaw dysków twardych HDD i/lub dysków SSD kontrolowanych przez minimum pojedynczą parę kontrolerów macierzowych, kontrolujących wszystkie zasoby dyskowe macierzy z poziomu pojedynczej konsoli WebGUI/CLI administratora;  2) Macierz musi posiadać architekturę modułową w zakresie obudowy dla instalacji kontrolerów oraz obsługiwanych dysków, z dopuszczeniem współdzielenia jednego z modułów przez kontrolery i dyski dla zapisów danych Użytkownika;  3) System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 4U w tej szafie;  4) Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia);  5) Każdy moduł/obudowa macierzy powinna posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii;  6) Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów, bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy;  7) Moduły dla dalszej rozbudowy o dodatkowe dyski i przestrzeń dyskową muszą zapewniać gęstości upakowania co najmniej 24 dysków 2,5” lub co najmniej 12 dysków 3,5” na każde 2U przestrzeni instalacyjnej w szafie przemysłowej rack standardu 19”;  8) Dostarczona konfiguracja macierzy musi pozwalać na połączenie kaskadowe lub w układzie pętli pomiędzy modułami rozwiązania (moduł kontrolerów, moduły/półki dyskowe), z wykorzystaniem minimum 2-torów kablowych w tych połączeniach – okablowanie to musi być zgodne ze standardem SAS 12Gb/s. W przypadku braku obsługi połączeń w układzie pętli dopuszcza się jako alternatywne rozwiązanie macierz z zainstalowanymi 4 kontrolerami RAID; |
| 2. | Pojemność | 1) Oferowana macierz musi obsługiwać min. 142 dyski wykonane w technologii hot-plug – jeżeli dla obsługi tej funkcjonalności konieczny jest zakup dodatkowych licencji to należy ją dostarczyć wraz z macierzą;  2) Model oferowanej macierzy musi obsługiwać przestrzeń dyskową w trybie tzw. surowym (RAW) minimum 4000 TB, bez konieczności wymiany zainstalowanych kontrolerów – wymagana zgodność z zapisami aktualnej na moment składania oferty specyfikacji technicznej macierzy, udostępnionej publicznie na stronie internetowej producenta lub jego przedstawiciela w Polsce;  3) Model oferowanej macierzy musi umożliwiać rozbudowę do wyższego modelu z tej samej rodziny urządzeń w trybie w „data-in-place” tj. z wykorzystaniem wszystkich modułów półek rozszerzeń dyskowych wykorzystywanych przed rozbudową i z dostępem do wcześniej zapisanych danych;  4) Wszystkie zainstalowane dyski hot-plug, z wyłączeniem dysków SSD stosowanych jako rozszerzenie pamięci Cache kontrolerów, muszą być dostępne dla zapisu danych Użytkownika; |
| 3. | Kontrolery | 1) Kontrolery macierzy muszą obsługiwać tryb pracy w układzie active-active lub mesh-active, macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami;  2) Każdy z kontrolerów macierzy musi posiadać po minimum 16 GB pamięci podręcznej Cache – kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych (cache mirror) przeznaczonych do zapisu;  3) Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o minimum 1,6 TB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności zainstalowanych dysków SSD,  4) W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk lub równoważny nośnik;  5) Kontrolery muszą posiadać możliwość ich wymiany (w przypadku awarii lub planowych zadań utrzymaniowych) bez konieczności wyłączania zasilania całego urządzenia – wymaganie w przypadku konfiguracji z min. 2 kontrolerami;  6) Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach;  7) Każdy z kontrolerów RAID powinien posiadać dedykowane minimum 2 interfejsy RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s - dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy;  8) Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej;  9) Każdy kontroler macierzy musi pozwalać na konfigurację interfejsów niezbędnych dla współpracy w sieci IP/FC/SAS SAN oraz NAS;  10) Dla obsługi operacji blokowych I/O w sieci IP/FC/SAS SAN kontrolery macierzy muszą wspierać protokoły transmisji: FC 32/16Gb/s , iSCSI 10/1Gb/s, SAS 12Gb/s;  11) Dla obsługi operacji plikowych I/O w sieci NAS kontrolery macierzy muszą wspierać minimum protokoły dostępu: CIFS, NFS. Obecnie nie jest wymagana obsługa protokołów CIFS, NFS, ale musi istnieć możliwość rozbudowy o tą funkcjonalność. Rozbudowa o tą funkcjonalność nie może wymagać montażu żadnych zewnętrznych elementów/modułów po za obudową macierzy;  12) Uruchomienie obsługi protokołów CIFS i NFS nie może powodować zmniejszenia rozmiaru pamięci podręcznej cache wykorzystywanej przez macierz do obsługi protokołów blokowych – jako równoważność dla tego wymagania dopuszczone jest skonfigurowanie dodatkowo minimum po 16GB pamięci podręcznej Cache dla każdego kontrolera lub 2 grup dyskowych RAID1z dyskami SAS SSD minimum 200GB – nie jest wymagane dostarczenie tej funkcjonalności w postepowaniu, możliwość rozbudowy w przyszłości;  13) Kontrolery macierzy muszą obsługiwać do 72 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów; |
| 4. | Interfejsy | 1. Oferowana macierz musi posiadać minimum:   - 2 porty FC 16Gb/s (obsadzone wkładkami), przeznaczone do dołączenia serwerów, wyprowadzone na każdy kontroler RAID;  - 2 porty iSCSI 10Gb/s SFP+ przypadające na każdy z kontrolerów;  2) Macierz musi umożliwiać wymianę portów do transmisji danych(z serwerami) na porty obsługujące protokoły: FC 32Gb/s, iSCSI 1Gb/s, SAS 12Gb/s;  3) Wymiana portów jw. nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu, a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych; |
| 5. | Poziomy RAID | Macierz musi zapewniać poziom zabezpieczenia danych na dyskach, definiowany poziomami RAID: 0, 1 , 10, 5 , 50, 6; |
| 6. | Wspierane dyski | 1) Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex;  2) Oferowana macierz musi wspierać dyski hot-plug:  - dyski elektroniczne SSD i mechaniczne HDD iż interfejsami SAS12Gb/s i SAS6Gb/s  - dyski mechaniczne HDD o prędkości obrotowej 7,2 krpm, 10 krpm oraz 15k rpm,  3) Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD (SAS i NLSAS) zainstalowanych w dowolnym module rozwiązania;  4) Model macierzy musi pozwalać na instalację dysków hot-plug w formacie 2,5” i 3,5”;  5) Macierz musi obsługiwać min. 72 dyski SAS SSD w całym rozwiązaniu;  6) Wymagane jest dostarczenie macierzy zawierającej min. 19 dysków NL-SAS o pojemności min. 10 TB każdy, o prędkości obrotowej 7200 obr/min;  7) Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy) w trybach:  - hot-spare dedykowany dla zabezpieczenia tylko wybranej grupy dyskowej RAID  - hot-spare dla zabezpieczenia dowolnej grupy dyskowej RAID;  8) W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. CopyBackLess);  9) Dostarczona macierz w oferowanej konfiguracji umożliwia szyfrowanie danych na zainstalowanych dyskach dowolnego typu – funkcjonalność realizowana bezpośrednio przez kontrolery macierzy dla danych blokowych – minimum AES 256. Jeżeli funkcjonalność ta wymaga dodatkowych elementów sprzętowych bądź aktywacji dodatkowej licencji to należy dostarczyć je wraz z rozwiązaniem dla maksymalnej pojemności macierzy. |
| 7. | Opcje software’owe | 1) Macierz musi być wyposażona w system kopii migawkowych umożliwiających wykonanie minimum 1024 kopii migawkowych – jeżeli funkcjonalność ta wymaga zakupu licencji to należy je dostarczyć w wariancie dla maksymalnej pojemności dyskowej dla oferowanej macierzy;  2) Macierz musi umożliwiać zdefiniowanie min. 4096 woluminów (LUN);  3) Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy;  4) Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową;  5) Macierz musi posiadać wsparcie dla systemów operacyjnych : MS Windows Server 2012R2/2016/2019, SuSE Linux, Oracle Linux, Oracle VM, RedHat Linux, HP-UX, IBM AIX, SUN Solaris, VMWare , Citrix XEN Server.  6) Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem);  7) Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, po protokołach FC oraz iSCSI, bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji – nie jest wymagane dostarczenie licencji dla tej funkcjonalności;  8) Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy, jako tzw. storage-based data replication;  9) Replikacja danych jak w pkt.7 musi być obsługiwana w połączeniu z każdą macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych;  10) Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – Licencja na wymienioną funkcjonalność NIE JEST przedmiotem niniejszego postępowania;  11) W przypadku obsługi protokołów CIFS i NFS wymagana jest funkcjonalność agregacji przepustowości dla interfejsów dedykowanych do obsługi tych protokołów;  12) Macierz musi obsługiwać dla interfejsów iSCSI i interfejsów obsługujących protokoły CIFS i NFS adresacje IP v.4 i IP v.6;  13) W przypadku korzystania z protokołów dostępu plikowego obsługa CIFS i NFS musi odbywać się jednocześnie;  14) Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy;  15) Model oferowanej macierzy musi wspierać rozwiązania klasy ‘klastra macierzowego’ tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych pomiędzy minimum 2 macierzami ;  16) Mechanizm klastra macierzowego musi być obsługiwany dla protokołów FC oraz iSCSI, zarówno w zakresie replikacji danych jak i w zakresie sposobu podłączenia serwerów do zasobów macierzy – Licencja na wymienioną funkcjonalność NIE JEST przedmiotem niniejszego postępowania;  17) Pod użytym w pkt. 15 pojęciem ‘wysoka dostępność zasobów dyskowych’ należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzy bądź awarii samej macierzą, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej; 18) Dla uruchomienia funkcjonalności ‘klastra macierzowego’ musi być możliwość wykorzystania istniejącej infrastruktury FC/IP SAN Użytkownika w zakresie przełączników FC/Ethernet i kart HBA FC/Ethernet zainstalowanych w serwerach Użytkownika;  19) Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie ‘klastra macierzowego’, musi wspierać poziomy RAID1, RAID10, RAID5, RAID6 bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i główną;  20) Funkcjonalność ‘klastra macierzowego’ musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover);  21) Funkcjonalność ‘klastra macierzowego’ musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover);  22) Funkcjonalność ‘klastra macierzowego’ musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback );  23) Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk i aplikacji korzystających z zasobów macierzy – Licencja na wymienioną funkcjonalność NIE JEST przedmiotem niniejszego postępowania;  24) Mechanizm AST musi być obsługiwany przy korzystaniu zarówno z trzech jak z dwóch dostarczonych technologii dyskowych: SSD, SAS, NLSAS;  25) Macierz musi pozwalać na definiowanie minimum 32 różnych polityk i zasad migrowania danych w obrębie tej samej macierzy;  26) Maksymalna wielkość pojedynczego bloku danych podczas migracji i realokacji mechanizmami AST nie może przekraczać 256MB;  27) Mechanizm AST musi być wyposażony w funkcję Quality-of-Services pozwalająca na zagwarantowaniu wydajności dla wybranych zasobów macierzy (woluminów) mierzonej jako maksymalny czas opóźnień operacji I/O wykonywanych przez serwer/środowisko/aplikację – Licencja na wymienioną funkcjonalność NIE JEST przedmiotem niniejszego postępowania;  28) Mechanizm AST musi pozwalać na definiowanie okna czasowego dla zbierania pomiarów wydajności operacji I/O oraz okna czasowego dla migrowania danych wg ustalonych zasad i polityk – minimalny definiowany czas trwania w/w operacji (długość okna czasowego) nie może być dłuższy niż 4 godziny;  29) Mechanizm AST musi pozwalać na wykluczanie wybranych godzin i dni z pomiarów wydajności operacji I/O;  30) Macierz musi obsługiwać mechanizmy migracji danych w trybie online z innej macierzy tej klasy, z zachowaniem obsługi operacji I/O dla serwerów podłączonych do migrowanej macierzy tj. do migrowanych zasobów LUN; |
| 8. | Konfiguracja, zarządzanie | 1) Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej zarówno przy obsłudze transmisji danych protokołami blokowymi (FC, iSCSI, SAS) jak i do obsługi transmisji protokołami CIFS/NFS;  2) Oprogramowanie zarządzające musi być dostarczone w wariancie dla maksymalnej obsługiwanej pojemności dyskowej macierzy oraz dla maksymalnej liczby dysków wspieranej przez oferowaną macierz;  3) Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.  4) Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (np. Internet Explorer, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora;  5) Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI; |
| 9. | Gwarancja i serwis | 1) Macierz dyskowa musi zostać objęta minimum 36 miesięcznym okresem gwarancji producenta z czasem reakcji najpóźniej w następnym dniu roboczym od dnia zgłoszenia usterki. Wymagane jest pisemne poświadczenia gotowości realizacji wymaganego poziomu serwisowego przez polskiego przedstawiciela producenta macierzy. Producent macierzy musi umożliwiać skuteczne zgłaszanie usterek w trybie całodobowym, 7 dni w tygodniu, również w dni świąteczne.  2) Macierz musi być zaoferowana z serwisem producenta macierzy, który w przypadku wymiany dysków twardych HDD/SSD, umożliwia pozostawienie wszystkich uszkodzonych nośników u Zamawiającego.  3) Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia, w ciągu 60 miesięcy od daty zakupu;  4) Po zakończeniu okresu gwarancji musi być zapewniony przez producenta rozwiązania bezpłatny dostęp do aktualizacji oprogramowania wewnętrznego oferowanej macierzy;  5) Macierz musi umożliwiać konfigurację i uruchomienie dedykowanej funkcji automatycznego powiadomienia serwisu o usterce przez samo urządzenie (poprzez dedykowany system wbudowany w macierz - bez pośrednictwa administratora, nie dopuszcza się użycia ogólnodostępnych mechanizmów - poczty email w tym m.in. protokołu SNMP i SMTP, nie dopuszcza się SMS – Zamawiający nie dopuszcza możliwości komunikacji z/do macierzy poprzez pocztę email/SNMP/SMTP itp. z powodów bezpieczeństwa). Funkcjonalność musi pozwalać na automatyczne otwarcie zgłoszenia serwisowego w bazie serwisowej producenta macierzy zgodnie z wymaganym w specyfikacji poziomem SLA; Opcja ta musi być dostępna bezpłatnie w trakcie całego okresu gwarancji producenta macierzy. Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do macierzy bezpośrednio przez Producenta – musi być do tego wykorzystany dedykowany system serwisowy macierzy.  6) Macierz musi pochodzić z legalnego kanału sprzedaży producenta w Polsce i musi reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych;  7) Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia;  8) Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu ofertowym należy podać pełen adres internetowy strony producenta macierzy, gdzie można zweryfikować wymagane informacje; |

