Ministerstwo Cyfryzacji

Narodowe Standardy Cyberbezpieczeństwa

Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO)

v. 1.00 – luty 2020

Ministerstwo Cyfryzacji
ul. Królewska 27I 00-060 Warszawa I tel.: +48 22 250 01 10 I tel.: +48 22 250 28 85 I e-mail: mc@mc.gov.pl www.mc.gov.pl

Spis treści

1 Wprowadzenie

Chmura obliczeniowa to technologia rozproszonego przetwarzania danych, w której skalowalne zasoby informacyjne (infrastruktura, platforma aplikacyjna i oprogramowanie) udostępniane są jako usługi dla wielu odbiorców organizacyjnych i indywidualnych.

Na chmurę obliczeniową składają się usługi teleinformatyczne dostosowywane dynamicznie do potrzeb i udostępniane w rozliczalny sposób za pośrednictwem sieci, z wykorzystaniem bezpiecznych protokołów sieciowych. Korzystanie z usług chmur obliczeniowych możliwe jest za pomocą interfejsów oferowanych przez dostawców usług.

Technologie chmur obliczeniowych wprowadzają nowe modele przetwarzania danych, niezależne od miejsca ich przechowywania – dlatego chmura obliczeniowa, to nie miejsce tylko model przetwarzania.

1.1 Przeznaczenie, cel i odbiorcy dokumentu

Dokument „Standardy Cyberbezpieczeństwa Chmur Obliczeniowych" został opracowany w ramach zbioru Narodowych Standardów Cyberbezpieczeństwa, przywołanego w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024[1].
Opracowanie Narodowych Standardów Cyberbezpieczeństwa jest realizacją celu szczegółowego 2 – *Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty*.
Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) stanowią zbiór wymagań prawnych, organizacyjnych i technicznych zapewniających cyberbezpieczeństwo w modelach wdrażania chmur obliczeniowych w ramach inicjatywy Wspólna Infrastruktura Informatyczna Państwa (WIIP)[2].
Wśród strategicznych kierunków, jakie realizuje inicjatywa WIIP są m.in:

- podniesienie poziomu bezpieczeństwa przetwarzania danych i świadczenia usług elektronicznych w administracji rządowej;
- trwałe obniżenie kosztów stałych przetwarzania danych;
- podniesienie efektywności wydatkowania środków w projektach zawierających elementy infrastruktury IT;
- skrócenie czasu realizacji nowych przedsięwzięć informatycznych przez szybsze udostępnianie wymaganej infrastruktury IT;
- ograniczenie zjawiska wielokrotnego gromadzenia tych samych danych w środowiskach informatycznych oraz zniesienie barier technologicznych w przypadku rejestrów publicznych;
- upowszechnienie modelu przetwarzania w chmurach obliczeniowych, jako głównego sposobu realizacji systemów teleinformatycznych państwa (w tym również zmiana technologii wytwarzania oprogramowania).

Ważnym elementem inicjatywy WIIP jest opracowanie klasyfikacji systemów teleinformatycznych[3] oraz wdrożenie jednolitych standardów bezpieczeństwa infrastruktury przetwarzania danych, które umożliwią migrację systemów i danych do modelu przetwarzania w chmurze obliczeniowej.

[1] Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 - http://monitorpolski.gov.pl/mp/2019/1037/1
[2] Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa - http://monitorpolski.gov.pl/mp/2019/862/1
[3] klasyfikacja zawarta została w załączniku nr 2 do uchwały ws. inicjatywy WIIP.

Działania w ramach inicjatywy WIIP są również elementem budowy krajowego systemu cyberbezpieczeństwa[4].

Standardy Cyberbezpieczeństwa Chmur Obliczeniowych określają wymagania, jakie muszą spełnić:

- podmioty administracji rządowej zarządzające Centrami Przetwarzania Danych (CPD), w celu ich przyłączenia do Rządowego Klastra Bezpieczeństwa (RKB) lub włączenia do wspólnych zasobów Rządowej Chmury Obliczeniowej (RChO).
- dostawcy usług chmur obliczeniowych w ramach Publicznej Chmury Obliczeniowej (PChO).

