Dotacje na innowacje. Inwestujemy w Waszą przyszłość
Projekt współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka

Załącznik nr 1

Szczegółowy opis przedmiotu zamówienia.

W przypadku, gdy w niniejszym opracowaniu podane są znaki towarowe Wykonawca może zaoferować sprzęt i oprogramowanie równoważne, pod warunkiem zapewnienia parametrów nie gorszych niż określono. Wykonawca składając ofertę równoważną musi przedłożyć informację o proponowanym produkcie, zawierającą nazwę i parametry techniczne. Przez produkt równoważny rozumie się taki, który posiada wszystkie cechy funkcjonalności przedmiotu zamówienia. W przypadku, gdy w niniejszym opracowaniu dokonano opisu przedmiotu zamówienia za pomocą norm, aprobat, specyfikacji technicznych lub systemów odniesienia dopuszcza się rozwiązania równoważne opisywanym.

Zamawiający informuje, iż widniejące w zamówieniu jednostki będą przekazane do nieodpłatnego wykorzystania przez osobę/osoby trzecie w celach niekomercyjnych. Zamawiający dopuszcza możliwość wystąpienia sytuacji zmiany podmiotów na rzecz których następować będzie użyczenie. Wykonawcy uwzględniając wskazania ujęte w SIWZ i OPZ winni dostosować oferowane licencje do rzeczywistych pól eksploatacji oprogramowania przez beneficjentów.

1. Zestawy komputerowe dla jednostek podległych – 45 szt.

a. Jednostka centralna

Lp.	Nazwa komponentu / funkcji	Wymagane minimalne parametry techniczne
1.	Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
2.	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji graficznych, dostępu do Internetu oraz poczty elektronicznej
3.	Procesor	Zaprojektowany do pracy w komputerach stacjonarnych. Osiągający w teście PassMark CPU Mark wynik min. 4950 punktów W ofercie wymagane podanie producenta i modelu procesora. Do oferty należy dołączyć wydruk ze strony: http://www.cpubenchmark.net potwierdzający spełnienie ww. wymagania na dzień nie wcześniej niż 15.06.2015r. lub wydruk z przeprowadzonych testów, potwierdzony za zgodność z oryginałem przez Wykonawcę. Wydruk dopuszcza się w j. angielskim.
4.	Pamięć operacyjna	Co najmniej 8 GB. W ofercie należy podać wielkość zainstalowanej oraz możliwej do rozbudowania pamięci.
5.	Parametry pamięci masowej	Pojemność co najmniej 500 GB. W ofercie należy podać pojemność oraz – dla dysków HDD - prędkość obrotową dysku.
6.	Grafika	Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową ze wsparciem OpenGL 4.0, Shader 5.0.
7.	Wyposażenie multimedialne	Minimum 24-bitowa karta dźwiękowa zintegrowana z płytą główną, zgodna z HD, wewnętrzny głośnik 2W w obudowie komputera lub głośniki zewnętrzne stereo. Porty słuchawek i mikrofonu na przednim oraz na tylnym panelu odbudowy.
8.	Obudowa	Małogabarytowa typu small form factor, fabrycznie przystosowana do pracy w układzie pionowym i poziomym, wyposażona w minimum 2 kieszenie: 1 szt. 5,25” zewnętrzne typu „slim” i 1 szt. 3,5” wewnętrzne.