## 2. Macierz wirtualizacyjna – 2 szt.

|  |  |
| --- | --- |
| **Lp.** | **Opis wymagania** |
|  | Macierz musi być wyposażona w co najmniej jedną parę kontrolerów macierzowych kontrolujących wszystkie zasoby dyskowe macierzy bez korzystania z zewnętrznych połączeń kablowych pomiędzy dowolnymi kontrolerami (nie dopuszcza się żadnych połączeń typu IP/LAN poprzez zewnętrzne switche, główki, itp.); |
|  | Macierz posiada architekturę modułową dla instalacji kontrolerów, portów komunikacyjnych, oraz obsługiwanych dysków, z dopuszczeniem współdzielenia jednego z modułów przez zainstalowane kontrolery i dyski; |
|  | Macierz musi być dostarczona ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” |
|  | Zajętość kompletnej macierzy z modułami dyskowymi i modułami kontrolerów w oferowanej konfiguracji - maksymalnie 3U szafie rack. |
|  | Macierz zawiera łącznie minimum:   * 14 dysków 2,5” SAS 12G 10k RPM o pojemności minimum 2400GB każdy; * 8 dysków 2,5” SSD SAS o pojemności minimum 3,84TB każdy; * Macierz w oferowanej konfiguracji musi posiadać minimum 2 wolne wnęki na instalację dysków 2,5” SAS; |
|  | Macierz musi być wyposażona w minimum:   * 4 aktywne porty FC 16Gb/s przypadające na każdy z kontrolerów; * 2 aktywne porty iSCSI 10Gb/s SFP+ przypadające na każdy z kontrolerów; |
|  | Każdy skonfigurowany moduł kontrolerów i/lub dyskowy musi posiadać nadmiarowy układ zasilania i chłodzenia zapewniający ciągłą pracę całej konfiguracji macierzy bez ograniczeń czasowych i wydajnościowych w przypadku usterki pojedynczego zasilacza lub elementu chłodzenia; |
|  | Macierz musi umożliwiać rozbudowę i jednoczesne podłączenie i używanie modułów dyskowych dla dalszej rozbudowy w co najmniej trzech wariantach:   * maksimum 2U przy gęstości upakowania minimum 24 dysków 2,5” typu hotplug (jednoczesna obsługa dowolnej kombinacji dysków SAS, NL-SAS,SSD w pojedynczej półce); * maksimum 2U przy gęstości upakowania minimum 12 dysków 3,5” typu hotplug lub 4U przy gęstości upakowania minimum 24 dyski 3,5” typu hotplug (jednoczesna obsługa dowolnej kombinacji dysków SAS, NL-SAS,SSD); * maksimum 4U przy gęstości upakowania minimum 60 dysków 3,5” typu hotplug (jednoczesna obsługa dowolnej kombinacji dysków SAS, NL-SAS,SSD); |
|  | Wszystkie zewnętrzne połączenia kablowe pomiędzy modułami muszą zapewniać komunikację nawet w przypadku awarii dowolnej z półek ze wszystkimi pozostałymi półkami/dyskami. |
|  | Połączenia kablowe SAS 12G pomiędzy modułami muszą zapewniać przepustowość minimum 48Gb/s w ramach pojedynczego połączenia. |
|  | Model oferowanej macierzy obsługuje minimum 220 dysków wykonanych w technologii hot-plug bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami; |
|  | Kontrolery macierzy obsługują tryb pracy w układzie active-active lub mesh-active. Macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami. |
|  | Każdy z kontrolerów macierzy posiada po minimum 64 GB pamięci podręcznej Cache – zawartość pamięci Cache musi być identyczna dla wszystkich kontrolerów macierzy. |
|  | Macierz w dostarczonej konfiguracji musi obsługiwać deduplikację i kompresję danych na dyskach wbudowanych w macierzy (nie dopuszcza się główek, kompresji zewnętrznej, programowej itp.) w następujących trybach równocześnie oraz niezależnie na poziomie każdego LUN:   * Sama kompresja wybranego LUN; * Kombinacja technologii kompresji i deduplikacji wybranego LUN; * Brak użycia technologii kompresji i deduplikacji dla wybranego LUN;   Jeżeli do uruchomienia wymaganych funkcjonalności deduplikacji i kompresji są wymagane jakiekolwiek licencje lub elementy hardware wymaga się ich dostarczenia dla maksymalnej obsługiwanej przez macierz pojemności. Deduplikacja i kompresja musi być wspierana przez macierz na dowolnym typie obsługiwanych dysków – co najmniej NL-SAS, SAS, SSD.  Mechanizmy deduplikacji i kompresji muszą być realizowane w tzw. Trybie „Online” to znaczy dane zapisywane na nośniki danych muszą być zapisywane przez kontrolery macierzy od razu w postaci skompresowanej/zdeduplikowanej bezpośrednio w trakcie zapisu danych przez macierz. Dopuszcza się technologię kompresji i deduplikacji w trybie tzw. „Offline” (czyli po uprzednim zapisaniu danych na pośredniczącą warstwę dysków w postaci niezdeduplikowanej i/lub nieskompresowanej) przy wykorzystaniu dedykowanego cache dyskowego SSD pod warunkiem dostarczenia dodatkowej pojemności dysków SSD w konfiguracji RAID 6 lub RAID 10 o pojemności użytecznej minimum równej 25% sumarycznej wymaganej pojemności RAW macierzy (z uwagi na konieczność zachowania odpowiedniej wydajności przy kilkukrotym wzroście pojemności i operacji na macierzy w trakcie cyklu wieloletniego użytkowania sprzętu); |
|  | Macierz musi być wyposażona zabezpieczenie stanu pamięci cache np. na wypadek awarii zasilania – zapis stanu pamięci cache na dyski flash lub równoważny nośnik nie wymagający zasilania. Czas przechowywania kopii pamięci flash nie może być ograniczony czasowo. |
|  | Macierz musi umożliwiać wymianę minimum 1 kontrolera bez konieczności wyłączania zasilania całego urządzenia. |
|  | Macierz posiada minimum 4 dedykowane interfejsy RJ-45 Ethernet 1Gb/s dedykowane dla zdalnej  komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy. |
|  | Każdy z kontrolerów macierzy wyposażony co najmniej w procesor wykonany w technologii wielordzeniowej z minimum 8 rdzeniami. |
|  | Każdy kontroler macierzy pozwala na konfigurację interfejsów niezbędnych dla współpracy w sieci LAN, FC SAN oraz NAS. |
|  | Dla komunikacji blokowej I/O z serwerami oferowany model macierzy wyposażony w oferowaną ilość kontrolerów musi obsługiwać co najmniej następujące protokoły i porty:   * Możliwość instalacji minimum 8 portów SAS 12Gbit/s * Możliwość instalacji minimum 16 portów FC 16Gbit/s * Możliwość instalacji minimum 8 portów iSCSI 10 Gbit/s SFP+ lub RJ-45 * Możliwość instalacji minimum 8 portów iSCSI 1 Gbit/s SFP+ lub RJ-45   Musi istnieć możliwość jednoczesnego wykorzystania różnych typów interfejsów. |
|  | Oferowany model macierzy umożliwia wymianę portów do transmisji danych na porty obsługujące protokoły: iSCSI 1 Gb/s, iSCSI 10Gb/s, FC 16Gb/s, FC 32Gb/s, SAS 12G. Wymiana portów nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu, w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych. |
|  | Dla komunikacji plikowej NAS z serwerami oferowany model macierzy wyposażony w oferowaną ilość kontrolerów musi obsługiwać co najmniej następujące protokoły i porty: CIFS, NFS oraz interfejsy Ethernet 1Gbit/s i 10Gbit/s. Oferowany model macierzy musi umożliwiać jednoczesne użytkowanie portów do komunikacji blokowej i plikowej. W obecnym postępowaniu wymagana jest macierz z aktywnym dostępem blokowym oraz możliwością rozbudowy o dostęp realizowany na poziomie plikowym. |
|  | Oprogramowanie do zarządzania zintegrowane jest z systemem operacyjnym macierzy zarówno przy obsłudze transmisji danych protokołami blokowymi (FC, iSCSI, SAS) jak i do obsługi transmisji protokołami CIFS oraz NFS (nie dopuszcza się tzw główek czy dodatkowych serwerów podłączonych do macierzy w celu realizacji obsługi dostępu protokołami CIFS i NFS do danych znajdujących się na macierzy). |
|  | Macierz jest wyposażona w nadmiarowe mechanizmy badania integralności składowanych danych. |
|  | Macierz obsługuje co najmniej następujące poziomy RAID: 0, 1 ,1+0 , 5 , 50, 6 |
|  | Oferowana macierz wspiera co najmniej następujące typy dysków hot-plug:   * dyski elektroniczne SSD SAS o pojemności minimum 30TB ; * dyski elektroniczne SSD SAS SED lub FDE; * dyski mechaniczne HDD SAS, NL-SAS; * Wszystkie dyski wspierane przez oferowany model macierzy wykonane są w technologii hot-plug i posiadają podwójne porty SAS obsługujące tryb pracy full-duplex |
|  | Model macierzy pozwala na instalację dysków hot-plug w formacie 2,5” i 3,5”. |
|  | Macierz umożliwia skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy) w trybach:   * hot-spare dedykowany dla zabezpieczenia tylko wybranej grupy dyskowej RAID * hot-spare dla zabezpieczenia dowolnej grupy dyskowej RAID lub zapewnia możliwość skonfigurowania równoważnej przestrzeni zapasowej. |
|  | W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk. |
|  | Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą odbywa się w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym. Zdalne zarządzanie macierzą odbywa się bez konieczności instalacji  żadnych dodatkowych aplikacji na stacji administratora. |
|  | Wbudowane oprogramowanie macierzy obsługuje połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI. |
|  | Macierz wyposażona jest w system kopii migawkowych umożliwiających wykonanie minimum 2048 kopii migawkowych – jeżeli funkcjonalność ta wymaga zakupu licencji to należy je dostarczyć w wariancie dla maksymalnej pojemności dyskowej dla oferowanej macierzy. |
|  | Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror). Jeżeli funkcjonalność ta wymaga zakupu licencji to należy ją dostarczyć w wariancie dla maksymalnej pojemności dyskowej dla oferowanej macierzy.  Funkcjonalność musi być objęta wsparciem technicznym producenta macierzy przez okres min. 3 lat, z gwarantowanym czasem reakcji w następnym dniu roboczym od momentu zgłoszenia; |
|  | Macierz umożliwia zdefiniowanie minimum 4096 woluminów LUN. |
|  | Dostarczona macierz w oferowanej konfiguracji umożliwia szyfrowanie danych na zainstalowanych dyskach dowolnego typu – funkcjonalność realizowana bezpośrednio przez kontrolery macierzy dla danych blokowych – minimum AES 256. Jeżeli funkcjonalność ta wymaga dodatkowych elementów sprzętowych bądź aktywacji dodatkowej licencji to należy dostarczyć je wraz z rozwiązaniem dla maksymalnej pojemności macierzy. |
|  | Macierz umożliwia aktualizację oprogramowania wewnętrznego, kontrolerów i dysków bez konieczności wyłączania macierzy i bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych serwerów. |
|  | Macierz umożliwia dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, alokowanie woluminu na inną grupę dyskową. |
|  | Macierz posiada wsparcie dla systemów operacyjnych: MS Windows Server 2016 i 2019, SuSE Linux, RedHat Linux, |
|  | Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath dla połączeń FC i iSCSI. |
|  | Macierz obsługuje woluminy logiczne o maksymalnej pojemności minimum 16TB. |
|  | Macierz umożliwia obsługę mechanizów QoS (ang. Quality of Services) czyli nadawanie priorytetów obsługi transmisji I/O dla skonfigurowanych hostów, LUN-ów, portów do hostów. |
|  | Macierz umożliwia rozproszenie alokacji danych dla pojedynczego woluminu LUN na maksymalnej liczbie obsługiwanych dysków HDD. |
|  | Macierz musi pozwalać na integrację macierzy w środowiskach Vmware w zakresie obsługi mechanizmów: Vmware VAAI, Vmware VVOL, Vmware VASA, Vmware MultiPath IO. |
|  | Wraz z macierzą należy zapewnić wsparcie dla mechanizmów Offloaded Data Transfer i Space Reclamation. |
|  | Macierz musi obsługiwać mechanizmy Thin Provisioning. Jeżeli taka funkcjonalność wymaga dodatkowych licencji to należy je dostarczyć wraz z macierzą dla maksymalnej pojemności dyskowej oferowanej macierzy. |
|  | Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering).Mechanizm ten musi być obsługiwany przy trzech różnych technologiach dyskowych równoczesnie: SSD, SAS, NLSAS. Macierz musi pozwalać na definiowanie minimum 120 różnych polityk i zasad migrowania danych w obrębie tej samej macierzy. Maksymalna wielkość pojedynczego bloku danych podczas migracji i realokacji mechanizmami AST nie może przekraczać 256MB. Mechanizm AST musi pozwalać na wykluczanie wybranych godzin i dni z pomiarów wydajności operacji I/O. Licencja na wymienioną funkcjonalność jest przedmiotem niniejszego postępowania.  Funkcjonalność musi być objęta wsparciem technicznym producenta macierzy przez okres min. 3 lat, z gwarantowanym czasem reakcji w następnym dniu roboczym od momentu zgłoszenia; |
|  | Macierz musi umożliwiać uruchomienie mechanizmów zdalnej replikacji danych z innymi macierzami (ten sam model/rodzina modeli) - w trybie synchronicznym i asynchronicznym - po protokołach FC oraz iSCSI bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji, główek typu serwer/wirtualizator, itp. Funkcjonalność replikacji danych jest zapewniona z poziomu oprogramowania wewnętrznego macierzy. Licencja na wymienioną funkcjonalność jest przedmiotem niniejszego postępowania.  Funkcjonalność musi być objęta wsparciem technicznym producenta macierzy przez okres min. 3 lat, z gwarantowanym czasem reakcji w następnym dniu roboczym od momentu zgłoszenia; |
|  | Model oferowanej macierzy musi wspierać rozwiązania klasy „wysokiej dostępności” tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych po FC lub iSCSI pomiędzy minimum 2 macierzami. Pod użytym pojęciem „wysoka dostępność zasobów dyskowych” należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej.  Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie „wysokiej dostępności”, musi wspierać poziomy RAID: 1,10,5, 6 bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i główną.  Funkcjonalność „wysokiej dostępności” musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover).  Funkcjonalność „wysokiej dostępności” musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover).  Funkcjonalność „wysokiej dostępności” musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback).  Funkcjonalność „wysokiej dostępności” musi wspierać konfiguracje z macierzą zapasową zainstalowaną w innej fizycznej lokalizacji o ile nadal spełnione są warunki dla realizacji synchronicznej replikacji danych pomiędzy lokalizacjami.  Funkcjonalność „wysokiej dostępności” musi wspierać dwukierunkowe przełączanie macierzy podstawowej na zapasową tj. przypadek, gdy każda z tych macierzy obsługuje własne środowisko produkcyjne, a rolę jej macierzy zapasowej pełni druga z macierzy. Licencja na wymienioną funkcjonalność nie jest przedmiotem niniejszego postępowania. |
|  | Macierz dyskowa objęta jest minimum 36 miesięcznym okresem gwarancji producenta z gwarantowanym czasem reakcji najpóźniej następnego dnia roboczego od zgłoszenia usterki. Producent macierzy musi umożliwiać skuteczne zgłaszanie usterek w trybie całodobowym, 7 dni w tygodniu, również w dni świąteczne. Zgłoszenia usterek muszą być akceptowane przez producenta zarówno drogą email (w ofercie należy podać dedykowany adres email serwisu producenta macierzy do zgłoszeń serwisowych) jak również drogą telefoniczną (ogólnie dostępna linia telefoniczna producenta, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny. Nie dopuszcza się numerów specjalnych, komórkowych, o podwyższonej płatności itp.). Linia telefoniczna musi być czynna 24 godziny na dobę, 7 dni w tygodniu również w dni świąteczne. W formularzu ofertowym należy podać pełen adres internetowy strony producenta macierzy, gdzie można zweryfikować dedykowany numer telefonu do obsługi zgłoszeń serwisowych. Wymagane jest oświadczenie Producenta oferowanej macierzy, iż wymagany poziom gwarancji i wsparcia na sprzęt i oferowane wraz z nim oprogramowanie został zaaferowany przez Producenta macierzy na potrzeby oferty w niniejszym postępowaniu |
|  | Serwis gwarancyjny obejmuje dostęp do poprawek i nowych wersji firmware, które są elementem zamówienia przez cały okres obowiązywania gwarancji. |
|  | Macierz musi być zaoferowana z serwisem producenta macierzy, który w przypadku wymiany dysków twardych HDD/SSD, umożliwia pozostawienie wszystkich uszkodzonych nośników u Zamawiającego. Serwis taki musi dotyczyć wszystkich oferowanych półek dyskowych i przewidywać ich uzupełnienie do maksymalnej pojemności poprzez dodanie dowolnych typów obsługiwanych dysków przez macierz bez konieczności ponoszenia żadnych dodatkowych kosztów przez Zamawiającego z tytułu gwarancji „pozostawienie dysku” dla tych dysków zainstalowanych w macierzy jak i dodatkowych dysków możliwych do zainstalowania w obrębie oferowanych półek dyskowych. |
|  | Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu ofertowym należy podać pełen adres internetowy strony producenta macierzy, gdzie można zweryfikować wymagane informacje; |
|  | Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną linię telefoniczną wsparcia technicznego w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej (telefon stacjonarny lub 0-800/0-801 , nie dopuszcza się numerów o podwyższonej płatności - specjalnych, komórkowych, itp.). Linia telefoniczna musi być czynna 24 godziny na dobę, 7 dni w tygodniu również w dni świąteczne. Po podaniu numeru seryjnego macierzy można zweryfikować telefonicznie co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia, jak również zgłosić problem/zapytanie techniczne związane z urządzeniem – w formularzu ofertowym należy podać pełen numer telefonu linii wsparcia technicznego producenta |
|  | Macierz musi umożliwiać konfigurację i uruchomienie dedykowanej funkcji automatycznego powiadomienia serwisu o usterce przez samo urządzenie (poprzez dedykowany system wbudowany w macierz - bez pośrednictwa administratora, nie dopuszcza się użycia ogólnodostępnych mechanizmów - poczty email w tym m.in. protokołu SNMP i SMTP, nie dopuszcza się SMS – Zamawiający nie dopuszcza możliwości komunikacji z/do macierzy poprzez pocztę email/SNMP/SMTP itp. z powodów bezpieczeństwa). Funkcjonalność musi pozwalać na automatyczne otwarcie zgłoszenia serwisowego w bazie serwisowej producenta macierzy zgodnie z wymaganym w specyfikacji poziomem SLA; Opcja ta musi być dostępna bezpłatnie w trakcie całego okresu gwarancji producenta macierzy. Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do macierzy bezpośrednio przez Producenta – musi być do tego wykorzystany dedykowany system serwisowy macierzy. |
|  | Oferowana macierz musi być fabrycznie nowa, Macierz pochodzi z legalnego kanału sprzedaży producenta na terenie Polski i reprezentuje model bieżącej linii produkcyjnej. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych. |
|  | Urządzenie wykonane jest zgodnie z europejskimi dyrektywami RoHS i WEEE. |
|  | Oferowana macierz musi pochodzić z autoryzowanego kanału producenta na terenie Polski oraz być fabrycznie nowa (nie dopuszcza się urządzeń odnawianych, używanych, itp.) |
|  | Przed podpisaniem protokołu ilościowo-jakościowego Wykonawca dostarczy pisemne potwierdzenie wykupienia i uruchomienia gwarancji producenta macierzy obowiązującej na terenie Polski, zgodnej co najmniej z wymaganiami specyfikacji i ze złożoną przez niego ofertą. |

## 3. Przełącznik Fiber Channel - 4 szt.

| **Lp.** | **Element składowy dostawy** | **Ilość i cechy techniczne** |
| --- | --- | --- |
|  | **Ilość portów FC** | Łączna ilość aktywnych portów FC – 24 porty 32Gbit/s Fibre Channel. Rozbudowa nie może odbywać się poprzez zakupu dodatkowych, z wyłączeniem modułów SFP/SFP+ lub kabli, modułów sprzętowych, jedynie poprzez zakup licencji.  W pełni rozbudowany przełącznik nie może zajmować w szafie RACK więcej niż 1U. |
|  | **Przepustowość portu** | Porty uniwersalne o przepustowości 32GB/s, z obsługą przepustowości 4Gbit/s, 8Gbit/s i 16 Gbit/s z automatycznym wyborem przepustowości (auto-sensing), obsługa trybu full-duplex dla wszystkich wspieranych przepustowości. |
|  | **Interfejsy optyczne** | Moduły do transmisji światłowodowej z prędkością min. 16Gbit/s poprzez kabel światłowodowy wielomodowy (Short-Wavelenght) z interfejsem LC, liczba modułów dostosowana do liczby aktywnych portów, możliwość pracy z prędkością min. 16Gbit/s. |
|  | **Inne funkcje i wyposażenie** | 1. 1. Obsługa trybów pracy portów FC: D\_Port, E\_port, F\_port, N-Port. 2. 2. Obsługa funkcji PoD (Ports on Demand) przydziału licencji dla aktywnych portów FC. 3. 3. Aktywne licencje :  * Webtools, * Full Fabric (z obsługą do min. 239 przełączników FC), * Zoning, * Ports on Demand.  1. 4. Możliwość zdalnej aktualizacji firmware’u switcha. 2. 5. Możliwość rozbudowy o funkcjonalności:  * FabricVision, * Extended Fabric, * Inter Switch Link (ISL) z przepustowością maks. 256 Gb/s /ISL.  1. 6. Dedykowany interfejs RJ-45 min 10/100/1000 Mb/s do zarządzania poprzez sieć Ethernet , 2. 7. Możliwość zarzadzania typu in-band poprzez Fibre Channel, 3. 8. Dedykowany interfejs RJ-45 lub DB9 do zarządzania poprzez interfejs szeregowy, dedykowany port USB umożliwiający upgrade FW i zapis logów, 4. 9. Sygnalizacja aktywnych i podłączonych portów na panelu przednim urządzenia, 5. 10. Zarządzanie poprzez przeglądarkę WWW z obsługą połączeń szyfrowanych min. 128-bit SSL oraz poprzez usługę SSH, 6. 11. Zarządzanie poprzez konsole znakową tzw. CLI, 7. 12. Wsparcie dla protokołu SNMP v.3. |
|  | **Kable** | Wraz z urządzeniem należy dostarczyć kabel sieciowy min. CAT 6A RJ-45 o długości min. 3 m. |
|  | **Typ obudowy** | Wysokość przełącznika 1U w systemie montażu w szafie typu rack 19”. Szyny montażowe w zestawie. Wraz z przełącznikiem należy dostarczyć również perforowany panel 1U. |
|  | **Zasilanie/chłodzenie** | Zasilanie z sieci prądu przemiennego o napięciu w zakresie 90- 264V/50-60Hz V, maksymalny pobór mocy podczas pracy urządzenia 77W. |
|  | **Gwarancja/dostawa** | Urządzenie ma być objęte min. 3 letnią gwarancją producenta z czasem reakcji najpóźniej w następnym dniu roboczym od zgłoszenia usterki. |

## 4. Switch – 4 szt.

|  |  |  |
| --- | --- | --- |
|  | **Parametr** | **Wymagania** |
|  | Ilość portów | * Urządzenie musi posiadać minimum 48 portów 10GE definiowanych za pomocą wkładek SFP/SFP+, * Urządzenie musi posiadać min. 4 porty 40G QSFP+, * Aktywne min. 24 porty SFP+, z możliwością aktywowania pozostałych portów przełącznika; * Urządzenie musi obsługiwać wkładki typu 1GE RJ45, 1GE-SX, 1GE-LX, 10GE-SR SFP+, 40 GE-BaseSR4 QSFP+; * Urządzenie musi obsługiwać kable typu 10GE Twinax lub równoważne. * Możliwość rozbudowy przełącznika o obsługę protokołu FCoE; |
|  | Parametry wydajnościowe | * Wymagana jest przepustowość przełączania 1.28 Tbps (data rate, full duplex); * Wymagany rozmiar tablicy MAC to min. 160000; * Maksymalna ilość VLAN min. 4096; * Maksymalna ilość członków vLAG, min. 64; * Maksymalna ilość ACL, min. 13000; |
|  | Wymiary | * Obudowa musi być przeznaczona do montażu w szafie rackowej 19”, szyny montażowe w zestawie; * Wysokość urządzenia maksymalnie 1 RU. |
|  | Implementacja zaleceń IEEE | Urządzenie musi obsługiwać następujące protokoły:   * IEEE 802.1D Spanning Tree Protocol * IEEE 802.1s Multiple Spanning Tree * IEEE 802.3ab 1000BASE-T * IEEE 802.3z 1000BASE-X * IEEE 802.1w Rapid Reconfiguration of Spanning Tree Protocol * IEEE 802.3 Ethernet * IEEE 802.3ad Link Aggregation with LACP * IEEE 802.3ae 10G Ethernet * IEEE 802.1Q VLAN Tagging * IEEE 802.1p Class of Service Prioritization and Tagging * IEEE 802.1v VLAN Classification by Protocol and Port * IEEE 802.1AB Link Layer Discovery Protocol (LLDP) * IEEE 802.3x Flow Control (Pause Frames) |
|  | Link aggregation | Urządzenie musi zapewniać:   * Wsparcie dla LACP |
|  | Mechanizmy Data Center | Urządzenie musi zapewniać:   * Wsparcie dla Data Center Bridging (DCB), * Wsparcie dla FIP snooping, * Wsparcie dla Data Center Bridging Exchange (DCBX), |
|  | Zarządzanie, zabezpieczenia | Urządzenie musi zapewniać:   * Port konsoli RJ-45, * Port RJ45 1000Mbps do zarządzania urządzeniem, * Port USB, * Wsparcie dla SSHv2, * Wsparcie dla NETCONF oraz REST API, * Wsparcie dla RADIUS (AAA), * Wsparcie dla SNMP v2c, v3, * Wsparcie dla Remote monitoring (RMON). |
|  | Zasilanie | * Oferowane urządzenie musi być wyposażone w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej, zamontowane w obudowie przełącznika. |
|  | Moduły SFP oraz SFP+ | * Należy dostarczyć 4 moduły SFP+ 10Gb SR (MM), * Należy dostarczyć 14 modułów Twinax o długości 5m każdy,   Wszystkie moduły SFP/SFP+/QSFP+ muszą znajdować się na liście kompatybilności producenta urządzenia oraz pochodzić z oficjalnego kanału sprzedaży. |
|  | Gwarancja | * 3 lata gwarancji w trybie z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od zgłoszenia usterki. |