Odbiorcami Standardów Cyberbezpieczeństwa Chmur Obliczeniowych są:

- publiczni i komercyjni dostawcy usług chmurowych dla administracji publicznej,
- jednostki administracji publicznej planujący wykorzystanie lub korzystający z rządowych i/lub publicznych usług przetwarzania w modelach chmur obliczeniowych.

Przetwarzanie w modelach chmur obliczeniowych opiera się na założeniu wysokiego poziomu standaryzacji sprzętu, oprogramowania i usług, których szczegółów implementacyjnych odbiorca zwykle nie zna. W związku z tym wymagany jest szczególnie wysoki poziom zaufania do dostawców usług w chmurach obliczeniowych.

Istnieją różne narodowe i branżowe standardy wymagań oraz certyfikacji bezpieczeństwa dla usług w chmurach obliczeniowych. Z tego powodu odbiorcy usług chmur obliczeniowych mają trudności z przeglądem i porównywaniem zakresu oraz poziomu bezpieczeństwa usług oferowanych przez różnych dostawców. Standardy Cyberbezpieczeństwa Chmur Obliczeniowych mają stanowić pomoc dla jednostek administracji publicznej planujących skorzystanie z modelu przetwarzania danych w chmurach obliczeniowych, upraszczając proces wyboru dostawcy, zakresu usług i oceny cyberbezpieczeństwa środowiska przetwarzania.

[4] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).

2 Struktura Standardów Cyberbezpieczeństwa Chmur Obliczeniowych

Zakres usług oferowanych w ramach modeli chmur obliczeniowych obejmuje całe spektrum technologii informacyjnych, w szczególności infrastrukturę (np. moc obliczeniowa, pamięć masowa), platformy aplikacyjne (np. repozytoria aplikacji), oprogramowanie i usługi bezpieczeństwa.

Do zdefiniowania wymagań bezpieczeństwa dla modeli chmur obliczeniowych niezbędne jest wprowadzenie standaryzacji definicji celów bezpieczeństwa informacji oraz poziomów potencjalnego wpływu na bezpieczeństwo informacji – zawiera je rozdział 3.

Proces wyboru optymalnego modelu chmury obliczeniowej powinien w szczególności uwzględniać analizę ryzyka z punktu widzenia celów bezpieczeństwa (poufności, integralności i dostępności) oraz klasyfikacji systemu (m.in. jego wpływu na realizowane zadania statutowe) – proces ten został opisany w rozdziale 4.

Dostawcy usług w modelach chmur obliczeniowych są odpowiedzialni za zaprojektowanie, opis, wdrożenie i skuteczne działanie zabezpieczeń organizacyjnych i technicznych spełniających wymagania bezpieczeństwa – wymagania te zostały opisane w rozdziale 5.

Usługi przetwarzania w modelach chmur obliczeniowych będą stanowiły element krajowego systemu stąd konieczne jest dostosowanie do zasad i wymagań zdefiniowanych w ustawie o krajowym systemie cyberbezpieczeństwa oraz rozporządzeń do tej ustawy, w szczególności regulujących kwestie realizacji usług cyberbezpieczeństwa oraz zgłaszania incydentów – tym zagadnieniom poświęcony jest rozdział 6.

W załącznikach do Standardów Cyberbezpieczeństwa Chmur Obliczeniowych zawarto następujące informacje:

- Załącznik 1 – Wykaz przepisów prawnych, przywoływanych norm krajowych i międzynarodowych,
- Załącznik 2 – Słownik pojęć,
- Załącznik 3 – Wykaz skrótów,
- Załącznik 4 – Podstawowe Wymagania Bezpieczeństwa – macierz zabezpieczeń,
- Załącznik 5 – Katalog zabezpieczeń.