		Obudowa powinna fabrycznie umożliwiać montaż min. 1 szt. dysku 3,5" lub 2,5". Suma wymiarów obudowy nie może przekraczać 75 cm. W ofercie należy podać wymiary obudowy. Zasilacz o mocy min. 250W pracujący w sieci 230V 50/60Hz prądu zmiennego. W ofercie należy podać moc zasilacza. Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń, napędu optycznego i 3,5" dysku twardego bez konieczności użycia narzędzi (wyklucza się użycia śrub motylkowych). Obudowa jednostki centralnej musi być otwierana bez konieczności użycia narzędzi oraz posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym producenta komputera. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady) oraz kłódki (oczko na kłódkę). Obudowa musi posiadać wbudowany wizualny lub dźwiękowy system diagnostyczny służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, a w szczególności musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie złączy PCIe, płyty głównej, uszkodzenie kontrolera video, uszkodzenie dysku twardego, awarię BIOS'u, awarię procesora Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być on wpisany na stałe w BIOS.
9.	Zgodność z systemami operacyjnymi i standardami	Oferowany model komputera musi posiadać certyfikat producenta systemu operacyjnego potwierdzający poprawną współpracę oferowanego modelu komputera z oferowanym systemem operacyjnym (do oferty należy załączyć wydruk ze strony producenta oprogramowania).
10.	BIOS	Zgodny ze specyfikacją UEFI. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - wersji BIOS, - nr seryjnym komputera, - ilości i sposobu obłożenia slotów pamięciami RAM, - typie procesora wraz z informacją o ilości rdzeni, wielkości pamięci cache L2 i L3, - pojemności zainstalowanego dysku twardego - rodzajach napędów optycznych - MAC adresie zintegrowanej karty sieciowej Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS) Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. Możliwość polegająca na kontrolowaniu urządzeń wykorzystujących magistralę komunikacyjną PCI, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych. Pod pojęciem kontroli Zamawiający rozumie funkcjonalność polegającą na blokowaniu/odblokowaniu slotów PCI. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego oraz możliwość ustawienia następujących zależności pomiędzy nimi: brak możliwości zmiany hasła pozwalającego na uruchomienie systemu bez podania hasła administratora. Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowy tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Funkcja ta ma wymuszać podanie hasła administratora przy próbie zmiany ustawień BIOS w sytuacji, gdy zostało podane hasło systemowe. Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej, portu równoległego, portu szeregowego z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.

		Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. Możliwość wyłączania portów USB w tym: wszystkich portów, tylko portów znajdujących się na przodzie obudowy, tylko tylnych portów.
11.	Certyfikaty i standardy	Deklaracja zgodności CE (załączyć do oferty). Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji producenta jednostki lub wykonawcy (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram. Komputer musi spełniać wymogi normy Energy Star 5.0. Wymagany wpis dotyczący oferowanego modelu komputera w internetowym katalogu http://www.eu-energystar.org lub http://www.energystar.gov (wydruk ze strony internetowej załączyć do oferty).
12.	Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (WORK) wynosząca maksymalnie 21 dB. (załączyć raport badawczy wystawiony przez niezależną, polską akredytowaną jednostkę).
13.	Warunki gwarancji	5-letnia gwarancja producenta świadczona w miejscu instalacji z czasem reakcji w następnym dniu roboczym. Oferowany okres i poziom gwarancji musi wynikać bezpośrednio z numeru seryjnego komputera i być weryfikowalny na stronie internetowej bądź infolinii producenta komputera przez cały okres gwarancyjny.
16.	Wsparcie techniczne producenta	Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu komputera - do oferty należy dołączyć link strony.
17.	Oprogramowanie	Zainstalowany system operacyjny spełniający wymagania wskazane w pkt. 2. W ofercie należy podać producenta i nazwę oprogramowania. Zainstalowane oprogramowanie antywirusowe spełniające wymagania wskazane w pkt. 3. W ofercie należy podać producenta i nazwę oprogramowania.
18.	Wymagania dodatkowe	- Porty zintegrowane z płytą główną: VGA, DisplayPort, min. 8 portów USB wyprowadzonych na zewnątrz obudowy komputera w tym min. 2 porty USB 3.0; minimum dwa porty USB z przodu obudowy; wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp; porty słuchawek i mikrofonu na przednim oraz tylnym panelu obudowy. - Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), PXE 2.1 - Płyta główna wyposażona w min 1 złącze PCIex16 i min. 1xPCIex1, min. 2 sloty na instalacje kości pamięci z obsługą do min. 16GB pamięci RAM, min. 2 złącza do instalacji dysku w tym 1 szt. o szybkości transmisji min. 600 MB/s; - Klawiatura USB w układzie polski programisty. - Mysz optyczna USB z min dwoma klawiszami oraz rolką (scroll). - Wewnętrzna nagrywarka DVD +/-RW. - Do oferowanego sprzętu należy dołączyć nośniki ze sterownikami
	Dostawa	Dostawa komputerów do jednostek podległych: 1. Publiczna Szkoła Podstawowa w Janowie (5 szt.) 2. Publiczna Szkoła Podstawowa w Brzezinkach Starych (5 szt.), 3. Zespół Szkół w Tczowie (5 szt.) 4. Publiczna Szkoła Podstawowa w Baryczy (15 szt.) 5. Publiczna Szkoła Podstawowa w Zwoleniu (15 szt.)