## 5. Serwer wirtualizacyjny - 6 szt.

|  |  |  |  |
| --- | --- | --- | --- |
| **LP** | **Parametr lub warunek** | | **Minimalne wymagania** |
| 1 | Obudowa | | -Typu Rack, wysokość maksimum 2U;  -Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack; |
| 2 | Płyta główna | | -Dwuprocesorowa, zaprojektowana i wyprodukowana przez producenta serwera, możliwość instalacji procesorów dwudziestoośmiordzeniowych;  -wyposażona w minimum 24 gniazda pamięci RAM DDR4, obsługa minimum 3000GB pamięci RAM DDR4 2933 Mhz;  -Oferowany model serwera musi obsługiwać pamięć nieulotną instalowaną w gniazdach pamięci RAM;  -Minimum 2 sloty dla dysków M.2 na płycie głównej lub dedykowanej karcie PCI Express - nie zajmujące klatek dla dysków hot-plug; (Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora w slocie M.2 bez zajmowania klatek dyskowych serwera);  -Minimum 2 wolne sloty PCI Express x8 do dalszej rozbudowy serwera, sloty aktywne;  -Zintegrowany moduł TPM 2.0; |
| 3 | Procesory | | -Obsługa procesorów minimum 28-rdzeniowych;  -Zainstalowane dwa procesory 8-rdzeniowe w architekturze x86 osiągające wynik w testach wydajności SPECrate2017\_int\_base min. 125 pkt dla dowolnej platformy dwuprocesorowej producenta serwera(w konfiguracji dwuprocesorowej), który jest oferowany w postępowaniu przez oferenta. Wymagamy aby był załączony PDF ze strony spec.org i poświadczony przez producenta serwera oferowanego w postępowaniu; (nie dopuszcza się procesorów o innej ilości rdzeni fizycznych z uwagi na optymalizację kosztową licencjonowania aplikacji i systemów operacyjnych) |
| 4 | Pamięć RAM | | -Zainstalowane 512GB pamięci RAM typu DDR4 Registered, 2933Mhz w kościach o pojemności 32GB;  -Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC lub równoważnej;  -Wsparcie serwera dla konfiguracji kopii lustrzanej pamięci RAM; |
| 5 | Kontroler RAID | | -Zainstalowany kontroler RAID 0,1 obsługujący dyski montowane z przodu obudowy serwera;  -Zainstalowany dodatkowy osobny kontroler RAID wyposażony w dwa złącza do instalacji dysków M.2 SATA SSD. Kontroler musi wspierać konfigurację poziomu zabezpieczeń RAID 1 na zainstalowanych dyskach M.2 SATA SSD. |
| 6 | Dyski | | -Zainstalowane 2 dyski M.2 SATA SSD o pojemności minimum 240GB każdy, niezajmujące wnęk na dyski z przodu serwera. Dyski zabezpieczone sprzętowo realizowanym poziomem RAID 1;  -Minimum 8 wolnych wnęk dla dysków twardych Hotplug 2,5; |
| 7 | Inne napędy zintegrowane | | Możliwość instalacji wewnętrznego napędu Blue-ray (odczyt/zapis) (dopuszcza się dostarczenie napędu zewnętrznego pod warunkiem objęcia serwisem o jednakowych parametrach z wymaganymi dla całego serwera) |
| 8 | Kontrolery LAN | | -Jedna dwuportowa karta 2x1Gbit/s ze wsparciem iSCSI, niezajmująca slotu PCI Express;  -Dodatkowa osobna karta 4x10Gbit/s SFP+, niezajmująca slotu PCI Express (dopuszcza się instalację kart w slocie PCI Express pod warunkiem dostarczenia serwera z większą niż wymagana ilością slotów PCI Express)  -Wraz z serwerem należy dostarczyć min. 4szt kabli DAC SFP+ (Twinax) o długości min. 3 m. Kable muszą być w pełni kompatybilne z wymaganą kartą 10Gb SFP+; |
| 9 | Kontrolery FC | | -Jedna dwuportowa karta FC x16Gb Qlogic; |
| 10 | Porty | | -zintegrowana karta graficzna ze złączem VGA;  -2x USB 3.0 dostępne na froncie obudowy  -2x USB 3.0 dostępne z tyłu serwera  -1x USB 3.0 wewnątrz serwera  -dodatkowe złącze VGA dostępne z przodu serwera;  Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera; |
| 11 | | Zasilanie, chłodzenie | -Redundantne zasilacze hotplug o mocy maksymalnej 800W, o sprawności 96% (tzw. klasa Titanium)  -Redundantne wentylatory hotplug;  -Należy dostarczyć kable zasilające C13-C14 o długości min. 4m każdy; |
| 12 | | Zarządzanie | -Wbudowane diody informacyjne informujące o stanie serwera;  -Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:   * Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; * Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; * Dostęp poprzez przeglądarkę Web (także SSL, SSH) * Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii * Zarządzanie alarmami (zdarzenia poprzez SNMP) * Możliwość przejęcia konsoli tekstowej * Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) * Karta zarządzająca musi sprzętowo wspierać wirtualizację warstwy sieciowej serwera, bez wykorzystania zewnętrznego hardware - wirtualizacja MAC i WWN na wybranych kartach zainstalowanych w serwerze (co najmniej wsparcie dla technologii kart 10Gbit/s Ethernet i kart FC 16Gbit/s oferowanych przez producenta serwera) * Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.). * Dedykowana, wbudowana w kartę zarządzającą pamięć flash o pojemności minimum 16 GB * Rozwiązanie musi umożliwiać instalację obrazów systemów, własnych narzędzi diagnostycznych w obrębie dostarczonej dedykowanej pamięci (pojemność dostępna dla obrazów własnych – minimum 8,5GB); * Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania; * Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; * Możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji; * Rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory, kontrolery RAID, karty rozszerzeń); * Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą; * Karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego w systemie producenta serwera). Jeżeli są wymagane jakiekolwiek dodatkowe licencje lub pakiety serwisowe potrzebne do uruchomienia automatycznego powiadamiania autoryzowanego serwisu o usterce należy takie elementy wliczyć do oferty – czas trwania minimum równy dla wymaganego okresu gwarancji producenta serwera; |
| 13 | | Wspierane OS | - Windows 2019 Hyper-V, Windows 2016 Hyper-V, VMWare 6.7 U2, U3 |
| 14 | | Gwarancja | -Minimum 3 lata gwarancji producenta serwera z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od zgłoszenia usterki; możliwość realizacji zgłoszeń serwisowych 7 dni w tygodniu , 24h na dobę.  -Zaoferowany serwis musi umożliwiać konfigurację automatycznego powiadamiania serwisu producenta (otwierania zgłoszenia serwisowego wg obowiązującego SLA) o przewidywanej bądź istniejącej usterce;  -Dostępność części zamiennych przez 5 lat od momentu zakupu serwera;  -Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji;  Zamawiający wymaga 3 form zgłoszeń serwisowych: telefonicznie (polska i polskojęzyczna infolinia producenta serwera, Formularz zgłoszeniowy online producenta serwera oraz adres email producenta serwera. Zamawiający będzie weryfikował podane dane w tym celu należy dostarczyć link www w ofercie pod którym Zamawiający odnajdzie podane formy zgłoszeń serwisowych. |
| 15 | | Dokumentacja, inne | -Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA (wymagane oświadczenie producenta serwera potwierdzające spełnienie wymagań dołączone do oferty).  -Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce - Wymagane oświadczenie producenta serwera, że oferowany do przetargu sprzęt spełnia ten wymóg;  -Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu;  -Ogólnopolska, polskojęzyczna telefoniczna infolinia/linia techniczna producenta serwera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;  -Wymagane jest oświadczenie Producenta oferowanego serwera, iż wymagany w postepowaniu poziom gwarancji i wsparcia na sprzęt na terenie Polski został zaaferowany przez Producenta serwera na potrzeby oferty w niniejszym postępowaniu;  -Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; |

## 6. Rozwiązanie UTM – szt. 2

# **Wymagania Ogólne**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

# **Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.
5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

# **Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall musi dysponować minimum:

* 20 portami Gigabit Ethernet RJ-45.
* 2 gniazdami SFP 1 Gbps.

1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System musi być wyposażony w zasilanie AC.

# **Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 2 mln. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 7 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 4 Gbps dla pakietów 64 B.
4. Przepustowość Stateful Firewall: nie mniej niż 7 Gbps dla pakietów 1518 B.
5. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1 Gbps.
6. Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps.
7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 500 Mbps.
8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps.
9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 130 Mbps.

# **Funkcje Systemu Bezpieczeństwa:**

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów: SMTP, POP3
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.

# **Polityki, Firewall**

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.

* Amazon Web Services (AWS).
* Microsoft Azure
* Cisco ACI.
* Google Cloud Platform (GCP).
* Nuage Networks VSP.
* OpenStack.
* VMware vCenter (ESXi).
* VMware NSX.

# **Połączenia VPN**

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

* Wsparcie dla IKE v1 oraz v2.
* Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19 i 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.

1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

# **Routing i obsługa łączy WAN**

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

* Routingu statycznego.
* Policy Based Routingu.
* Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

# **Zarządzanie pasmem**

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

# **Ochrona przed malware**

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

# **Ochrona przed atakami**

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

# **Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

# **Kontrola WWW**

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
7. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
8. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

# **Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

# **Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

# **Logowanie**

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

# **Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

* ICSA lub EAL4 dla funkcji Firewall.

# **Serwisy i licencje**

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a)     Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

b)     Kontrola Aplikacji, IPS, Antywirus, Analiza typu Sandbox (z uwzględnieniem sygnatur do ochrony urządzęń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

# **Gwarancja oraz wsparcie**

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

* Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne  o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
* Certyfikat ISO 9001 podmiotu serwisującego.

## **7. Wymagania dla wirtualizatora**

|  |  |
| --- | --- |
| 1 | Wraz ze sprzętem należy dostarczyć oprogramowanie do wirtualizacji. Dostarczane oprogramowanie musi być w najnowszej wersji obecnie dostępnej na rynku. |
| 2 | Licencje powinny umożliwiać uruchomianie wirtualizacji na serwerach fizycznych o łącznej liczbie 6 procesorów oraz jednej licencji konsoli do zarządzania całym środowiskiem. Centralna konsola tego samego producenta co oprogramowanie do wirtualizacji |
| 3 | Wszystkie licencje powinny być dostarczone wraz z 3 letnim wsparciem technicznym, w trybie, w następnym dniu roboczym |
| 4 | Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych |
| 5 | Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. |
| 6 | Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji. |
| 7 | Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć  i wykorzystać procesory fizyczne wyposażone w 768 logicznych wątków oraz do 16TB pamięci fizycznej RAM. |
| 8 | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych. |
| 9 | Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB. |
| 10 | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych  z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM. |
| 11 | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych. |
| 12 | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe. |
| 13 | Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. |
| 14 | Rozwiązanie musi wspierać następujące systemy operacyjne: MS-DOS 6.22, Windows XP, Windows Vista, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows 7, Windows 8, SLES 12, SLES 11, SLES 10, SLES 9, SLES 8, REHL 7, RHEL 6, RHEL 5, RHEL 4, RHEL 3, REHL Atomic 7, Solaris 11 ,Solaris 10, Solaris 9, Solaris 8, OS/2 Warp 4.0, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu, SCO OpenServer, SCO Unixware, Mac OS X, Photon OS, eCommStation 1/2/2.1, Oracle Linux , CoreOS, NeoKylin |
| 15 | Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. |
| 16 | Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. |
| 17 | Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi oraz serwerami fizycznymi z zainstalowanym oprogramowaniem wirtualizacyjnym. Centralna konsola graficzna powinna mieć możliwość działania zarówno, jako aplikacja na maszynie fizycznej lub wirtualnej, jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. |
| 18 | Oprogramowanie do centralnego zarządzania musi posiadać możliwość zarządzania min. 1000 serwerów fizycznych z zainstalowanym oprogramowaniem wirtualizacyjnym. |
| 19 | Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. |
| 20 | Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. |
| 21 | Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. |
| 22 | Rozwiązanie musi zapewnić wbudowany, bezpieczny mechanizm do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych. Mechanizm ten musi umożliwiać również odtwarzanie pojedynczych plików z kopii zapasowej oraz zapewnia stosowanie deduplikacji dla kopii zapasowych. Mechanizm zapewnia możliwość wykonywania spójnych kopii zapasowych serwerów aplikacyjnych (Microsoft SQL Server, Microsoft Exchange Server, Microsoft SharePoint Server) oraz replikację kopii zapasowych. |
| 23 | Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych. |
| 24 | Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie. |
| 25 | Rozwiązanie musi mieć możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych w czasie ich pracy pomiędzy fizycznymi zasobami dyskowymi. |
| 26 | Przy konfiguracji wysokiej dostępności (HA) musi zostać zapewniona odpowiednia redundancja i taki mechanizm, aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. |
| 27 | Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny, które na nim pracowały, były bezprzerwowo dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym. Mechanizm ten umożliwia zabezpieczenie maszyn wirtualnych wyposażonych w minimum 2 wirtualne procesory. |
| 28 | System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów. |
| 29 | Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. |
| 30 | Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). |

## **8. System operacyjny serwerów wirtualizacyjnych**

Dla każdej z dwóch lokalizacji:

Oprogramowanie musi zostać dostarczone dla trzech serwerów fizycznych w poniższej konfiguracji:

Serwer 1 : **2 procesory o sumarycznej ilości 16 rdzeni obliczeniowych;**

Serwer 2 : **2 procesory o sumarycznej ilości 16 rdzeni obliczeniowych;**

Serwer 3 : **2 procesory o sumarycznej ilości 16 rdzeni obliczeniowych;**

Licencje na serwerowy system operacyjny muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Dostarczane oprogramowanie musi być w najnowszej, obecnie dostępnej wersji na rynku.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.

2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.

3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.

4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.

6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.

7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.

8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.

9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:

a. pozwalają na zmianę rozmiaru w czasie pracy systemu,

b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,

c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,

d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).

10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET

13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.

14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:

a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.

16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,

17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.

18. Mechanizmy logowania w oparciu o:

a. Login i hasło,

b. Karty z certyfikatami (smartcard),

c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),

19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..

20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).

21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.

23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).

24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.

25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,

b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,

ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,

iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.

iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1

c. Zdalna dystrybucja oprogramowania na stacje robocze.

d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej

e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

i. Dystrybucję certyfikatów poprzez http

ii. Konsolidację CA dla wielu lasów domeny,

iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

f. Szyfrowanie plików i folderów.

g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.

i. Serwis udostępniania stron WWW.

j. Wsparcie dla protokołu IP w wersji 6 (IPv6),

k. Wsparcie dla algorytmów Suite B (RFC 4869),

l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:

i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.

iii. Obsługi 4-KB sektorów dysków

iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra

v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.

vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.

27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).

28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

## **9.** **System kopii zapasowych**

Wymagania ogólne

* Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,
* Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5 oraz 6.7 oraz Microsoft Hyper-V 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
* Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
* Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
* Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V
* Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

Całkowite koszty posiadania

* Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
* Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
* Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)
* Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
* Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
* Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
* Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
* Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
* Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
* Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
* Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

Wymagania RPO

* Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
* Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
* Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
* Oprogramowanie musi wspierać kopiowanie plików na taśmy
* Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
* Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
* Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
* Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
* Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
* Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V
* Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
* Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere
* Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)

Wymagania RTO

* Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.
* Dodatkowo dla środowiska vSphere powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
* Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
* Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
* Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
* Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
* Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
* Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
* Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
  + **Linux** 
    - ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
  + **BSD** 
    - UFS, UFS2
  + **Solaris** 
    - ZFS, UFS
  + **Mac** 
    - HFS, HFS+
  + **Windows** 
    - NTFS, FAT, FAT32, ReFS
  + **Novell OES** 
    - NSS
* Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
* Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
* Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects").
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze.
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze.
* Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Ograniczenie ryzyka

* Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.

Monitoring

* System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
* System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.x oraz 6.x – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
* System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
* System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware
* System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
* System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
* System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
* System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
* System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
* System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
* System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
* System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
* System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
* System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
* System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
* System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
* System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
* System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 8.x i 9.x

Raportowanie

* System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.x oraz 6.x vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019
* System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
* System musi być certyfikowany przez VMware i posiadać status „VMware Ready”
* System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
* System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
* System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
* System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
* System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
* System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
* System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
* System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
* System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
* System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
* System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
* System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
* System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)

System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

## **10. Tablet ratownika –** 9 sztuk

1. Urządzenie fabrycznie nowe
2. Gwarancja 24 miesiące door-to-door
3. Przekątna ekranu co najmniej 7 cali
4. Pamięć wbudowana co najmniej 16 GB
5. Pamięć operacyjna co najmniej 3 GB
6. Moduły łączności co najmniej LTE, Wi-Fi, Bluetooth
7. System operacyjny Android
8. Nawigacja GPS i GLONASS
9. Wspomagana nawigacja GPS – AGPS
10. Wyposażony we wzmocnioną obudowę
11. Stopień ochrony co najmniej IP 68
12. Spełniający wymagania standardu MIL-STD-810G
13. Wyposażony przednią oraz tylną kamerę
14. Wyposażony w dedykowany rysik umożliwiający pełną obsługę tabletu w rękawicach
15. Wyposażony w uchwyt umożliwiający przenoszenie na przedramieniu
16. Tablet wraz z akcesoriami zabezpieczony w walizce transportowej wyłożonej od wewnątrz gąbką amortyzującą. Walizka powinna spełniać wymagania standardu MIL-STD-810G

## **11. Komputer dowódcy –** 9 sztuk

1. Urządzenie fabrycznie nowe
2. Gwarancja 24 miesiące door-to-door
3. Komputer typu laptop klasy gamingowej
4. Procesor co najmniej 6 rdzeniowy
5. Pamięć operacyjna co najmniej 32 GB
6. Dysk SSD o pojemności co najmniej 512 GB
7. Komputer wyposażony we wbudowane głośniki, mikrofon oraz kamerę
8. Dedykowana karta graficzna
9. Pamięć karty graficznej co najmniej 6 GB GDDR6
10. Łączność co najmniej LAN, Wi-Fi, Bluetooth
11. Wyposażony w system operacyjny zgodny z dotychczas wykorzystywanym systemem użytkownika końcowego
12. Wyposażony w co najmniej dwa porty USB
13. Wyposażony w co najmniej jeden port HDMI
14. Przekątna ekranu co najmniej 17 cali, matryca matowa
15. Komputer wyposażony w bezprzewodową myszkę
16. Komputer wraz z zasilaczem i myszką zabezpieczony w walizce transportowej wyłożonej od wewnątrz gąbką amortyzującą. Walizka powinna spełniać wymagania standardu MIL-STD-810G.

## **12. Kamera nasobna ratownika –** 18 sztuk

1. Urządzenie fabrycznie nowe
2. Gwarancja 24 miesiące door-to-door
3. Rozdzielczość matrycy co najmniej 12 Mpix
4. Rozdzielczość filmów co najmniej FullHD
5. Łączność Wi-Fi, Bluetooth
6. Stopień ochrony co najmniej IP68
7. Możliwość przekazywania obrazu kamery w trybie live
8. Bateria co najmniej 1200 mAh
9. W zestawie akcesoria umożliwiające łatwe przenoszenie kamery w ręku, na klatce piersiowej oraz na głowie.
10. Kamera wraz z akcesoriami zabezpieczona w walizce transportowej wyłożonej od wewnątrz gąbką amortyzującą. Walizka powinna spełniać wymagania standardu MIL-STD-810G.