3 Cele bezpieczeństwa i kategorie potencjalnego wpływu na bezpieczeństwo

3.1 Cele bezpieczeństwa (poufność, integralność, dostępność)

Cele bezpieczeństwa informacji uwzględniają zagrożenia w zakresie poufności, integralności i dostępności[5].

Zgodnie z FIPS 199:

- poufność - zachowanie autoryzowanych ograniczeń w dostępie i ujawnianiu informacji, w tym środki ochrony prywatności i informacji o zastrzeżonym dostępie. Utrata poufności to nieuprawnione ujawnienie informacji.
- integralność - zabezpieczenie przed niewłaściwą modyfikacją lub zniszczeniem informacji; obejmuje zapewnienie niezaprzeczalności i autentyczności informacji. Utrata integralności to nieautoryzowana modyfikacja lub zniszczenie informacji. Należy zauważyć, że nieuprawnione zniszczenie informacji spowoduje utratę dostępności tych informacji.
- dostępność - zapewnienie terminowego i niezawodnego dostępu do informacji i ich wykorzystywania. Utrata dostępności oznacza zakłócenie dostępu lub możliwości korzystania z informacji lub systemu teleinformatycznego.

Zgodnie z uchwałą WIIP wymaga się od odbiorców usług chmur obliczeniowych, aby klasyfikowali swoje systemy informatyczne uwzględniając łącznie potencjalny wpływ na bezpieczeństwo wynikający z konieczności zapewnienia poufności, integralności i dostępności informacji.

Bezpośredni wpływ na kategoryzację systemu teleinformatycznego ma najwyższa wartość spośród oszacowanych celów bezpieczeństwa. Ogólny wzór wyznaczania kategoryzacji bezpieczeństwa (SC[6]) systemu teleinformatycznego:

System teleinformatyczny SC = {(poufność, wpływ), (integralność, wpływ), (dostępność, wpływ)},

gdzie dopuszczalne wartości potencjalnego wpływu są niskie, umiarkowane lub wysokie, zgodnie z Tabelą 1.

[5] NIST FIPS Publication 199
[6] ang. Security Categorization

Tabela 1. Macierz – cele bezpieczeństwa i kategorie potencjalnego wpływ na bezpieczeństwo

	Poziom potencjalnego wpływ na bezpieczeństwo		
Cele bezpieczeństwa	**Niski (L)**	**Umiarkowany (M)**	**Wysoki (H)**
Poufność - zachowanie autoryzowanych ograniczeń w dostępie i ujawnianiu informacji, w tym środki ochrony prywatności i informacji o zastrzeżonym dostępie	Nieuprawnione ujawnienie informacji będzie miało **ograniczony** niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.	Nieuprawnione ujawnienie informacji będzie miało **poważny** niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.	Nieuprawnione ujawnienie informacji będzie miało **silny lub katastrofalny** niekorzystny wpływ na operacje organizacyjne, aktywa organizacyjne lub osoby fizyczne.
Integralność - zabezpieczenie przed niewłaściwą modyfikacją lub zniszczeniem informacji; obejmuje zapewnienie niezaprzeczalności i autentyczności informacji	Nieautoryzowana modyfikacja lub zniszczenie informacji będzie miała **ograniczony** niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.	Nieautoryzowana modyfikacja lub zniszczenie informacji może miała **poważny** niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.	Nieautoryzowana modyfikacja lub zniszczenie informacji będzie miała **silny lub katastrofalny** niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.
Dostępność - zapewnienie terminowego i niezawodnego dostępu do informacji i ich wykorzystywania	Zakłócenie dostępu lub możliwości korzystania z informacji lub systemu teleinformatycznego będzie miało **ograniczony** niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.	Zakłócenie dostępu lub możliwości korzystania z informacji lub systemu teleinformatycznego będzie miało **poważny** niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.	Zakłócenie dostępu lub możliwości korzystania z informacji lub systemu teleinformatycznego będzie miało **silny lub katastrofalny** niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.