b. Monitor

Lp.	Nazwa komponentu / funkcji	Wymagane minimalne parametry techniczne

1.	Typ	Monitor z ekranem ciekłokrystalicznym z aktywną matrycą TFT IPS min. 21,5”. W ofercie wymagane jest podanie modelu, symbolu oraz producenta
2.	Rozmiar plamki	max. 0,248 mm
3.	Podświetlenie	System podświetlenia LED
4.	Jasność	min. 250 cd/m ²
5.	Kontrast	Typowy 1000:1
6.	Kąty widzenia (pion/poziom)	Co najmniej 178°/178°
7.	Obsługiwana rozdzielczość	min. 1920 x 1080 @60 HZ
8.	Głębia kolorów	16,7 mln
9.	Możliwość pochylenia monitora	Wymagana w zakresie co najmniej 20 stopni do tyłu
10.	Bezpieczeństwo	Możliwość zastosowania zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady)
11.	Złącza	15-stykowe złącze D-Sub, złącze HDMI
12.	Certyfikaty i standardy	– Deklaracja zgodności CE (załączyć do oferty). – Monitor musi spełniać wymogi normy Energy Star 6.0. Wymagany wpis dotyczący oferowanego modelu komputera w internetowym katalogu http://www.eu-energystar.org lub http://www.energystar.gov (wydruk ze strony internetowej załączyć do oferty).
13.	Warunki gwarancji	5-letnia gwarancja producenta świadczona w miejscu instalacji. Czas reakcji serwisu - do końca następnego dnia roboczego.

2. System operacyjny dla jednostek podległych wraz z licencją umożliwiającą użytkowanie przez grupę docelową projektu – 45 szt.

Licencje bezterminowe na system operacyjny w polskiej wersji językowej, uprawniające do użytkowania najnowszej dostępnej w dniu składania oferty wersji systemu operacyjnego danego producenta.
Licencje muszą umożliwiać użytkowanie systemu na komputerach udostępnionych w punktach publicznego dostępu do Internetu.
System operacyjny zainstalowany na dostarczanych w ramach zamówienia komputerach musi spełniać następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;
2. możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;
3. darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat);
4. internetowa aktualizacja zapewniona w języku polskim;
5. wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
6. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe;
7. wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi);
8. funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer;
9. interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem
10. użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta;
11. możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
12. zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie;
13. praca systemu w trybie ochrony kont użytkowników;
14. zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych;
15. zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych;

16. funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika;
17. zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi;
18. wbudowany system pomocy w języku polskim;
19. możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabowidzących);
20. możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;
21. wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
22. automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
23. rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;
24. system musi posiadać narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
25. wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;
26. wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;
27. zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem;
28. rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami (obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową);
29. rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację;
30. graficzne środowisko instalacji i konfiguracji;
31. transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;
32. zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe udostępnianie modemu;
33. oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;
34. możliwość przywracania plików systemowych;
35. system operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.);
36. możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).

3. Oprogramowanie antywirusowe dla jednostek podległych – 45 szt.

1. Subskrypcja na minimum 60 miesięcy. Licencje umożliwiające użytkowanie na komputerach użyczonych beneficjentom projektu oraz udostępnionych w punktach publicznego dostępu do Internetu.
2. Pełne wsparcie dla zaoferowanego systemu operacyjnego.
3. Polska wersja programu.
4. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim.

Ochrona antywirusowa i antyspyware

5. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
6. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
7. Wbudowana technologia do ochrony przed rootkitami.
8. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
9. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
10. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania.
11. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
12. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
13. Aplikacja musi umożliwiać automatyczne uruchomienie skanowania w momencie wykrycia bezczynności systemu.