# **II. Część aplikacyjna**

## **1. Opis wymagań, które ma spełniać aplikacja SWDP**

|  |  |
| --- | --- |
| L.p. | Wymagania |
|  | Systemu Wymiany Danych Pomiarowych (SWDP) przeznaczony jest dla wybranych Specjalistycznych Grup Ratownictwa Chemiczno – Ekologicznego (SGR CHEM-EKO) jako system pozwalający na szybką wyminę danych pomiarowych, danych geoprzestrzennych, informacji opisowych, wszelkiego rodzaju plików oraz przekazu obrazu z miejsca zdarzenia, a także zapewnienia łączności audio pomiędzy ratownikami na miejscu zdarzenia, a specjalistami Centralnej Jednostki Analitycznej (CJA) i ekspertami zewnętrznymi (zwanych dalej ekspertami). |
|  | SWDP ma zapewnić:   * gromadzenie, archiwizowanie i wymianę wyników pomiarów oraz informacji powiązanych z akcjami ratownictwa chemicznego, pomiędzy Specjalistycznymi Grupami Ratownictwa Chemiczno-Ekologicznego (SGR CHEM-EKO) i ekspertami z całego kraju włączonymi do działań, * tworzenie bazy wiedzy dostępnej dla wszystkich uczestników współpracujących w ramach systemu, * tworzenie meldunków z akcji realizowanych przez SGR CHEM-EKO wraz z wizualizacją na mapach miejsc wykonania pomiarów, zawierających zdjęcia, filmy, wyniki analiz i wszystkie inne potrzebne informacje, które mogą być wykorzystane w przyszłości do usuwania zagrożeń w innych miejscach kraju, * dostęp do systemu przez specjalistów CJA, jak i ekspertów zewnętrznych, niebędących bezpośrednio na miejscu działań, a zapewniających wiedzę merytoryczną potrzebną ratownikom prowadzącym działania, |
|  | Umożliwienie współpracy ekspertów poprzez:   * transmisję obrazu „na żywo” z miejsca akcji do ekspertów, * dwustronną łączność pomiędzy ratownikami prowadzącymi działania i ekspertami, * dwustronną wymianę plików (np. zdjęć, schematów, danych pomiarowych, widm spektralnych) pomiędzy ratownikami i ekspertami, * użycie kamer nasobnych przeznaczonych do pracy w strefie zagrożenia chemicznego, które mogą zostać poddane procesowi dekontaminacji, * użycie tabletów przeznaczonych do pracy w strefie zagrożenia chemicznego, które mogą zostać poddane procesowi dekontaminacji, * użycie sprzętu transmisji danych (zainstalowanego na wytypowanych pojazdach ratowniczych), zapewniającego pewną i bezpieczną transmisję danych do i z miejsca akcji. |
|  | Zadania postawione przed SWDP: |
|  | Dane zbierane automatycznie:   * data, czas, * pozycja GPS, * dane pomiarowe wysyłane z połączonych urządzeń pomiarowych, * strumień wideo z kamer nasobnych |
|  | Dane wprowadzane ręcznie:   * autoryzacja użytkownika (autoryzacja bez wykorzystania danych osobowych, np. nr identyfikacyjny funkcjonariusza) * identyfikacja numeru roty pracującej w strefie, * opis okoliczności zdarzenia (w trakcie dojazdu), * opis sytuacji zastanej, * archiwizacja trasy (pozycji GPS w czasie) przemieszczania się ratownika, * oznaczanie pozycji GPS (oznaczonej czasem), * oznaczanie trasy pomiędzy pozycjami GPS * oznaczanie obszaru między pozycjami GPS, * lokalizacja na mapie * oznaczanie punktów na mapie, * oznaczanie trasy na mapie, * oznaczanie obszarów na mapie * wizualizacja lokalizacji oraz punktów, tras i obszarów wprowadzanych ręcznie jak i z pozycji GPS * wyniki pomiarowe urządzeń będących w bazie wprowadzane ręcznie, * wyniki pomiarowe z urządzeń zewnętrznych/“cywilnych”, * robienie zdjęć z możliwością tytułowania oraz robienia opisu, zdjęcie oznaczone czasem i pozycją GPS, * wprowadzanie pobranych próbek oznaczonych czasem, pozycją GPS, tytułem/numerem, opisem, zdjęciem * przeszukiwanie w wielu wyszukiwarkach równocześnie, * przeszukiwanie zdarzeń będących w bazie (np. po nazwie , po okolicznościach, po właściwościach, po wynikach pomiarowych itp.) * określenie środków ochrony indywidualnej ŚOI, * znakowanie rozpoczęcia pracy w strefie oraz jej zakończenia |
|  | Funkcjonalności dodatkowe   * szybkie wyszukiwanie informacji w wielu bazach, * szybki dostęp do procedur, * możliwość poproszenie o wsparcia eksperckie z możliwością doprecyzowania zakresu wsparcia (analiza widm, analiza wyników, zasady postępowania, itp.), * możliwość poproszenia o wsparcie Eksperta zewnętrznego z określeniem formy przesłania zaproszenia (SMS, e-mail), * akceptacja wsparcia eksperckiego, * zmiana zakresu dostępu do informacji dla Eksperta w trakcie prowadzonych prac * odtworzenie obrazu z kamer wpiętych do systemu (dronów, robotów kamer na samochodach PSP) wpięcie za pomocą kabla HDMI, audio wideo, z rejestratorów CBRN-lab, SDł?) * komunikator tekstowy z Ekspertem oraz Dowódcą SGR CHEM-EKO, * komunikator głosowy z Ekspertem oraz dowódcą SGR CHEM-EKO, * przekazywanie i udostępnianie plików * otrzymywanie tras lub punktów, gdzie ma się ratownik udać, * wysyłanie komunikatu “RATUNEK” * otrzymywanie komunikatu “NATYCHMIASTOWY POWRÓT” * archiwizacja wideo oraz audio, * monitorowanie czasu pracy ratownika, * szacowanie pozostałego czasu pracy ratownika w strefie na podstawie danych wprowadzonych wcześniej do bazy w zależności od ŚOI oraz czynnika skażającego, * ostrzeganie o kończącym się czasie pracy w strefie, * informacja o wszystkich osobach pracujących na bieżącym zdarzeniu, * Lista możliwych opcji: udostępnienie dokumentu (np. pliku PDF), udostępnienie grafiki, udostępnienie obrazu z kamery eksperta, transmisja audio, odebranie dokumentów i obrazów od meldunkowego, odebranie transmisji video od ratowników (podgląd on-line), komunikacja audio z ratownikiem (on-line), pobranie aktualnych wyników pomiarów od ratownika, pobranie wcześniejszych wyników pomiarów (znajdujących się już w systemie), podgląd mapy sytuacyjnej (możliwość oznaczenia/wskazania punktów na mapie). |
|  | Systemu SWDP ze względu na miejsce pracy operatora oraz jego uprawnienia i możliwe w obsłudze funkcjonalności dzieli się na trzy podstawowe moduły:   * Moduł 1 przeznaczony jest dla ratownika pracującego na miejscu zdarzenia w strefie zagrożenia, którego podstawową funkcją jest gromadzenie jak największej ilości danych o zdarzeniu chemicznym z wykorzystaniem mobilnej platformy. * Moduł 2 przeznaczony jest dla ratownika/dowódcy pracującego na miejscu zdarzenia poza strefą zagrożenia w okolicach samochodu rozpoznania chemicznego na którym zainstalowany zostaną urządzenia zapewniającą łączność on-line , budować własną sieć WiFi, Podstawową funkcją modułu jest gromadzenie oraz przetwarzanie danych o zdarzeniu chemicznym, a także nawiązywanie współpracy z ekspertami i specjalistami wspierającymi działania zdalnie. * Moduł 3 przeznaczony jest dla specjalistów i ekspertów łączących się z systemem SWDP zdalnie i wspierających wiedzą, a także udostępnienie specjaliście i ekspertowi dużychmocy obliczeniowych na potrzeby np. analizy widm mieszanin wielu substancji, gdzie zdolności obliczeniowe mają wielki wpływ na czas uzyskania wyniku. |
|  | Pracę w systemie SWDP posiadają jedynie użytkownicy, którym nadano login, hasło i określono uprawnienia. |
|  | Sposoby nadawania uprawnień dostępowych do SWDP:  Użytkownikowi tymczasowemu   * login, hasło oraz uprawnienia i zakres dostępu do danych EKSPERTOWI ZEWNĘTRZNEMU nadaje każdorazowo do danej akcji i odbiera, ratownik/dowódca będący na miejscu zdarzenia proszący o wsparcie lub * login, hasło oraz uprawnienia i zakres dostępu do danych EKSPERTOWI ZEWNĘTRZNEMU nadaje każdorazowo do danej akcji i odbiera, specjalista CJA proszący o wsparcie eksperta zewnętrznego,   Użytkownikowi stałemu   * login, hasło oraz uprawnienia i zakres dostępu do danych SPECJALIŚCIE CJA nadaje i odbiera Dowódca JRG, Zastępca Dowódcy JRG na bazie których funkcjonuje CJA oraz administrator SWDP, * login, hasło oraz uprawnienia i zakres dostępu do danych DOWÓDCY JRG i ZASTĘPCY DOWÓDCY JRG NA BAZIE KTÓRYCH FUNKCJONUJĄ CJA nadaje i odbiera administrator SWDP, * login, hasło oraz uprawnienia i zakres dostępu do danych DOWÓDCY SGR CHEM-EKO i ZASTĘPCY DOWÓDCY SGR CHEM-EKO nadaje i odbiera administrator SWDP, * login, hasło oraz uprawnienia i zakres dostępu do danych RATOWNIKOM SGR CHEM-EKO nadaje i odbiera Dowódca SGR CHEM-EKO, Zastępca Dowódcy SGR CHEM-EKO i administrator SWDP. |
|  | Tworząc użytkownika tymczasowego system SWDP rejestruje:   * nazwisko i imię użytkownika, * instytucję/firmę jaką użytkownik reprezentuję, * login literowo cyfrowy składający się z przedrostka „e-„ oraz numeru kolejnego np: „E-3”, „E-61”, „E-325”, „E-8461”, „E-62541” * hasło literowo cyfrowe składające się co najmniej z 6 znaków, * ID zdarzenia do którego ekspert uzyskał dostęp. |
|  | Tworząc użytkownika stałego system SWDP rejestruje:   * nazwisko i imię użytkownika, * login, czyli indywidualny numer funkcjonariusza każdego z użytkowników systemu SWDP, login może zawierać cyfry i litery – do 10 znaków, (sposób kodowania loginów Zamawiający przekaże Wykonawcy na jego wniosek w trakcie realizacji zamówienia), * jednostkę organizacyjną do której przynależy (SGR CHEM-EKO, CJA), wybierane z listy rozwijanej, * telefon kontaktowy (funkcjonalność dla specjalistów CJA), * adres e-mail (funkcjonalność dla specjalistów CJA), * oznaczenie statusu: aktywny, nieaktywny wybierane z listy rozwijanej (domyślnie aktywny), * system pełnienia służby: zmian 1, zmiana 2, zmiana 3, codzienny wybierane z listy rozwijanej. |
|  | Tabelę z zestawieniem użytkowników widzi osoba mająca uprawnienia do nadawania loginów tylko użytkowników którym może edytować dane. |
|  | Nadawanie/generowanie hasła:   * Użytkownikowi tymczasowemu nadawany jest automatycznie razem z generowaniem loginu, * Użytkownikowi stałemu hasło generowane jest automatycznie podczas tworzenia użytkownika w systemie. Hasło to jest jednorazowe i podczas pierwszego logowania musi zostać zmienione na hasło wprowadzone przez użytkownika osobiście. System musi przewidywać możliwość resetowania hasła z jednoczesnym generowaniem hasła jednorazowego |
|  | Tworzenie Baza danych urządzeń pomiarowych i analitycznych:  Wykonawca wprowadzi do systemu SWDP urządzenia pomiarowe wykorzystywane przez Użytkownika końcowego. Baza ta musi zawierać co najmniej:   * producenta urządzenia, * nazwa urządzenia * model urządzenia * nr seryjny urządzenia, * datę ważności legalizacji: kalibracji/ wzorcowania   dla urządzeń zwracających wynik numeryczny:   * ilość sensorów (dla detektorów wielogazowych) * rodzaj sensorów (wykrywane gazy, zakres pomiarowy, czułość) * jednostką wyniku * datę kalibracji   Informację o wykorzystywanych urządzeniach pomiarowych Zamawiający przekaże na wniosek Wykonawcy w trakcie realizowania zamówienia. |
|  | System SWDP gromadzi wszystkie dane jakie ma przetwarzać grupując je w zdarzenia – akcje ratowniczo-gaśnicze. Każde zdarzenie identyfikowane jest przez co najmniej datę rozpoczęcia oraz numer ewidencyjny zdarzenia. |
|  | Strumień obrazu wideo z kamer nasobnych jest przesyłany i gromadzony na serwerach w maksymalnej jakości lub w jakości zdefiniowanej przez Użytkownika końcowego. Materiał ten ma być przechowywany minimum przez 240 godzin. Należy przewidzieć możliwość przechowywania 4400 godzin materiału w jakości 4K 30fps. |
|  | Każde nowe zdarzenie dostaje automatyczny numer tymczasowy. |
|  | Do każdej akcji ratowniczo-gaśniczej można dopisać jedno lub wiele zdarzeń z numerem tymczasowym. |
|  | Każda akcja ratowniczo-gaśnicza identyfikowana jest co najmniej przez datę rozpoczęcia oraz numer informacji ze zdarzenia. |
|  | Moduł 1 przeznaczony jest dla ratownika pracującego na miejscu zdarzenia w strefie zagrożenia. |
|  | Wykonawca musi uwzględnić, że ratownik pracujący w strefie zagrożenia obsługujący elementy systemu będzie ubrany w jeden z poniższych zestawów:   * ubraniach ochronnych kat. typ 1a z aparatem ochrony dróg oddechowych wewnątrz lub * ubraniach ochronnych kat. typ 3 z aparatem ochrony dróg oddechowych na zewnątrz lub * ubraniach ochronnych kat. typ 3 z systemem filtrowentylacji wymuszone lub * ubraniach ochronnych kat. typ 3 z maską z filtropochłaniaczem lub * ubranie specjalne (typu nomex) z aparatem ochrony dróg oddechowych lub * ubranie specjalne (typu nomex ) z maską z filtropochłaniaczem lub * ubranie specjalne (typu nomex) bez maski. |
|  | Tablet i kamera nasobna musi być w pełni dekontaminowalna oraz musi mieć możliwość obsługi w grubych chemoodpornych rękawicach. |
|  | Kamera ma mieć możliwość założenia/przyczepienie na ubranie. |
|  | Tablet najlepiej z mocowaniem na przedramieniu. poszczególne ekran muszą być czytelne i łatwe do wyboru w trudnych warunkach (duże czytelne przyciski). Dane numeryczne wprowadzane przy użyciu klawiatury numerycznej. Przycisk powrotu do poprzedniego ekranu. |
|  | System musi mieć możliwość funkcjonowania bez dostępu do internetu (z oczywistymi ograniczeniami), a w sytuacji odzyskania połączenia bieżącej synchronizacji. System w sytuacji utraty łączności GSM z internetem ma podejmować próby łączności z siecią WiFi samochodu lub Dowódcy SGR CHEM-EKO. |
|  | Wszystkie dane wprowadzane przez RATOWNIKA mają być w pełni identyfikowalne. |
|  | Na wszystkich ekranach aplikacji mobilnej:   * w lewym górnym rogu ma byś podana „lokalizacja w aplikacji”, czyli opis na jakim ekranie obecnie ratownik się znajduje, * w prawym górnym rogu ma byś wyświetlona data, godzina, współrzędne GPS, siłą sygnału WiFi, siłą sygnału GSM, siłą sygnału GPS. |
|  | UWAGA:  Poniżej przedstawiono podstawowe minimalne zadania aplikacji w formie rozpisanej funkcjonalności aplikacji. Wykonawca może zaproponować zamawiającemu inne bardziej ergonomiczne lub bardziej funkcjonalne rozwiązania, na które zamawiający musi wyrazić zgodę. |
|  | Po włączeniu tableta aplikacja systemu SWDP uruchamia się tak jak inne aplikacje bezpośrednio z pulpitu. Po uruchomieniu pojawia się ekran logowania [00].Na ekranie logowania ma znajdować się co najmniej:   * [01] miejsce wprowadzania loginu użytkownika, * [02] miejsce wprowadzania hasła, * [03] przycisk Zaloguj, * [04] przycisk Nowe zdarzenie, * [05] przycisk Zdarzenie w trakcie realizacji, * [06] przycisk Zdarzenie archiwalne. |
|  | Do czasu poprawnego zalogowania przyciski [04], [05], [06] pozostają nieaktywne. |
|  | Po zalogowaniu aktywują się przyciski [04], [05], [06] |
|  | Po wciśnięciu przycisku [04] aktywuje się ekran Nowe zdarzenie, na którym ma znajdować się co najmniej:   * [04.1] miejsce na wprowadzeniu nazwy miejscowości z dookreśleniem powiatu i województwa, * [04.2] miejsce na wprowadzeniu nazwy ulicy, numeru domu, numeru mieszkania, * [04.3] przycisk Rodzaju zdarzenia, * [04.4] przycisk Miejsce zdarzenia, * [04.5] przycisk Nr informacji ze zdarzenia, * [04.6] miejsce na wprowadzeniu Opisu zgłoszenia * [04.9] przycisk Anuluj, * [04.10] przycisk START,   Uwaga:  Na tym ekranie Wykonawca ma przewidzieć możliwość wprowadzenia jeszcze co najmniej 2 przycisków o dowolne funkcjonalności. Funkcjonalności te będą mogły być określone w kolejnym etapie rozwoju SWDP, nie objętym obecnym postępowaniem. |
|  | Wpisując nazwę miejscowości [04.01] i nazwę ulicy [04.02] aplikacja ma podpowiadać pełną nazwę oraz wprowadzone dane ma być w łatwy sposób identyfikowalne na mapie aplikacji. |
|  | Po wciśnięciu przycisku [04.3] Rodzaj zdarzenia pojawia się zdefiniowana lista do wyboru. Lista Rodzajów zdarzenia zawiera co najmniej:   * Pożarowe * Wybuchowe * Chemiczne * Ekologiczne * Radiacyjne (nuklearne) * Biologiczne * nieznane   Uwaga:  Wykonawca ma przewidzieć możliwość wprowadzenia zmian przez administratora SWDP w podanej liście w fazie eksploatowania systemu. |
|  | Po wciśnięciu przycisku [04.4] Miejsce zdarzenia pojawia się zdefiniowana lista do wyboru. Lista Miejsca zdarzenia zawiera co najmniej:  1 W komunikacji:  1.1 Drogowej  1.2 Kolejowej   * 1. Lotniczej   2. Wodnej:      1. Śródlądowej   1.4.2 Morskiej  2 Obiekty (budynki):  2.1 Zakłady (magazyny)  2.2 Użyteczności publicznej  2.3 Naukowe (badawcze)  2.4 Produkcyjne  2.5 Wojskowe  2.6 Inne  3 Obszary:  3.1 Morskie  3.2 Lotnicze  3.3 Górnicze  3.4 Górskie  3.5 Podległe MON  3.6 Podległe MSWiA  3.7 Wód śródlądowych  3.8 Zabudowane:  3.8.1 Miejskie  3.8.2 Wiejskie  3.9 Niezabudowane  3.10 Pokopalniane  3.11 Inne  Uwaga:  Wykonawca ma przewidzieć możliwość wprowadzenia zmian przez administratora SWDP w podanej liście w fazie eksploatowania systemu. |
|  | W polu [04.5] Nr informacji ze zdarzenia wpisywany będzie numer literowy zgodnie z formatem XXXXXXX-YYYY. |
|  | W polu [04.6] Opis zgłoszenia wpisywany będzie krótki logiczny opis okoliczności zdarzenia (zgodny z przekazanymi informacjami zgłaszającego lub KDRa będącego na miejscu). |
|  | Po wciśnięciu przycisku [04.9] Anuluj aplikacja wraca do ekranu logowanie z aktywnymi przyciskami [04], [05], [06] |
|  | By rozpocząć nowe zdarzenie dane z [04.1], [04.2], [04.3], [04.4], [04.5], [04.6] mogą być kompletne, mogą być częściowe lub mogą być w ogóle nie wprowadzone. Dane te mogą być uzupełnione w późniejszej czasie. |
|  | Po wciśnięciu przycisku [04.10] START system zaczyna automatycznie zbieranie danych:   * data, godzina, * pozycja GPS, * strumień wideo z kamer nasobnych, * informacje (wyniki pomiarów) z urządzeń zintegrowanych z SWDP (jeżeli Wykonawca taką integrację wykonał),   pojawia się ekran Pulpitu głównego.  Uwaga:  Wykonawca ma przewidzieć możliwość automatycznego łączenia się aplikacji z urządzeniami pomiarowymi i przechwytywania wyników pomiarowych przez SWDP. Funkcjonalności te będą się pojawiać w kolejnym etapie rozwoju SWDP, nie objętym obecnym postępowaniem. |
|  | Po wciśnięciu przycisku [05] aktywuje się ekran Zdarzenia w trakcie realizacji, na którym ma znajdować się co najmniej:   * [05.1] miejsce na wprowadzeniu nazwy miejscowości z dookreśleniem powiatu i województwa, * [05.2] miejsce na wprowadzeniu nazwy ulicy, numeru domu, numeru mieszkania, * [05.3] przycisk Rodzaju zdarzenia, * [05.4] przycisk Miejsce zdarzenia, * [05.5] przycisk Nr informacji ze zdarzenia, * [05.7] przycisk Szukaj, * [05.8] okienko Wskazany adres i ID zdarzenia/ Nr informacji ze zdarzenia * [05.9] przycisk Anuluj, * [05.10] przycisk START,   Uwaga:  Na tym ekranie Wykonawca ma przewidzieć możliwość wprowadzenia jeszcze co najmniej 1 przycisku o dowolne funkcjonalności. Funkcjonalności te będą mogły być określone w kolejnym etapie rozwoju SWDP, nie objętym obecnym postępowaniem. |
|  | Funkcjonalność przycisków i pól [05.1], [05.2], [05.3], [05.4], [05.5] analogicznie do przycisków i pól [04.1], [04.2], [04.3], [04.4], [04.5] |
|  | By rozpocząć wyszukiwanie dane z [05.1], [05.2], [05.3], [05.4], [05.5] mogą być kompletne, mogą być częściowe lub mogą być w ogóle nie wprowadzone by SWDP przeszukało zasoby Zdarzeń w trakcie realizacji. |
|  | Po wciśnięciu przycisku [05.7] Szukaj pojawia się okienko z listą zdarzeń spełniające warunki przeszukiwania.  Jeżeli [05.1], [05.2], [05.3], [05.4], [05.5] będą puste lub wybór nie zostanie dokonany SWDP pokarze wszystkie Zdarzenia w trakcie realizacji. |
|  | Po wybraniu z listy interesującego nas zdarzenia w okienku [05.8] Wskazany adres i ID zdarzenia/ Nr informacji ze zdarzenia pojawi się wybrane zdarzenie |
|  | Po wciśnięciu przycisku [05.9] Anuluj aplikacja wraca do ekranu logowanie z aktywnymi przyciskami [04], [05], [06] |
|  | By dołączyć do Zdarzenia w trakcie realizacji w okienku [05.8] Wskazany adres i ID zdarzenia/ Nr informacji ze zdarzenia musi pojawić się wybrane zdarzenie |
|  | Po wciśnięciu przycisku [05.10] START system zaczyna automatycznie zbieranie danych:   * data, godzina, * pozycja GPS, * strumień wideo z kamer nasobnych, * informacje (wyniki pomiarów) z urządzeń zintegrowanych z SWDP (jeżeli Wykonawca taką integrację wykonał),   pojawia się ekran Pulpitu głównego.  Uwaga:  Wykonawca ma przewidzieć możliwość automatycznego łączenia się aplikacji z urządzeniami pomiarowymi i przechwytywania wyników pomiarowych przez SWDP. Funkcjonalności te będą się pojawiać w kolejnym etapie rozwoju SWDP, nie objętym obecnym postępowaniem. |
|  | Po wciśnięciu przycisku [06] aktywuje się ekran Zdarzenie archiwalne, na którym ma znajdować się co najmniej:   * [06.1] miejsce na wprowadzeniu nazwy miejscowości z dookreśleniem powiatu i województwa, * [06.2] miejsce na wprowadzeniu nazwy ulicy, numeru domu, numeru mieszkania, * [06.3] przycisk Rodzaju zdarzenia, * [06.4] przycisk Miejsce zdarzenia, * [06.5] przycisk Nr informacji ze zdarzenia, * [06.7] przycisk Szukaj, * [06.8] okienko Wskazany adres i ID zdarzenia/ Nr informacji ze zdarzenia * [06.9] przycisk Anuluj, * [06.10] przycisk START,   Uwaga:  Na tym ekranie Wykonawca ma przewidzieć możliwość wprowadzenia jeszcze co najmniej 1 przycisku o dowolne funkcjonalności. Funkcjonalności te będą mogły być określone w kolejnym etapie rozwoju SWDP, nie objętym obecnym postępowaniem. |
|  | Funkcjonalność przycisków i pól [06.1], [06.2], [06.3], [06.4], [06.5], [06.7], [06.8], [06.9], [06.10] analogicznie do przycisków i pól [05.1], [05.2], [05.3], [05.4], [05.5], [05.7], [05.8], [05.9], [05.10] ale dotyczą zdarzeń mających statut zakończonych w SWDP. Zbierane i wprowadzane dane w SDWP muszą być wyraźnie oznaczone jako dane zbierane po pierwotnym zakończeniu zdarzenia. |
|  | Po pojawieniu się ekranu Panelu głównego, na którym ma znajdować się co najmniej:   * [1] przycisk Praca w strefie, * [2] przycisk Pomiar, * [3] przycisk Pobór próbki, * [4] przycisk Aparat, * [5] przycisk Opis - Notatka, * [6] przycisk Mapa, * [7] przycisk Baza wiedzy, * [8] przycisk Wsparcie specjalisty CJA, * [10] przycisk ZAKOŃCZ,   Uwaga:  Na tym ekranie Wykonawca ma przewidzieć możliwość wprowadzenia jeszcze co najmniej 1 przycisku o dowolnej funkcjonalności. Funkcjonalności te będą mogły być określone w kolejnym etapie rozwoju SWDP, nie objętym obecnym postępowaniem. |
|  | Po wciśnięciu przycisku [1] aktywuje się ekran Praca w strefie, na którym ma znajdować się co najmniej:   * [1.1] przycisk Rozpoczęcie pracy w strefie, * [1.2] przycisk Zakończenie pracy w strefie, * [1.3] przycisk Rodzaj ubrania, * [1.4] przycisk Rodzaj ODO, * [1.5] przycisk Wybór urządzeń pomiarowych, * [1.8] przycisk Powrót,   Uwaga:  Na tym ekranie Wykonawca ma przewidzieć możliwość wprowadzenia jeszcze co najmniej 2 przycisków o dowolnej funkcjonalności. Funkcjonalności te będą mogły być określone w kolejnym etapie rozwoju SWDP, nie objętym obecnym postępowaniem. |