3.2 Poziomy wymagań bezpieczeństwa SCCO determinujące stosowanie poszczególnych modeli chmur obliczeniowych

Poziomy Wymagań Bezpieczeństwa SCCO determinujące stosowanie poszczególnych modeli chmur obliczeniowych są określane przez korelację:

1) wrażliwości lub poziomu poufności informacji (np. publicznych, urzędowych, niejawnych itp.), które mają być przechowywane oraz przetwarzane w środowisku dostawcy usług chmur obliczeniowych;
2) poziomu potencjalnego wpływu zdarzenia, które powoduje utratę poufności, integralności lub dostępności tych informacji.

Kategoryzacja bezpieczeństwa systemu teleinformatycznego ma bezpośredni wpływ na określenie Poziomu Wymagań Bezpieczeństwa determinującego wybór modelu chmur obliczeniowych - RChO/PChO.

Kategoryzacji systemu teleinformatycznego dokonuje jego gestor.

Poziomy Wymagań Bezpieczeństwa SCCO:

- Poziom SCCO1: Niekontrolowane informacje nieklasyfikowane,
- Poziom SCCO2: Kontrolowane informacje urzędowe,
- Poziom SCCO3: Kontrolowane wrażliwe informacje urzędowe,
- Poziom SCCO4: Informacje niejawne[7].

[7] Obecnie wyłączone z inicjatywy WIIP

SCCO	KATEGORIE INFORMACJI	WYMAGANE ZABEZPIECZENIA DLA CHMURY OBLICZENIOWEJ	CENTRA PRZETWARZANIA DANYCH - JURYSDYKCJA	DOSTĘP DO ZASOBÓW	SEPARACJA	WYMAGANIA DLA PERSONELU
1	Niekontrolowane informacje nieklasyfikowane	Zabezpieczenia SCCO na poziomie NISKIM / UMIARKOWANYM potencjalnego wpływu na atrybuty bezpieczeństwa	Przetwarzanie dozwolone w centrach danych poza polską jurysdykcją	Internet i/lub wydzielone usługi transmisji danych	Wirtualna/Logiczna DOSTĘP PUBLICZNY	Personel dopuszczany przez dostawcę usług chmur obliczeniowych
2	Kontrolowane informacje urzędowe	Poziom SCCO1 + zabezpieczenia do ochrony informacji urzędowych	Przetwarzanie dozwolone w centrach danych w polskiej jurysdykcji	Internet i/lub wydzielone łącza logiczne – wymagania Narodowych Standardów Cyberbezpieczeństwa	Wirtualna/Logiczna Silna separacja pomiędzy organizacyjnymi zasobami publicznych chmur obliczeniowych (tenantami) oraz dedykowany kontrolowany dostęp do zasobów informacyjnych	Personel posiadający poświadczenia bezpieczeństwa osobowego na poziomie „POUFNE”
3	Kontrolowane wrażliwe informacje urzędowe	Poziom SCCO2 + zabezpieczenia Rządowego Klastra Bezpieczeństwa	Przetwarzanie danych w Rządowej Chmurze Obliczeniowej (RChO)	Rządowy Klaster Bezpieczeństwa	Wirtualna/Logiczna Silna separacja pomiędzy organizacyjnymi zasobami RChO oraz dedykowane i kontrolowane przez RKB punkty styku z sieciami publicznymi	Personel posiadający poświadczenia bezpieczeństwa osobowego na poziomie „TAJNE”
4	Informacje niejawne	Poziom SCCO3 + wymagania ochrony informacji niejawnych	Przetwarzanie w centrach danych akredytowanych do przetwarzania określonej klauzuli informacji niejawnych	Sieci akredytowane do przekazywania określonej klauzuli informacji niejawnych	Akredytacja bezpieczeństwa dla wszystkich zasobów dedykowanych chmur obliczeniowych. Silna separacja od sieci publicznych	Personel posiadający poświadczenia bezpieczeństwa osobowego na poziomie „ŚCIŚLE TAJNE” lub „TAJNE”

3.2.1 Poziom SCCO1: Niekontrolowane informacje nieklasyfikowane

Poziom SCCO1 obejmuje wszystkie dane przeznaczone do publicznego udostępnienia – bez prawnych wymagań dotyczących zachowania poufności (np. publiczne strony internetowe). Obejmuje również niektóre informacje wymagające minimalnej kontroli dostępu.