14. Bezczynność systemu musi być wykrywana co najmniej w oparciu o aktywny wygaszacz ekranu, blokadę komputera, wylogowanie użytkownika.
15. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
16. Możliwość skanowania dysków sieciowych i dysków przenośnych.
17. Skanowanie plików spakowanych i skompresowanych.
18. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń).
19. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
20. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
21. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
22. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
23. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
24. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
25. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
26. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird (w wersji 5.x lub starszej) i Windows Live Mail. Funkcje programu dostępne są bezpośrednio z menu programu pocztowego.
27. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird (w wersji 5.x lub starszej) i Windows Live Mail.
28. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
29. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
30. Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.
31. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
32. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
33. Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.
34. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez użytkownika.
35. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
36. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.
37. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
38. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
39. Użytkownik ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
40. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
41. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
42. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
43. W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne.
44. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
45. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość

określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.

46. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika
47. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
48. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
49. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
50. Interfejs programu ma oferować funkcję pracy w trybie bez grafiki gdzie cały interfejs wyświetlany jest w formie formatek i tekstu.
51. Interfejs programu ma mieć możliwość automatycznego aktywowania trybu bez grafiki w momencie, gdy użytkownik przełączy system Windows w tryb małej ilości kolorów (256).
52. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
53. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
54. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji musi być takie samo.
55. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
56. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
57. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
58. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
59. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
60. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych i płyt CD/DVD.
61. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model i wersję modelu urządzenia.
62. Aplikacja musi posiadać funkcjonalność, która automatycznie uzupełni elementy wymagane dla tworzenia reguł w oparciu o informacje dostępne z aktualnie podłączonego nośnika.
63. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia.
64. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
65. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
66. Użytkownik ma posiadać możliwość takiej konfiguracji aplikacji aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
67. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
68. Moduł HIPS musi posiadać możliwość pracy w jednym z czterech trybów:
    a. tryb automatyczny z regułami gdzie aplikacja automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    b. tryb interaktywny, w którym to aplikacja pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    c. tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    d. tryb uczenia się, w którym aplikacja uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu aplikacja musi samoczynnie przełączyć się w tryb pracy oparty na regułach.
69. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
70. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
71. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
72. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.

73. Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
74. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
75. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
76. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
77. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.
78. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się harmonogramie zadań aplikacji.
79. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie aplikacja włączała powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.
80. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.
81. Aplikacja musi posiadać opcję która umożliwi zgłoszenie podejrzanej witryny phishingowej bezpośrednio do laboratorium producenta.
82. Aplikacja musi posiadać funkcję, która automatycznie powiadomi o dostępnej, nowszej wersji oprogramowania.
83. Po zainstalowaniu aplikacji musi przeprowadzić wstępne skanowanie komputera.
84. Oprogramowanie musi posiadać zaawansowany skaner pamięci, który pozwala na wykrywanie i blokowanie zagrożeń, ukrytych w zmodyfikowanych aplikacjach
85. Program musi posiadać funkcję blokowania zagrożeń, które ukierunkowane są na luki (exploity) w aplikacjach takich jak m. in. przeglądarki internetowe, klienci pocztowi, czytniki PDF, itp.
86. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Ochrona przed spamem

87. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail, Windows Live Mail oraz Mozilla Thunderbird (w wersji 5.x lub starszej) wykorzystująca filtry Bayes-a, białą i czarną listę oraz bazę charakterystyk wiadomości spamowych.
88. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
89. Pełna integracja z programami pocztowymi MS Outlook, Outlook Express, Windows Mail, Windows Live Mail oraz Mozilla Thunderbird (w wersji 5.x lub starszej) – antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego.
90. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
91. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym.
92. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam.
93. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam.
94. Program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci" obecnym w programie Microsoft Outlook.
95. Program ma umożliwiać funkcjonalność która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana" oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana".
96. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

Zapora osobista (personal firewall)

97. Zapora osobista mogąca pracować jednym z 4 trybów:
98. tryb automatyczny – program umożliwia administratorowi zdefiniowanie wyjątków dla ruchu przychodzącego i wychodzącego na liście reguł. W przypadku, gdy nie będzie użytecznej reguły, tryb automatyczny blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące,
99. tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo),
100. tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany,
101. tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji.
102. Możliwość tworzenia list sieci zaufanych.