|  | Po wciśnięciu przycisku [1.1] Rozpoczęcie pracy w strefie SWDP zaczyna rejestrować czas pracy ratowników w strefie. W zależności od zastosowanych ubrań ochronnych i rodzaju sprzętu Ochrony Dróg Oddechowych (ODO) program kontroluje i wyświetla czas jaki ratownik może jeszcze pracować w strefie. Maksymalny czas możliwy do pracy w strefie będzie określany przez Użytkownika końcowego dla każdego z ratowników z zależności od jakiego indywidualnych predyspozycji, rodzaju ubrań ochronnych oraz sprzętu ODO jakie zastosuje. Czas ten musi być możliwy do zmiany w czasie zwykłej eksploatacji SWDP z poziomu Dowódcy SGR CHEM-EKO lub Zastępcy Dowódcy SGR CHEM-EKO |
|  | Po wciśnięciu przycisku [1.2] Zakończenie pracy w strefie SWDP kończy rejestrować czas pracy ratowników w strefie. |
|  | Po wciśnięciu przycisku [1.3] Rodzaj ubrania pojawia się zdefiniowana lista do wyboru. Lista Rodzajów ubrania ochronnego zawiera co najmniej:   * ubraniach ochronnych kat. III typ 1a z aparatem ochrony dróg oddechowych wewnątrz * ubraniach ochronnych kat. III typ 3 * ubraniach ochronnych kat. III typ 3 z systemem filtrowentylacji wymuszonej * ubraniach ochronnych kat. III typ 4 * ubraniach ochronnych kat. III typ 5 * ubraniach ochronnych kat. III typ 6 * ubranie specjalne (typu nomex) * inne   Uwaga:  Wykonawca ma przewidzieć możliwość wprowadzenia zmian przez administratora SWDP w podanej liście w fazie eksploatowania systemu. |
|  | Po wciśnięciu przycisku [1.4] Rodzaj ODO pojawia się zdefiniowana lista do wyboru. Lista Rodzajów sprzętu ODO zawiera co najmniej:   * aparatem ochrony dróg oddechowych wewnątrz ubraniach ochronnych kat. III typ 1a * aparatem ochrony dróg oddechowych * system filtrowentylacji wymuszonej * maska z filtropochłaniaczem * półmaska z filtropochłaniaczem * maseczka FFP3 * maseczka FFP2 * maseczka chirurgiczna * inne   Uwaga:  Wykonawca ma przewidzieć możliwość wprowadzenia zmian przez administratora SWDP w podanej liście w fazie eksploatowania systemu. |
|  | Po wciśnięciu przycisku [1.5] Wybór urządzeń pomiarowych pojawia się zdefiniowana lista do wyboru, dostępnych urządzeń pomiarowych dla danej SGR CHEM-EKO. Listę tą Wykonawca otrzyma od każdego z Użytkowników końcowych w fazie realizacji przedmiotu zamówienia.  Uwaga:  Wykonawca ma przewidzieć możliwość wprowadzenia zmian z poziomu Dowódcy SGR CHEM-EKO lub Zastępcy Dowódcy SGR CHEM-EKO, w podanej liście w fazie eksploatowania systemu. |
|  | Po wciśnięciu przycisku [1.8] Powrót aktywuje się ekran Panel główny |
|  | Po wciśnięciu przycisku [2] aktywuje się ekran Pomiar, na którym ma znajdować się co najmniej:   * [2.0] okienko Listy dostępnych urządzeń pomiarowych (wybranych np. po wciśnięciu przycisku [1.5], * [2.1] przycisk Dodaj urządzenie, * [2.2] przycisk Nowy pomiar, * [2.3] przycisk Przeglądanie wyników, * [2.5] przycisk Powrót,   Uwaga:  Na tym ekranie Wykonawca ma przewidzieć możliwość wprowadzenia jeszcze co najmniej 1 przycisk o dowolnej funkcjonalności. Funkcjonalności te będą mogły być określone w kolejnym etapie rozwoju SWDP, nie objętym obecnym postępowaniem. |
|  | W okienku [2.0] z listy dostępnych urządzeń można wybrać (zaznaczyć) dowolne urządzenie. Przyciski [2.2], [2.3] pozostają nieaktywne do czasu poprawnego wybrania jednego z urządzeń.  Po wyborze z listy jednego z urządzeń w okienku [2.0] aktywują się przyciski [2.2], [2.3] |
|  | Funkcjonalność przycisku [2.1] analogiczna do przycisku [1.5] |
|  | Po wciśnięciu przycisku [2.2] aktywuje się ekran z okienkiem widoku schematycznego urządzenia.  Dla wszystkich urządzeń zwracających wynik numeryczny np. detektorów jedno i wielogazowych, mierników promieniowania jonizacyjnego, itp., po wybraniu okienka dla danego sensora/detektora/miernika pojawia się klawiatura numeryczna do wprowadzenia wartości wskazania, po wprowadzeniu wszystkich wartości należy zatwierdzić nowy pomiar.  Dla wszystkich urządzeń zwracających wynik w formie opisu np. nazwy substancji numeru ONZ, numeru CAS, itp., pojawia się możliwość wprowadzania danych analogicznie do punktu [5.1] Klawiatura, [5.2] Pisanie rysikiem, [5.3] Pisanie głosem.  Do każdego wprowadzanego wyniku będzie możliwość wykonania przypisanego zdjęcia lub kilku zdjęć. |
|  | Po wciśnięciu przycisku [2.3] aktywuje się ekran z okienkiem Przeglądania wyników pomiarowych oraz suwaki/przełączniki umożliwiające płynnie regulować wartości brzegowe przedziału czasowego jaki chcemy wyświetlić.  Dla wszystkich urządzeń zwracających wynik numeryczny np. detektorów jedno i wielogazowych, mierników promieniowania jonizacyjnego, itp., wyniki będą prezentowane w formie wykresu. Na osi poziomej będzie czas, na osi pionowej wartość odczytu. Skala osi poziomej będzie płynnie dostosowana do wybranego przedziału czasowego. Skala osi pionowej będzie płynnie dostosowana do wartości maksymalnych odczytów w danym przedziale czasowym. Przy urządzeniach dających więcej niż jeden odczyt wykresy prowadzone różnymi kolorami, obok legenda kolorów.  Dla wszystkich urządzeń zwracających wynik w formie opisu np. nazwy substancji numeru ONZ, numeru CAS, itp., pojawia się lista kolejnych wprowadzonych wpisów z sygnaturą godziny i ewentualnie daty, jeżeli jest inna niż aktualna. |
|  | Po wciśnięciu przycisku [2.5] Powrót aktywuje się ekran Panel główny |
|  | Po wciśnięciu przycisku [3] aktywuje się ekran Pobór próbki, na którym ma znajdować się co najmniej:   * [3.0] okienko Listy pobranych próbek, * [3.1] przycisk Nr próbki, * [3.2] przycisk Opis próbki, * [3.3] przycisk Zdjęcie próbki, * [3.5] przycisk Powrót,   Uwaga:  Na tym ekranie Wykonawca ma przewidzieć możliwość wprowadzenia jeszcze co najmniej 1 przycisk o dowolnej funkcjonalności. Funkcjonalności te będą mogły być określone w kolejnym etapie rozwoju SWDP, nie objętym obecnym postępowaniem. |
|  | W okienku [3.0] znajduje się lista pobranych próbek oraz pozycja Nowa próbka. Przyciski [3.1], [3.2], [3.3] pozostają nieaktywne do czasu poprawnego wybrania jednej z pozycji w okienku [3.0].  Po wyborze z listy jednej z pozycji w okienku [3.0] aktywują się przyciski [3.1], [3.2], [3.3].  By dodać nową próbkę należy z listy pobranych próbek wybrać pozycję Nowa próbka i wcisnąć jeden z przycisków [3.1], [3.2], [3.3] i poprawnie zakończyć funkcję. Jeżeli nie będzie to przycisk [3.1] wówczas system nada numer automatyczny próbki indywidualny dla każdej z próbek.  W każdej chwili można wybrać jedną z pobranych próbek i dopisać kolejne informacje korzystając z przycisków [3.1], [3.2], [3.3]. |
|  | Po wciśnięciu przycisku [3.1] Nr próbki pojawia się możliwość wprowadzania danych na klawiaturze numerycznej z możliwością przejścia do funkcjonalności analogicznych do punktu [5.1] Klawiatura, [5.2] Pisanie rysikiem, [5.3] Pisanie głosem. |
|  | Po wciśnięciu przycisku [3.2] Opis próbki aktywuje się ekran z okienkiem na wprowadzany tekst oraz możliwość wprowadzania danych za pomocą funkcjonalności analogicznych do punktu [5.1] Klawiatura, [5.2] Pisanie rysikiem, [5.3] Pisanie głosem. |
|  | Funkcjonalność przycisku [3.3] Zdjęcie próbki analogiczna do przycisku [4], dodatkowo wykonane zdjęcie zostaje przypisane konkretnie do pobranej próbki. Po wciśnięciu przycisku powrót na ekranie aparatu następuje aktywacja ekranu [3] Pobór próbki. |
|  | Po wciśnięciu przycisku [3.5] Powrót aktywuje się ekran Panel główny |
|  | Po wciśnięciu przycisku [4] aktywuje się ekran Aparat, na którym ma znajdować się co najmniej:   * [4.0] okienko Widoku aparatu, * [4.1] przycisk Zrób zdjęcie, * [4.3] przycisk Opis zdjęcia, * [4.3] przycisk Galeria, * [4.5] przycisk Powrót,   Uwaga:  Na tym ekranie Wykonawca ma przewidzieć możliwość wprowadzenia jeszcze co najmniej 1 przycisk o dowolnej funkcjonalności. Funkcjonalności te będą mogły być określone w kolejnym etapie rozwoju SWDP, nie objętym obecnym postępowaniem. |
|  | W okienku [4.0] Widok aparatu znajduje się cały widok wykonywanego zdjęcia. Zaleca się by okno było jak największe, a przyciski były rozmiarem dobrane tak by nie przysłaniać widoku zdjęcia, ale by również nie utrudniać obsługi SWDP. |
|  | Po wciśnięciu przycisku [4.1] następuje wykonanie zdjęcia, które zostaje oznaczone datą, godziną, współrzędną GPS oraz identyfikatorem zalogowanego użytkownika. |
|  | Po wciśnięciu przycisku [4.3] Opis zdjęcia aktywuje się ekran z okienkiem na wprowadzany tekst oraz możliwość wprowadzania danych za pomocą funkcjonalności analogicznych do punktu [5.1] Klawiatura, [5.2] Pisanie rysikiem, [5.3] Pisanie głosem. |
|  | Po wciśnięciu przycisku [4.4] Galeria aktywuje się ekran z okienkiem (galerią zdjęć) gdzie można przeglądać w wykonane zdjęcia oraz dodawać im opisy analogicznie do funkcjonalności przycisku [4.3]. |
|  | Po wciśnięciu przycisku [4.5] Powrót aktywuje się ekran Panel główny |
|  | Po wciśnięciu przycisku [5] aktywuje się ekran Opis - Notatka, na którym ma znajdować się co najmniej:   * [5.0] okienko Notatnik, * [5.1] przycisk Klawiatura, * [5.2] przycisk Pisanie rysikiem, * [5.3] przycisk Pisanie głosem, * [5.5] przycisk Powrót,   Uwaga:  Na tym ekranie Wykonawca ma przewidzieć możliwość wprowadzenia jeszcze co najmniej 1 przycisk o dowolnej funkcjonalności. Funkcjonalności te będą mogły być określone w kolejnym etapie rozwoju SWDP, nie objętym obecnym postępowaniem. |
|  | W okienku [5.0] Notatnik znajduje się lista wprowadzonych kolejnych notatek i opisów z sygnaturą godziny i ewentualnie daty, jeżeli jest inna niż aktualna. |
|  | Po wciśnięciu przycisku [5.1] Klawiatura aktywuje się ekran z okienkiem na wprowadzany tekst oraz klawiaturą QWERTY.  Ten panel musi posiadać funkcję usuwania tekstu błędnie wprowadzonego. |
|  | Po wciśnięciu przycisku [5.2] Pisanie rysikiem aktywuje się ekran z okienkiem na wprowadzany tekst oraz okienko na pisanie rysikiem, które to zapisy będą przetwarzane na tekst umieszczany w okienku powyżej.  Ten panel musi posiadać funkcję usuwania tekstu błędnie przetwarzanego. |
|  | Po wciśnięciu przycisku [5.3] Pisanie głosem aktywuje się ekran z okienkiem na wprowadzany tekst oraz przycisk mikrofonu po wciśnięciu którego następuje rejestracja dźwięku, który będzie zmieniany na tekst umieszczany w okienku powyżej okienko na pisanie rysikiem, które to zapisy będą przetwarzane na tekst umieszczany w okienku powyżej.  Ten panel musi posiadać funkcję usuwania tekstu błędnie przetwarzanego. |
|  | Po wciśnięciu przycisku [5.5] Powrót aktywuje się ekran Panel główny |
|  | Po wciśnięciu przycisku [6] aktywuje się ekran Mapa, na którym ma znajdować się co najmniej:   * [6.0] okienko Widok mapy – z legendą elementów zaznaczonych na mapie, * [6.1] przycisk Funkcje edycji mapy, * [6.2] przycisk Zapisz pozycję * [6.3] przycisk Zaznacz pozycję, * [6.4] przycisk Zaznacz linię, * [6.6] przycisk Zaznacz obszar, * [6.7] przycisk Nawiguj, * [6.8] przycisk Powrót,   Uwaga:  Na tym ekranie Wykonawca ma przewidzieć możliwość wprowadzenia jeszcze co najmniej 1 przycisk o dowolnej funkcjonalności. Funkcjonalności te będą mogły być określone w kolejnym etapie rozwoju SWDP, nie objętym obecnym postępowaniem. |
|  | W okienku [6.0] Widok mapy – z legendą elementów zaznaczonych na mapie znajduje się widok Wybranego fragmentu mapy z podkładem (do wyboru: mapy fizycznej oraz ortofotomapy). Zaleca się by okno było jak największe, a przyciski były rozmiarem dobrane, tak by nie przysłaniać widoku Mapy, ale by również nie utrudniać obsługi SWDP. Mapa musi posiadać skalę odniesienia oraz legendę elementów zaznaczonych na mapie. Po najechaniu na element zaznaczony na mapie pojawi się opis elementu naniesionego z sygnaturą godziny i ewentualnie daty, jeżeli jest inna niż aktualna. |
|  | Przyciski [6.1] Funkcje edycji mapy to zespół przycisków: zmieniających skalę mapy (zwiększenie i zmniejszania), przełączenia podkładu mapy między mapą fizyczną, a ortofotomapą. Przyciski do określenia przedziału czasowego z jakiego elementy mają być wyświetlane na mapie. Przycisk wyboru elementów jakie mają być wyświetlane na mapie. Elementy wyświetlane na mapie to co najmniej:   * bieżąca pozycja, * punkty zaznaczone, * linie zaznaczone, * obszary zaznaczone, * miejsca wykonania Pomiarów, * miejsce Pobrania próbki, * miejsce wykonania Zdjęcia,   Uwaga:  Na tym ekranie Wykonawca ma przewidzieć możliwość wprowadzenia jeszcze co najmniej 3 rodzajów elementów do wyświetlania na mapie. Funkcjonalności te będą mogły być określone w kolejnym etapie rozwoju SWDP, nie objętym obecnym postępowaniem. |
|  | Po wciśnięciu przycisku [6.2] Zapisz pozycję następuje zapisanie aktualnej pozycji oraz aktywuje się ekran z okienkiem na wprowadzenie opisu Zapisanej pozycji. Wprowadzany tekst za pomocą funkcjonalności analogicznych do punktu [5.1] Klawiatura, [5.2] Pisanie rysikiem, [5.3] Pisanie głosem. |
|  | Po wciśnięciu przycisku [6.3] Zaznacz pozycję aktywuje się funkcja zapisania pozycji wskazanej na mapie oraz aktywuje się ekran z okienkiem na wprowadzenie opisu Zaznaczonej pozycji. Wprowadzany tekst za pomocą funkcjonalności analogicznych do punktu [5.1] Klawiatura, [5.2] Pisanie rysikiem, [5.3] Pisanie głosem. |
|  | Po wciśnięciu przycisku [6.4] Zaznacz linię aktywuje się funkcja zapisania kilku pozycji wskazanych na mapie połączonych liniami prostymi oraz aktywuje się ekran z okienkiem na wprowadzenie opisu Zaznaczonej linii. Wprowadzany tekst za pomocą funkcjonalności analogicznych do punktu [5.1] Klawiatura, [5.2] Pisanie rysikiem, [5.3] Pisanie głosem. |
|  | Po wciśnięciu przycisku [6.6] Zaznacz obszar aktywuje się funkcja zapisania kilku pozycji wskazanych na mapie połączonych liniami prostymi, z domkniętym początkiem i końcem, z zaznaczeniem półprzezroczystym kolorem powstałej figury oraz aktywuje się ekran z okienkiem na wprowadzenie opisu Zaznaczonego obszaru. Wprowadzany tekst za pomocą funkcjonalności analogicznych do punktu [5.1] Klawiatura, [5.2] Pisanie rysikiem, [5.3] Pisanie głosem. |
|  | Po wciśnięciu przycisku [6.6] Nawiguj aktywuje się funkcja nawigacji do wybranego punktu. Punkt do którego SWDP ma nawigować ma to być co najmniej:   * punkt pozycji zapisany na mapie, * punkt zaznaczony na mapie, * jeden z punktów linii zaznaczonej, * jeden z punktów obszaru zaznaczonego, * miejsc wykonania Pomiarów, * miejsce Pobrania próbki, * miejsce wykonania Zdjęcia, * adres wpisany za pomocą funkcjonalności analogicznych do punktu [5.1] Klawiatura, [5.2] Pisanie rysikiem, [5.3] Pisanie głosem.   zapisania kilku pozycji wskazanych na mapie połączonych liniami prostymi, z domkniętym początkiem i końcem, z zaznaczeniem półprzezroczystym kolorem powstałej figury oraz aktywuje się ekran z okienkiem na wprowadzenie opisu Zaznaczonego obszaru. Wprowadzany tekst za pomocą funkcjonalności analogicznych do punktu [5.1] Klawiatura, [5.2] Pisanie rysikiem, [5.3] Pisanie głosem. |
|  | Po wciśnięciu przycisku [6.8] Powrót aktywuje się ekran Panel główny |
|  | Po wciśnięciu przycisku [7] aktywuje się ekran Baza wiedzy, na którym ma znajdować się co najmniej:   * [7.1] przycisk Zasady i procedury, * [7.2] przycisk Aplikacji ERG 2020, * [7.3] przycisk Wyszukiwarka wielowątkowa, * [7.4] przycisk Aplikacji ADR Tool, * [7.10] przycisk Powrót,   Uwaga:  Na tym ekranie Wykonawca ma przewidzieć możliwość wprowadzenia jeszcze co najmniej 5 przycisków o dowolnej funkcjonalności. Funkcjonalności te będą mogły być określone w kolejnym etapie rozwoju SWDP, nie objętym obecnym postępowaniem. |
|  | Po wciśnięciu przycisku [7.1] Zasady i procedury aktywuje się ekran z wykazem zasad i procedur. Po wybraniu danej zasady lub procedury wyświetla się jej treść. Podczas wyświetlania procedury ma być dostępna funkcja wyszukiwania dowolnego ciągu znaków (dowolnego słowa lub fragmentu słowa).  Listę zasad i procedur Zamawiający przekaże na wniosek Wykonawcy w trakcie realizowania zamówienia.  Listę zasad i procedur będzie można dowolnie zmieniać przez administratora w trakcie eksploatacji SWDP.  Wprowadzany tekst za pomocą funkcjonalności analogicznych do punktu [5.1] Klawiatura, [5.2] Pisanie rysikiem, [5.3] Pisanie głosem. |
|  | Po wciśnięciu przycisku [7.2] Aplikacji ERG 2020aktywuje się aktywuje się aplikacja ERG 2020 z możliwością jej pełnej obsługi.  Wprowadzany tekst za pomocą funkcjonalności analogicznych do punktu [5.1] Klawiatura, [5.2] Pisanie rysikiem, [5.3] Pisanie głosem. |
|  | Po wciśnięciu przycisku [7.3] Wyszukiwarka wielowątkowa aktywuje się ekran z wyszukiwarką, która wprowadzone słowa/zwroty/oznaczenia równocześnie wyszukuje w wielu bazach i przeszukiwanie w wielu wyszukiwarkach równocześnie. Zamawiający wymaga by z poziomu tabletu pojawiły się co najmniej odpowiedzi z minimum 2 wyszukiwarek i minimum 2 baz danych w minimum 4 okienkach (jedna wyszukiwarka lub jedna baza danych w jednym okienku). SWDP pojawiły się odpowiedzi co najmniej z:   * wyszukiwarki Google, * innej popularnej wyszukiwarki internetowej (dowolnej), * bazy PubChem * bazy ChemSpider   Wprowadzany tekst za pomocą funkcjonalności analogicznych do punktu [5.1] Klawiatura, [5.2] Pisanie rysikiem, [5.3] Pisanie głosem. |
|  | Po wciśnięciu przycisku [7.4] Aplikacji ADR Tool aktywuje się aplikacja ADR Tool z możliwością jej pełnej obsługi.  Wprowadzany tekst za pomocą funkcjonalności analogicznych do punktu [5.1] Klawiatura, [5.2] Pisanie rysikiem, [5.3] Pisanie głosem. |
|  | Po wciśnięciu przycisku [7.10] Powrót aktywuje się ekran Panel główny |
|  | Po wciśnięciu przycisku [8] aktywuje się ekran Wsparcie specjalisty CJA, na którym ma znajdować się co najmniej:   * [8.0] okienko Lista dostępnych specjalistów CJA, * [8.1] przycisk Prośba o wsparcie, * [8.2] przycisk Zaakceptuj specjalistę, * [8.5] przycisk Powrót,   Uwaga:  Na tym ekranie Wykonawca ma przewidzieć możliwość wprowadzenia jeszcze co najmniej 2 przyciski o dowolnej funkcjonalności. Funkcjonalności te będą mogły być określone w kolejnym etapie rozwoju SWDP, nie objętym obecnym postępowaniem. |
|  | W okienku [8.0] Lista dostępnych specjalistów CJA znajduje się lista specjalistów którzy zareagowali na Prośbę o pomoc i są gotowi do nawiązania współpracy z ratownikiem.  Przyciski [8.2] pozostają nieaktywne do czasu poprawnego wybrania jednej z pozycji w okienku [8.0].  Po wyborze z listy jednej z pozycji w okienku [8.0] aktywują się przyciski [8.2]. |
|  | Po wciśnięciu przycisku [8.1] Prośba o wsparcie następuje automatyczne powiadamianie wszystkich specjalistów CJA.  1. W pierwszej kolejności powiadamiani są specjaliści CJA, którzy są na liście dostępnych w chwili aktywacji funkcji Prośba o wsparcie.  Powiadamianie o aktywowanej funkcji Prośba o wsparcie następuje poprzez:   * wysłanie wiadomości e-mail na wprowadzone adresy specjalistów CJA, * wysłanie wiadomości sms na wprowadzone nr telefonów specjalistów CJA, * wysłanie wiadomości e-mail na wprowadzone adresy Punktów Alarmowych Jednostek Ratowniczo – Gaśniczych na bazie których utworzone są CJA, * wykonanie automatycznego połączenia głosowego z wprowadzonym nr telefonu Punktów Alarmowych Jednostek Ratowniczo – Gaśniczych na bazie których utworzone są CJA, * wykonanie automatycznego połączenia z wprowadzonymi nr telefonów specjalistów CJA.   2. W przypadku braku zalogowania się (zareagowania widzialnego dla SWDP) któregokolwiek ze specjalistów do SWDP procedura powiadamiania uruchamiana jest po raz drugi po czasie 5 minut.  3. Jeżeli po czasie 15 minut nie zareaguje żaden ze specjalistów wówczas procedura powiadamiania rozszerzana jest o specjalistów CJA, którzy są na liście niedostępnych w chwili aktywacji funkcji Prośba o wsparcie.  Funkcję dostępności każdy ze specjalistów CJA ustawia sobie sam. SWDP ma podpowiadać specjaliście CJA jego dostępności po wyborze systemu pełnienia służby z podziałem na: zmiana 1, zmian 2, zmiana 3, system codzienny. Szczegóły wprowadzania dostępności, wprowadzania czasowej niedostępności krótkotrwałej (pojedyncze służby), wprowadzania czasowej niedostępności długoterminowej (urlop) zostanie strony ustalą w trakcie realizacji przedmiotu zamówienia.  Ratownik może połączyć się tylko z jednym ze specjalistów CJA w jednym czasie.  Jeżeli na Prośbę o pomoc zareaguje więcej niż jeden specjalista CJA, to drugi i kolejni specjaliści widzą wszystkie dane dotyczące zdarzenia, ale nie mogą nawiązać kontaktu bezpośredniego z ratownikiem. Mogą natomiast nawiązać kontakt bezpośredni z specjalistą CJA połączonym bezpośrednio z ratownikiem.  Specjalista CJA, który jest połączony bezpośrednio z ratownikiem może przekazać łączność bezpośrednią innemu specjaliście CJA lub ekspertowi zewnętrznemu. Zmiana łączności bezpośredniej z innym użytkownikiem SWDP musi być zarejestrowana i odnotowana. |
|  | Po wybraniu z listy specjalistę CJA oraz wciśnięciu przycisku [8.2] aktywuje się ekran [8.2] Specjalista CJA, na którym ma znajdować się co najmniej:   * [8.2.0] okienko Okno komunikatora, * [8.2.1] przycisk Pisanie, * [8.2.2] przycisk Pliki, * [8.2.3] przycisk Komunikacja głosowa nadawanie, * [8.2.5] przycisk Powrót,   Uwaga: Na tym ekranie Wykonawca ma przewidzieć możliwość wprowadzenia jeszcze co najmniej 1 przycisk o dowolnej funkcjonalności. Funkcjonalności te będą mogły być określone w kolejnym etapie rozwoju SWDP, nie objętym obecnym postępowaniem. |
|  | W okienku [8.2.0] Okno komunikatora rejestrowana jest cała historia dialogu oraz przesyłane pliki. znajduje się lista wprowadzonych kolejnych notatek, opisów (historia dialogu), przesyłanych plików z sygnaturą godziny i ewentualnie daty, jeżeli jest inna niż aktualna. |
|  | Po wciśnięciu przycisku [8.2.1] Pisanie aktywuje się ekran z okienkiem na wprowadzany tekst oraz możliwość wprowadzania danych za pomocą funkcjonalności analogicznych do punktu [5.1] Klawiatura, [5.2] Pisanie rysikiem, [5.3] Pisanie głosem. |
|  | Po wciśnięciu przycisku [8.2.2] Pliki aktywuje się ekran z okienkiem, w którym zebrane są wszystkie pliki przesyłane między ratownikiem a specjalistą CJA. |
|  | Po wciśnięciu przycisku [8.2.3] Komunikacja głosowa nadawanie aktywuje się funkcja pozwalająca na nawiązanie komunikacji głosowej w trybie on-line. Wciśnięcie tego przycisku powoduje przekazanie dźwięku rejestrowanego przez tablet. Należy rozważyć konieczność używania zestawów słuchawkowych w celu polepszenia jakości dźwięku. |
|  | Po wciśnięciu przycisku [8.2.5] Powrót aktywuje się ekran Panel główny. |

# 

## **2. Opis wymagań i funkcjonalności przeznaczonych dla analityka**

Analityk stanowi wsparcie zarówno dla dowódcy jak i ratownika znajdujących się przy zdarzeniu. Jego rolą jest udzielenie merytorycznego wsparcia służącego opanowaniu sytuacji i podejmowaniu dalszych działań. Wobec tego analityk powinien posiadać maksymalnie dużą wiedzę na temat zdarzenia które wspiera skomasowaną w jednym miejscu. Zasadnym jest żeby widział to co widzi ratownik, znał odczyty jego urządzeń a jednocześnie miał pogląd na całą sytuację tak jak dowódca.

Swoją rolę analityk spełnia z koszar zlokalizowanych w Warszawie oraz Poznaniu, bądź z dowolnego komputera po zalogowaniu się do serwera. W celu szybszej analizy danych, analityk ma dostęp do dużych mocy obliczeniowych dostępnych z poziomu serwerów centralnych systemu. Dzięki temu jest w stanie szybko przeszukiwać duże bazy danych oraz wykonywać skomplikowane obliczeniowo analizy danych na dedykowanych programach.

Analitycy dopisywani są do zdarzenia po otrzymaniu wezwania o pomoc, przyjęciu go i zalogowaniu się do systemu. Zgłoszenia o pomoc przychodzą do tych analityków którzy w danym okresie czasu zadeklarowali dostępność.

Aplikację dla analityka podzielono na dwie fazy wprowadzania.

Faza I

W fazie pierwszej aplikacją powinna osiągnąć następujące funkcjonalności:

1. Funkcja mapowa:
   1. Podgląd na mapie trwających zdarzeń
   2. Funkcjonalności identyczne jak u dowódcy po przyznaniu dostępu do zdarzenia.
2. Baza danych
   1. Dostęp do bazy danych o substancjach PubChem, Chemspider, NIST, Wiley
   2. Dane meteo z IMGW dla wybranego obszaru
   3. Wtyczka do programu ALOHA
   4. Wtyczka do aplikacji ERG 2020
   5. Wtyczka do aplikacji ADR Tool
   6. Baza danych o urządzeniach
   7. Baza danych o środkach ochrony indywidualnej
   8. Baza danych zasad i procedur PSP
   9. Dostęp do archiwalnych meldunków
3. Funkcje analityczne
   1. Wtyczka do oprogramowania umożliwiającego analizę widm różnego (min. IR, GC, MS, IC, Raman) [oprogramowanie dedykowane do danego rodzaju widma lub oprogramowanie o zastosowaniu uniwersalnym]
   2. Bazy danych widm dopasowane do zastosowanego oprogramowania analitycznego (min. NIST, Wiley)
4. Połączenie live z dowódcą/ratownikiem lub innym analitykiem
   1. Tekstowe w formie czatu
   2. Audio
   3. Audio i wideo
5. Możliwość przesyłania plików o różnych rozszerzeniach

Faza II

Faza druga wprowadzania aplikacji dla ratownika obejmuje włączenie do systemu samochodów laboratorium ze wszystkimi ich funkcjonalnościami. Należy przewidzieć możliwość korzystania przez samochody-laboratoria z dostępnych w systemie mocy obliczeniowych oraz baz danych. Samochody-laboratoria będą mogły działać zarówno jako ratownik, dowódca jak i analityk.

## **3. Opis wymagań i funkcjonalności przeznaczonych dla dowódcy**

Wstęp

Aplikacja dowódcy ma za zadanie agregować dane zbierane przez ratowników, informację otrzymywane od ekspertów oraz zarządzać tymi danymi zarówno na miejscu zdarzenia jak i poza nim. Dowódca do obsługi aplikacji będzie stosował laptop przewożony w pojeździe.

Aplikacja powinna umożliwiać pracę w trybie on-line tj. w połączeniu z serwerem centralnym, jak również off-line. Bez względu na sposób działania, aplikacja powinna umożliwiać utrzymywanie stałego kontaktu z przypisanym do niej tabletem ratownika i na bieżąco zbierać z niego dane. Po odzyskaniu łączności internetowej, zgromadzone dane i opracowane materiały powinny zostać zaktualizowane na serwerze centralnym.

Zakłada się zastosowanie aplikacji w dwóch trybach pracy – koszarowym i bojowym. Tryb koszarowy to tryb przeglądania archiwalnych danych, wprowadzanie i modyfikacja baz danych o posiadanych urządzeniach i strażakach. Sporządzanie meldunków z zakończonych działań. Podczas bojowego trybu pracy aplikacja musi umożliwiać zbieranie i analizę danych zbieranych przez ratownika, dołączanie kolejnych tabletów do zdarzenia, wezwanie pomocy eksperta.

Faza I

Osiąganie poszczególnych funkcjonalności i zasięgu systemu podzielono na trzy fazy. Faza I aplikacji dowódcy powinna zawierać następujące funkcjonalności:

1. Funkcje mapowe:
   1. Podgląd pozycji ratowników i pojazdów
   2. Podgląd ścieżek ruchu ratowników i pojazdów
   3. Podgląd przesłanych przez ratowników punktów i stref
   4. wysyłanie punktów do nawigowania dla ratowników
   5. Wyszukiwanie adresów na mapie
   6. Wykonywanie pomiarów na mapie (długość, pole powierzchni)
   7. Nanoszenie obszarów skażenia, granic stref etc.
2. Funkcje analizy danych pomiarowych:
   1. Zestawienia zbiorcze zebranych danych pomiarowych (przedstawienie zapisanych danych pomiarowych ze wszystkich lub z wybranych urządzeń w formie tabelarycznej)
   2. Podgląd danych pomiarowych na mapie (miejsce wykonania pomiaru i wartość)
   3. Podgląd zmiany parametrów w czasie
3. Meteo
   1. Import danych meteo ze strony IMGW
   2. Eksport pobranych danych meteo do programu ALOHA
   3. Wprowadzenie danych meteo ze stacji pojazdu
4. Monitoring ratowników
   1. Czas pracy ratowników
   2. Rozpoczęcie i zakończenie pracy ratownika w strefie zagrożenia
   3. Rodzaj zastosowanych środków ochrony indywidualnej
   4. identyfikacja ratownika
5. pomoc analityka z CJA
   1. wezwanie pomocy analityka
   2. przyznanie dostępu na określonym, możliwym do wyboru poziomie
   3. przesyłanie i odbieranie plików (tekstowych, arkuszy, zdjęć, archiwów, etc.)
   4. wymiana informacji w formie czatu, rozmowy audio, rozmowy audio-wideo
6. Zarządzanie zdarzeniami
   1. Tworzenie nowych zdarzeń
   2. Podgląd archiwalnych zdarzeń (pomiarów, map, korespondencji tekstowej, meldunków, zdjęć)
7. BAZA DANYCH
   1. Wtyczka do bazy danych o substancjach chemicznych PubChem, Chemspider
   2. Wtyczka do aplikacji ERG 2020
   3. Wtyczka do programu ALOHA
   4. procedury i zasady obowiązujące w PSP
   5. Wtyczka do aplikacji ADR Tool
   6. Baza danych ratowników
   7. Baza danych urządzeń pomiarowych i analitycznych
   8. Baza danych środków ochrony osobistej
8. Raportowanie
   1. Tworzenie plików tekstowych, arkuszy danych
   2. Półautomatyczne tworzenie raportów na podstawie szablonu
9. Podgląd z kamer ratowników

Faza II

Faza II przewiduje rozwój aplikacji poprzez implementacje nowych funkcji oraz rozszerzenie jej działania na kolejne SGRChem.