103. Możliwość dezaktywacji funkcji zapory sieciowej na kilka sposobów: pełna dezaktywacja wszystkich funkcji analizy ruchu sieciowego, tylko skanowanie chronionych protokołów oraz dezaktywacja do czasu ponownego uruchomienia komputera.
104. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
105. Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję.
106. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń.
107. Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu.
108. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet.
109. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
110. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu.
111. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
112. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
113. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
114. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, aktywności wyłącznie jednego połączenia sieciowego lub wielu połączeń sieciowych konkretny interfejs sieciowy w systemie.
115. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS zarówno z wykorzystaniem adresów IPv4 jak i IPv6.
116. Opcje związane z autoryzacją stref mają oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji celem zwiększenia dokładności identyfikacji danej sieci.
117. Możliwość aktualizacji sterowników zapory osobistej po restarcie komputera.
118. Program musi umożliwiać ochronę przed lukami w systemie operacyjnym.
119. Program musi posiadać opcję zaawansowanego logowania PCAP

Kontrola rodzicielska

120. Aplikacja musi być wyposażona w zintegrowany moduł kontroli rodzicielskiej.
121. Moduł Kontroli rodzicielskiej musi posiadać możliwość dodawania różnych użytkowników dla których będą stosowane reguły filtrowania.
122. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.
123. Dla kont użytkowników musi istnieć możliwość przypisania gotowych profili filtrowania kategorii.
124. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
125. Aplikacja musi posiadać możliwość filtrowania url w oparciu o co najmniej 46 kategorii.
126. Podstawowe kategorie w jakie aplikacja musi być co najmniej wyposażona to: Poczta email i sms, rozrywka, moda i uroda, sprawność i rekraracja, zdrowie i medycyna, Informatyka, mapy, Aktualności Usługi biznesowe, pobieranie plików, komunikatory czaty i fora, nagość, zakupy, broń, treści dla dorosłych, przestępczość i narkotyki, hazard, przemoc i nienawiść, dla dzieci, gry, wyszukiwarki i portale, informatyka, bezpieczeństwo i szkodliwe oprogramowanie, przestępczość i podejrzane oprogramowanie.
127. Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta.
128. Aktualizacje baz filtrowanych url mają być pobierane wraz z aktualizacjami sygnatur wirusów – nie jest wymagane uruchamianie osobnego zadania aktualizacji adresów url dla modułu kontroli rodzicielskiej.
129. Dla poszczególnych kont użytkownik ma posiadać możliwość utworzenia wyjątków dla konkretnych adresów url które mogą być wyświetlone nawet w przypadku gdy dany adres znajduje się w którejkolwiek z blokowanych kategorii.
130. Aplikacja musi być wyposażona w moduł logowania zablokowanych stron oraz kategorii niezależnie od zalogowanego użytkownika.
131. Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli rodzicielskiej.

Zabezpieczenie portali społecznościowych

132. Aplikacja musi posiadać możliwość uruchomienia skanera zawartości profil użytkownika na portalu Facebook.
133. Skaner musi posiadać możliwość skanowania obiektów znajdujących się na tablicach znajomych użytkownika.
134. Skaner musi mieć możliwość dodania ostrzeżenia pod zarażonymi lub podejrzanymi obiektami.
135. Skaner musi posiadać możliwość automatycznego skanowania dodawanych obiektów oraz możliwość uruchomienia skanowania na żądanie.

136. Skaner musi posiadać możliwość uruchomienie skanera antywirusowego online bezpośrednio z poziomu interfejsu aplikacji Facebook'a.
137. Skaner musi posiadać możliwość gromadzenia statystyk skanowania profili.
138. Aplikacja musi posiadać możliwość powiadomienia użytkownika poprzez wiadomość e-mail o zagrożeniach wykrytych podczas procesu automatycznego skanowania zawartości profilu.
139. Aplikacja musi posiadać możliwość publikacji statystyk odnośnie liczby wykonanych skanowań oraz wykrytych zagrożeń na ścianie użytkownika.