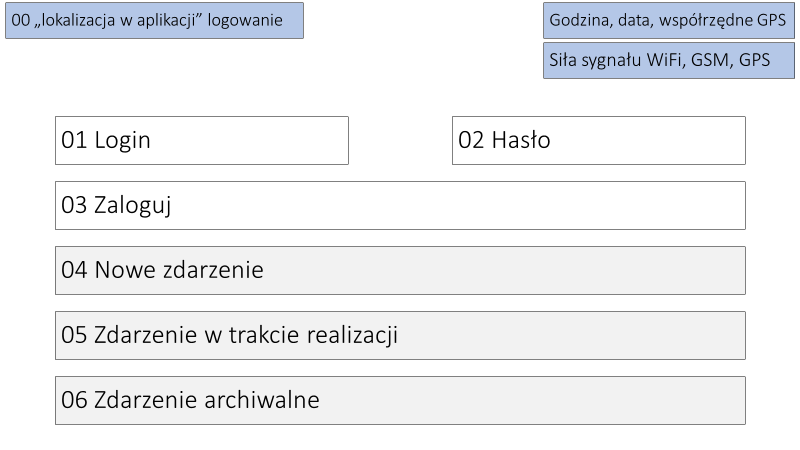
Nowe funkcje w Fazie II:

1. Pobieranie danych z urządzeń zdalnej detekcji (np. RAPID) i prezentacja ich na mapie
2. Pobieranie obrazu z drona
3. Pobieranie obrazu z robota
4. Współpraca kilku SGRChem w ramach jednego zdarzenia:
   1. Dołączanie kolejnych tabletów ratowników pod jednego dowódcę
   2. Podpinanie dowódców odcinków bojowych pod jednego dowódcę – tworzenie zhierarchizowanej sieci

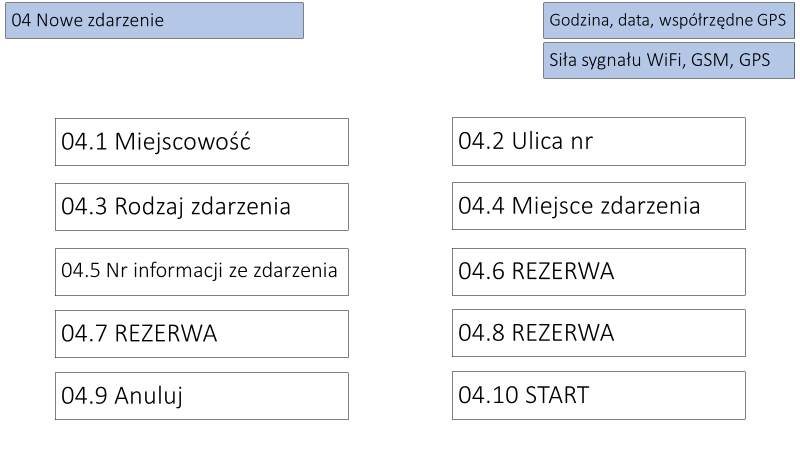
Faza III

Ostatnia faza rozwoju aplikacji. W tej fazie działaniem aplikacji zostają objęte wszystkie SGRChem.

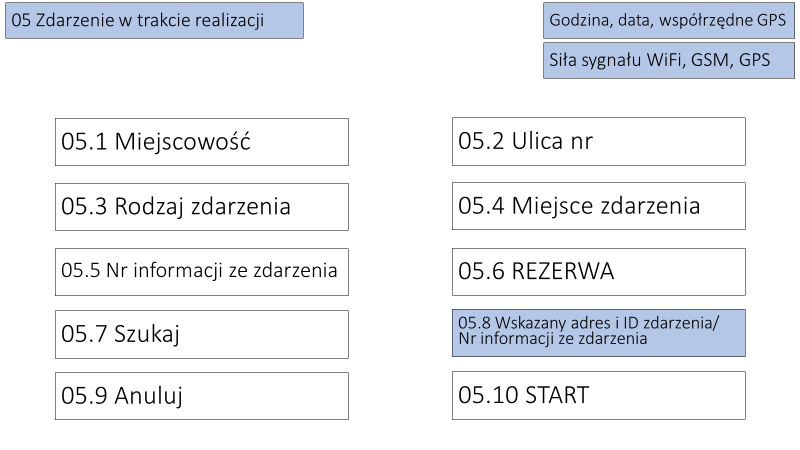
## **4. Wizualizacja funkcjonalności aplikacji SWDP (opisanych w punkcie II.1)**



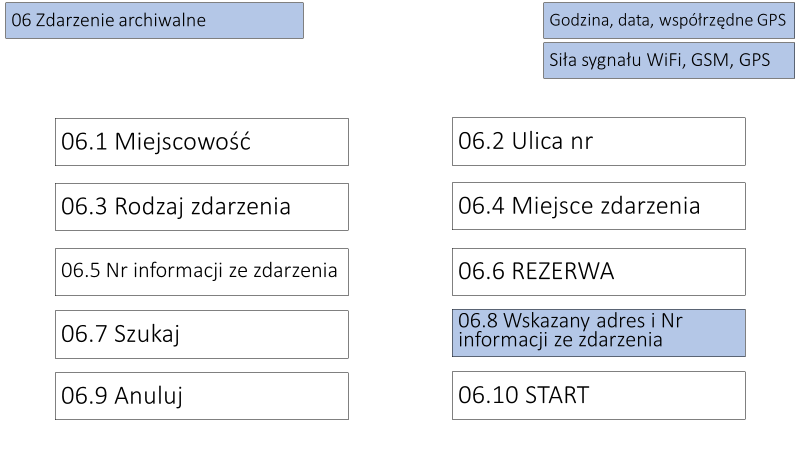
Rysunek 1



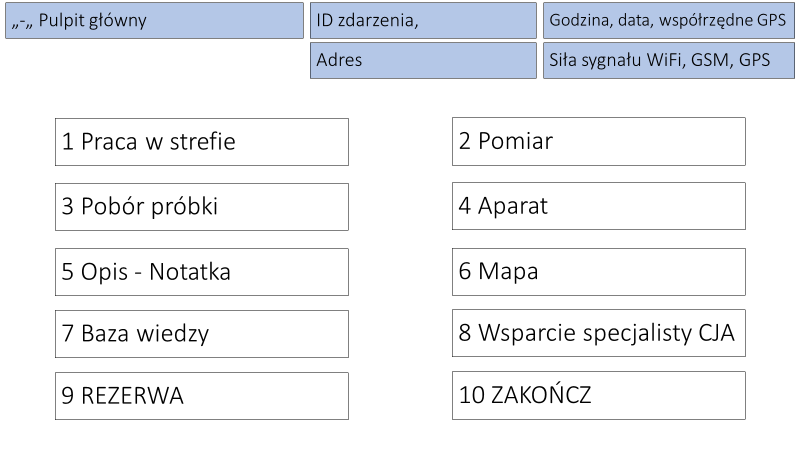
Rysunek 2



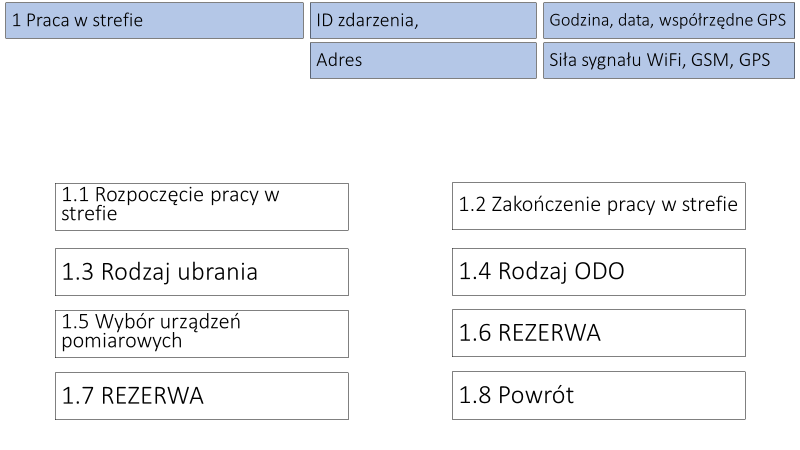
Rysunek 3



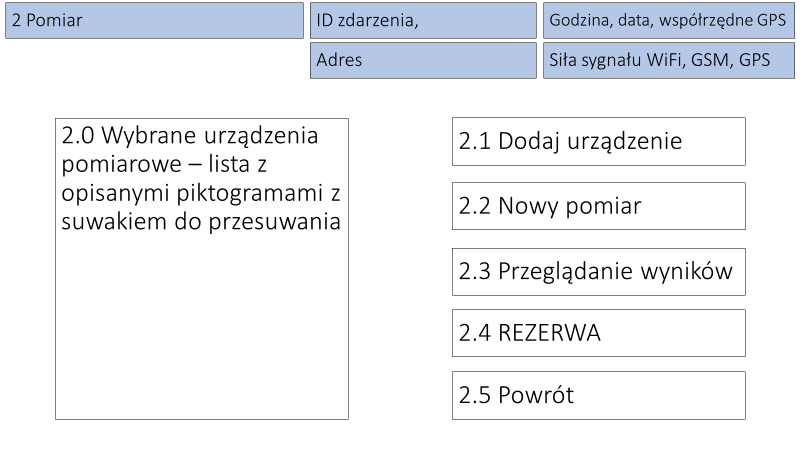
Rysunek 4



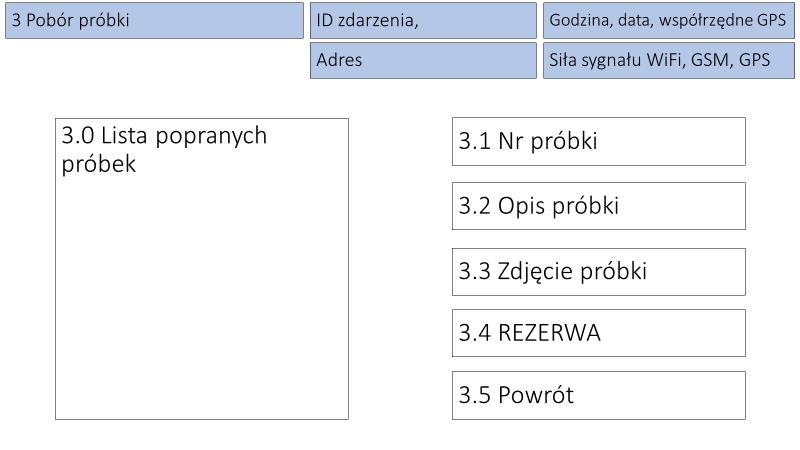
Rysunek 5



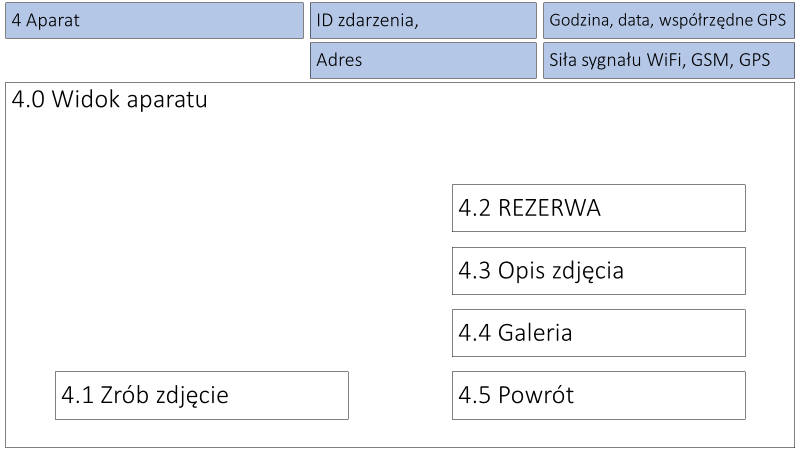
Rysunek 6



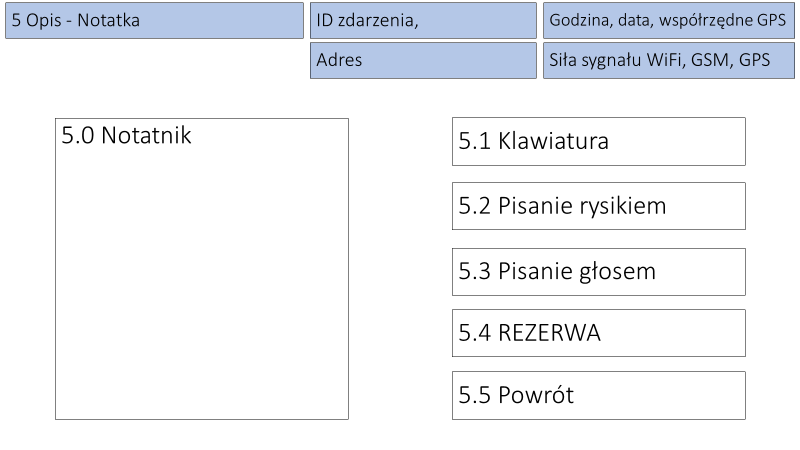
Rysunek 7



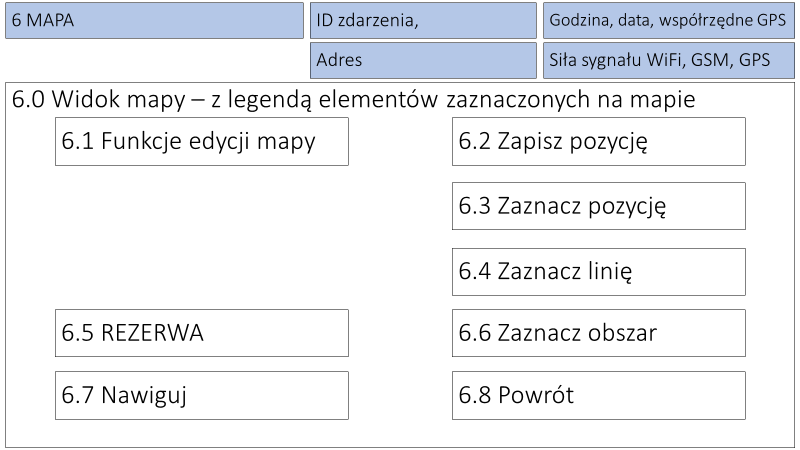
Rysunek 8



Rysunek 9



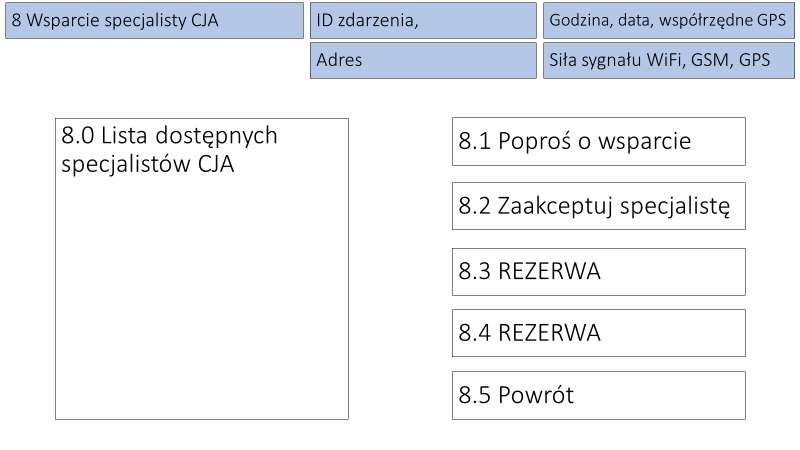
Rysunek 10



Rysunek 11



Rysunek 12



Rysunek 13



Rysunek 14



Rysunek 15

## **6. Graficzne przedstawienie koncepcji SWDP.**

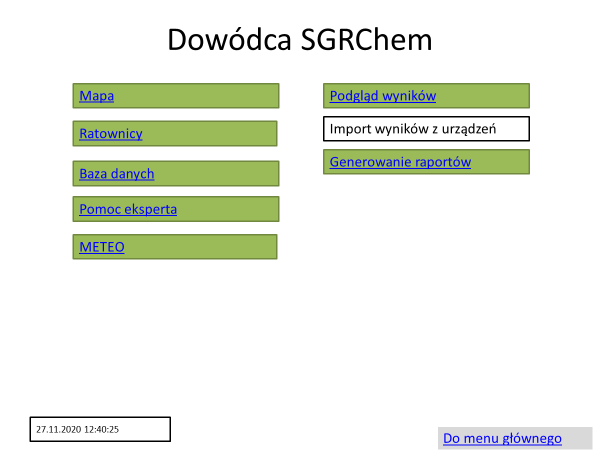
Zamawiający opracował przykładową koncepcję jak według niego powinna wyglądać aplikacja oraz jej funkcjonalności (ilustracje zamieszono poniżej).



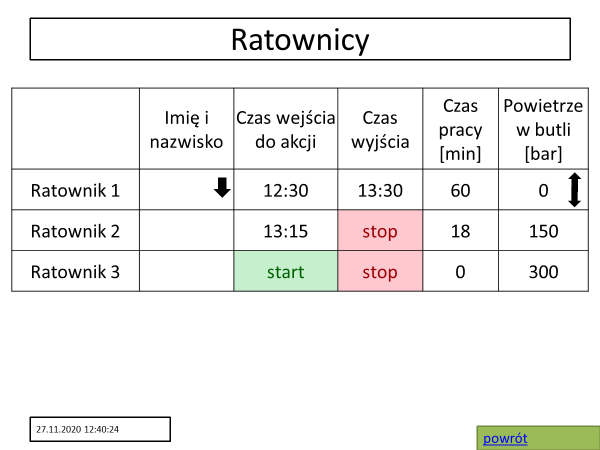
Rysunek 1



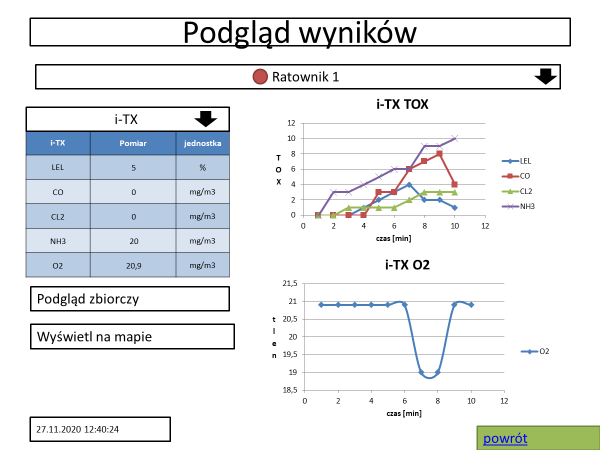
Rysunek 2



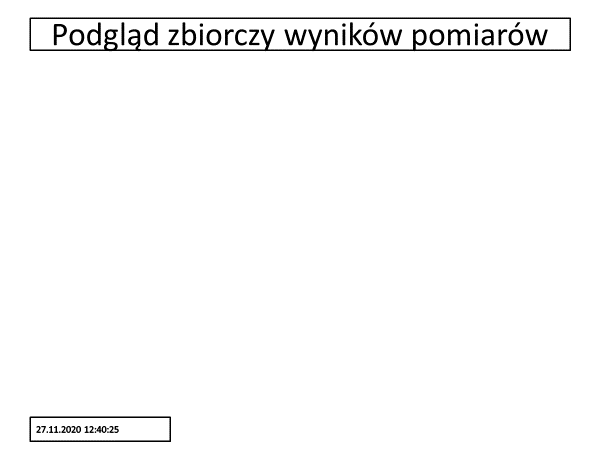
Rysunek 3



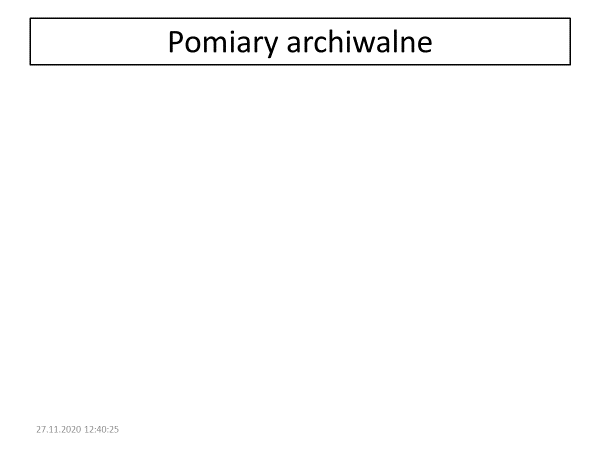
Rysunek 4



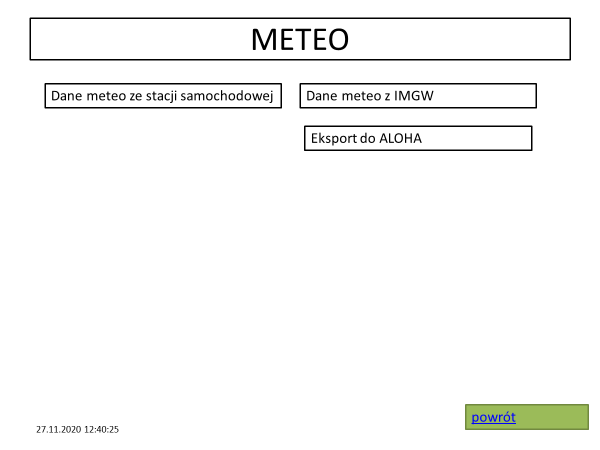
Rysunek 5



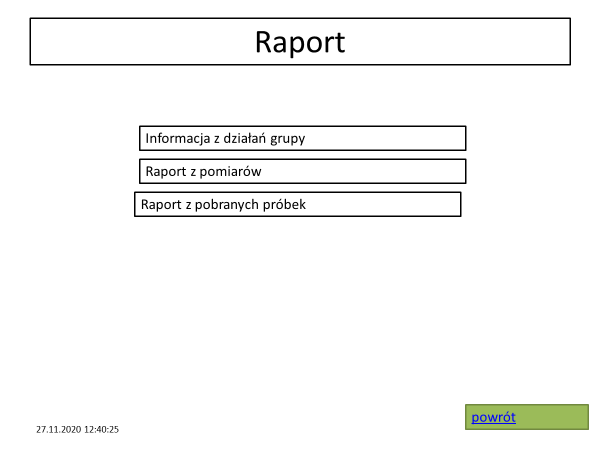
Rysunek 6



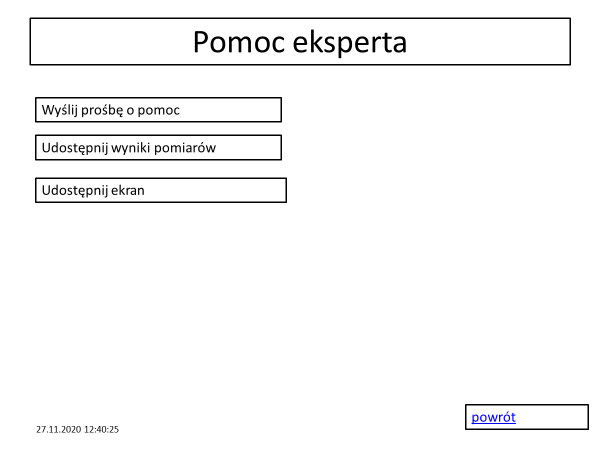
Rysunek 7



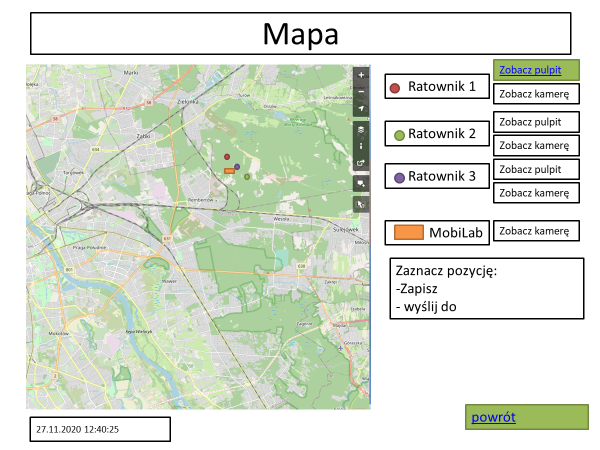
Rysunek 8



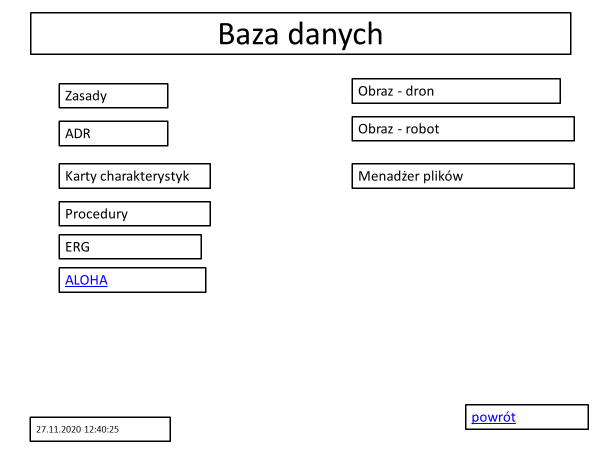
Rysunek 9



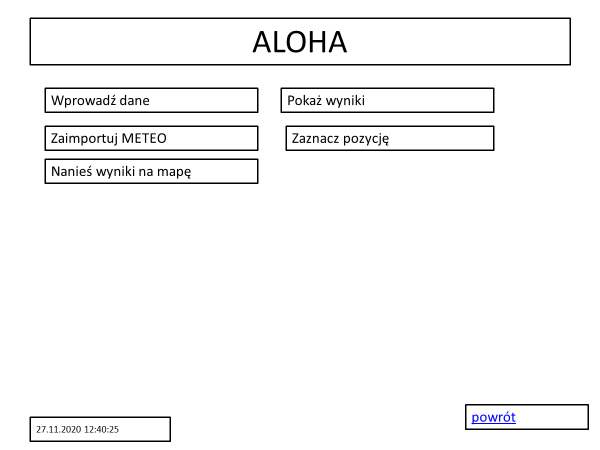
Rysunek 10



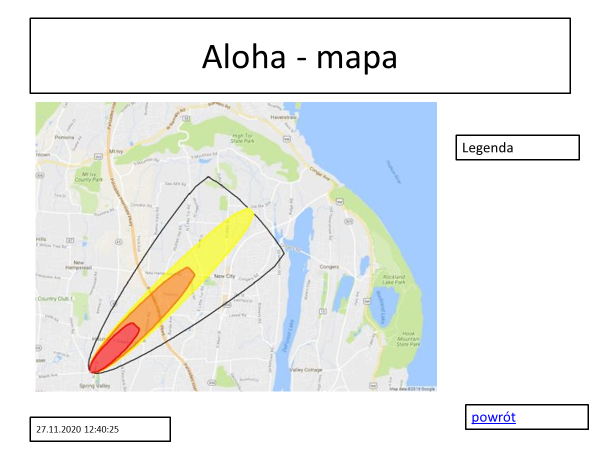
Rysunek 11



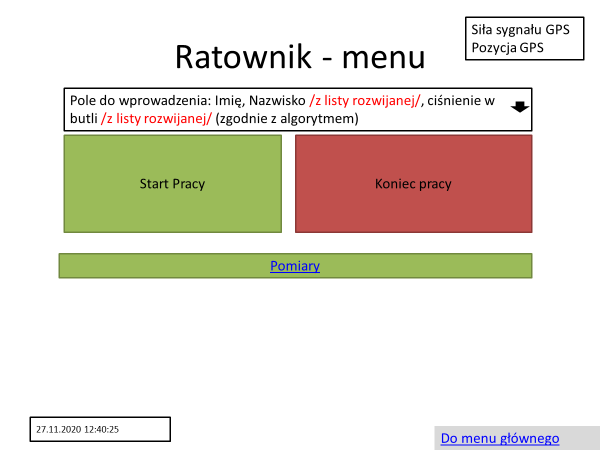
Rysunek 12



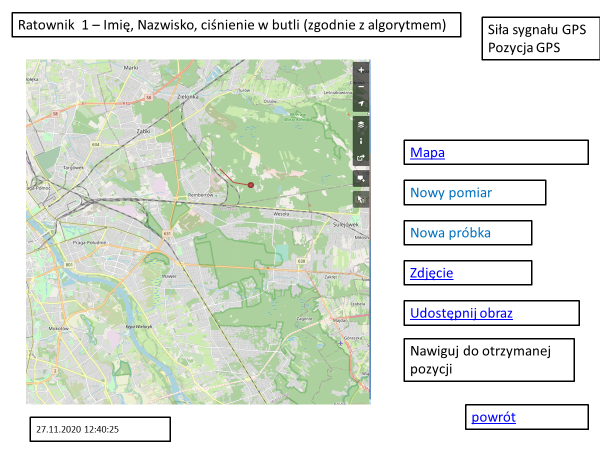
Rysunek 13

e

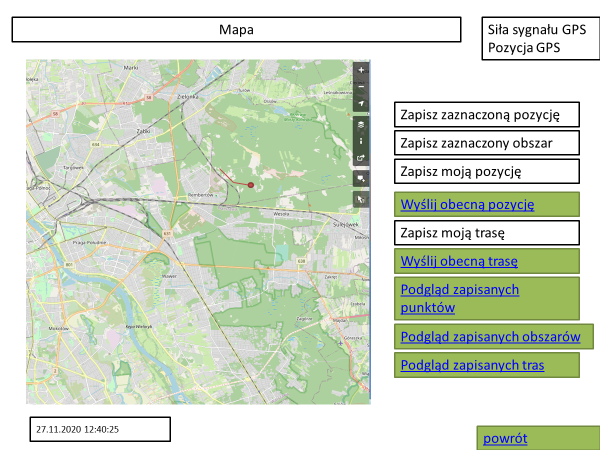
Rysunek 14



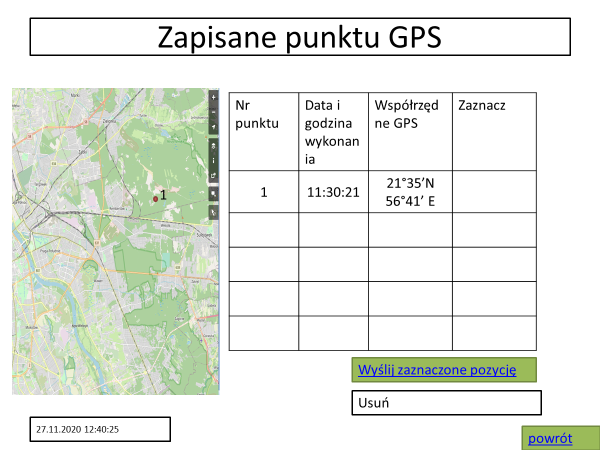
Rysunek 15



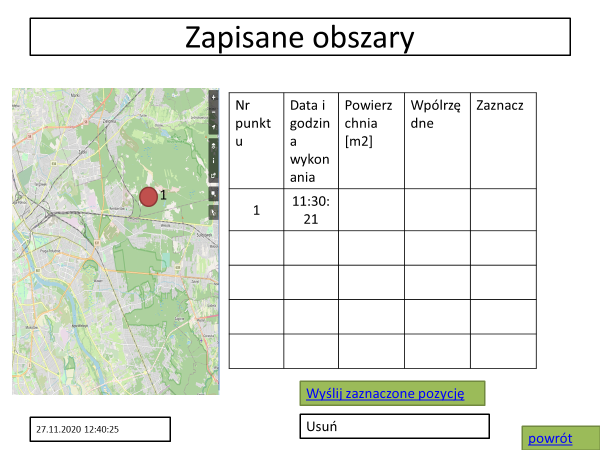
Rysunek 16



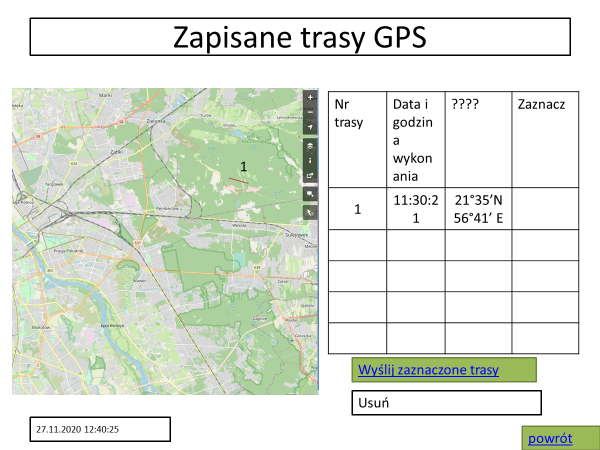
Rysunek 17



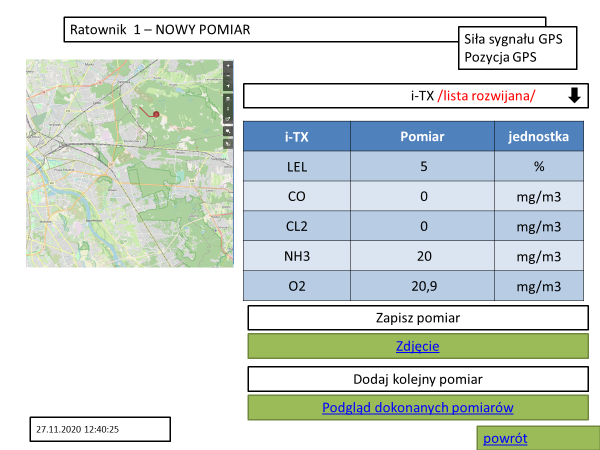
Rysunek 18



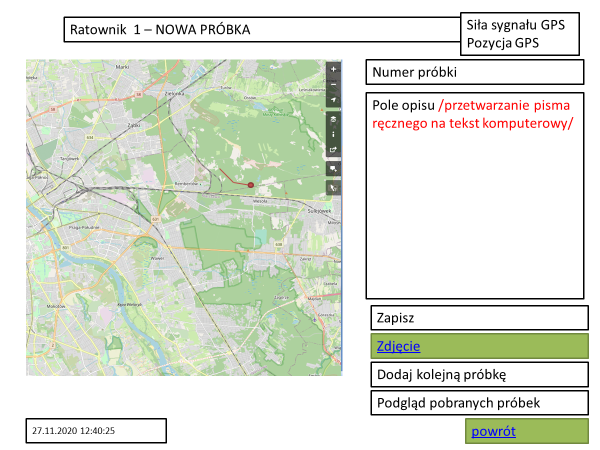
Rysunek 19



Rysunek 20



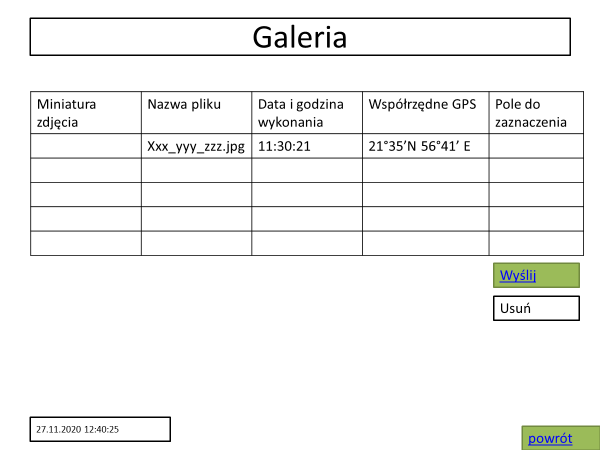
Rysunek 21



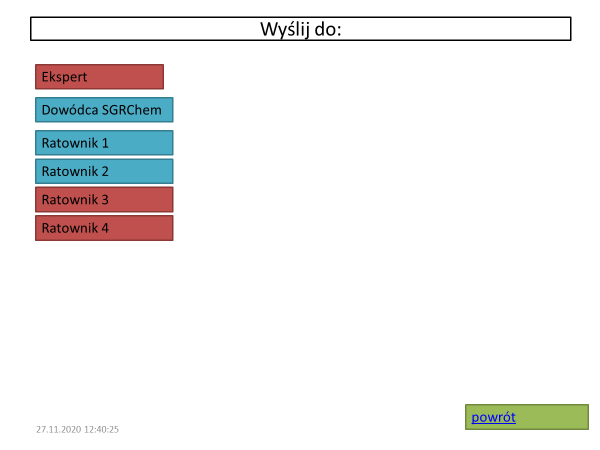
Rysunek 22



Rysunek 23



Rysunek 24



Rysunek 25

# III. Wymagania Ogólne.

## **1. Szkolenia**

## **1.1. Szkolenia aplikacyjne**

Wykonawca po Odbiorze Funkcjonalnym zorganizuje szkolenie dla 90 użytkowników systemu z zakresu obsługi system oraz dostarczonych urządzeń służących do zbierania danych w wymiarze 8 godzin lekcyjnych (45 minut każda) oraz dla 6 administratorów systemu w wymiarze 8 godzin lekcyjnych (45 minut każda).

## **1.2. Szkolenia z rozwiązań sprzętowych**

Wykonawca zapewni autorskie szkolenie dla 6 administratorów z zakresu:

- konfiguracji, zarządzania i odtwarzania po awarii zastosowanego rozwiązania macierzowego: w wymiarze 3 x 8 godzin lekcyjnych (po 45 minut każda)

- konfiguracji, zarządzania oraz odtwarzania po awarii zastosowanych rozwiązań infrastruktury sieciowej (switche LAN, FiberChannel, UTM) w wymiarze 2 x 8 godzin lekcyjnych (po 45 minut każda)

- konfiguracji, zarządzania oraz odtwarzania po awarii zastosowanego środowiska wirtualizacyjnego oraz zastosowanego systemu backupu dla wirtualizatora w wymiarze 8 godzin lekcyjnych (po 45 minut każda).

Wykonawca ponadto zapewni autoryzowane lub certyfikowane szkolenie z zakresu zastosowanego systemu bazodanowego, dla 3 administratorów.

## **2. Dokumentacja**

1. Język

Dokumentacja musi być dostarczona w języku polskim. Dopuszcza się dostarczenie w języku angielskim dokumentacji dla developerów i dokumentacji standardowej gotowych komponentów.

1. Postać i forma

Dokumentacja musi zawierać spis wraz z charakterystyką wszystkich składników dokumentacji.

Dokumentacja musi być dostarczona:

* dwa egzemplarze w postaci papierowej – zszytej lub zbindowanej, na potrzeby Zamawiającego;
* w edytowalnej postaci elektronicznej zapisanej na płycie DVD lub nośniku USB.

Każdy egzemplarz oprócz tytułu musi posiadać oznaczenie wersji identycznej jak aktualna wersja systemu, którą opisuje (wraz z datą produkcji lub dostawy).

Dokumentacja musi się charakteryzować:

* czytelną i zrozumiałą strukturą dokumentów z podziałem na rozdziały i podrozdziały,
* spójną i jednolitą strukturą,
* jednolitą formą prezentacji treści,
* kompletnością – zawierać pełny i wyczerpujący opis zagadnienia, nie może zawierać sformułowań typu „zgodnie ze standardowym opisem...”,
* spójnością i niesprzecznością w obrębie pojedynczego dokumentu, jak i całej dokumentacji.

1. Dokumentacja użytkownika

Dokumentacja musi zawierać szczegółowy opis wszelkich funkcjonalności i cech Systemu, pozwalający na poprawną konfigurację i eksploatację zgodnie z jego przeznaczeniem. W szczególności dokumentacja musi zawierać:

* opis funkcjonalności Systemu,
* opis zarządzania dostępem i uprawnieniami użytkowników,
* opis ról użytkowników i zasad ich tworzenia,
* opis sposobu korzystania z Systemu przez użytkownika,
* podręczniki eksploatacji Systemu.

1. Dokumentacja administratora

Dokumentacja szczegółowo opisująca zastosowane rozwiązania dotyczących bezpiecznej eksploatacji Systemu, w szczególności musi zawierać:

* tworzenia/odtwarzania kopii bezpieczeństwa operacyjnego i kopii zapasowych oraz odtwarzania z kopii infrastruktury software’owej Systemu;
* uruchomienia/zatrzymania Systemu – muszą być opisane kolejne kroki pozwalające na bezpieczne zatrzymanie/uruchomienie elementu infrastruktury hardware’owej i infrastruktury software’owej;
* opis zastosowanych mechanizmów logowania zdarzeń, kontroli i monitorowania działań w Systemie, w tym wszelkich prób naruszenia zasad bezpieczeństwa;
* opis zasad zarządzania kontami (użytkownikami) oraz uprawnieniami poszczególnych ról, profili, użytkowników itp., zestawienie wszystkich założonych kont i haseł.;
* opis wymagań sprzętowych, systemowych, sieciowych oraz spis kompletnych informacji o wymaganiach i ograniczeniach w zakresie technologii, sprzętu, dopuszczalnych wersji użytych komponentów, liczby jednocześnie pracujących użytkowników, maksymalnej liczby użytkowników itp.;
* opis zabezpieczeń interfejsów oraz opis metod zapewnienia poufności i kontrolowalności kanałów przepływu informacji;
* zarządzania danymi historycznymi – opis zasad zarządzania danymi historycznymi i archiwalnymi.

W dokumentacji muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację Systemu.

## **3. Pozostałe**

W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.