Dostęp do usług odbywa się przez Internet i/lub za pośrednictwem logicznie wydzielonych usług transmisji danych.

Poziom SCCO1 obejmuje informację publiczną, która:

- nie jest informacją prawnie chronioną,
- może posiadać ograniczenia związane z prawem autorskim.

Konsekwencje ujawnienia niekontrolowanej informacji nieklasyfikowanej:

- brak negatywnych konsekwencji dostępu osób nieuprawnionych do informacji lub konsekwencje w postaci skutków prawnych związanych z prawem autorskim.

Poziom SCCO1 Obsługuje informacje o **niskim poziomie poufności**, maksymalnie **umiarkowanym poziomie integralności,** niskim **poziomie dostępności** - SC=(L, M, L).

Jednostki administracji publicznej mogą przetwarzać informacje na poziomie SCCO1 z wykorzystaniem usług publicznych chmur obliczeniowych.

3.2.2 Poziom SCCO2: Kontrolowane informacje urzędowe

Poziom SCCO2 obejmuje informacje istotne dla realizacji działań statutowych instytucji administracji publicznej, udostępniane bez ograniczeń pracownikom instytucji lub na podstawie porozumień o zachowaniu poufności.

Poziom SCCO2 obejmuje informacje, która:

- zawiera dane osobowe podlegające ochronie ustawowej,
- zawiera tajemnicę przedsiębiorcy, w tym tajemnice branżowe/instytucjonalne podlegające prawnej ochronie,
- nie jest informacją niejawną, chronioną na podstawie odrębnych przepisów.

Konsekwencje ujawnienia informacji:

- negatywne konsekwencje związane z nieupoważnionym dostępem związane są z naruszeniem ustawy o ochronie danych osobowych, naruszeniem ustaw o ochronie tajemnic zawodowych, naruszeniem tajemnicy przedsiębiorcy i co za tym idzie, mogą wywołać określone ustawowe sankcje (np. art. 23 ustawy o dostępie informacji publicznej).

Poziom SCCO2 Obsługuje informacje o **umiarkowanym poziomie poufności**, umiarkowanym **poziomie integralności**, **umiarkowanym poziomie dostępności** - SC=(M, M, M).

Jednostki administracji publicznej mogą przetwarzać informacje ma poziomie SCCO2 z wykorzystaniem usług publicznych chmur obliczeniowych pod warunkiem spełnienia przez dostawcę usług organizacyjnych i technicznych wymagań SCCO.

3.2.3 Poziom SCCO3: Kontrolowane wrażliwe informacje urzędowe

Poziom SCCO3 obejmuje:

- wrażliwe, prawnie chronione informacje i dane referencyjne krajowych rejestrów - określone w odrębnych przepisach (w tym dane o kluczowym znaczeniu dla bezpieczeństwa publicznego);
- inne informacje wymagające jednoznacznego oznaczenia jako informacje o ograniczonym dostępie, w szczególności których nieuprawnione ujawnienie może obniżać skuteczność zabezpieczeń stosowanych w systemach administracji rządowej.

Ze względu na wrażliwość tych informacji mogą one być przechowywane i przetwarzane tylko w środowisku Rządowej Chmury Obliczeniowej (RChO). Wysoka dostępność wymagana jest dla zachowania ciągłości realizacji procesów biznesowych i zadań statutowych jednostek administracji publicznej, również w przypadku braku dostępu do usług sieci Internet.
Poziom SCCO 3 Obsługuje informacje o **wysokim poziomie poufności**, **wysokim poziomie integralności** oraz **wysokim poziomie dostępności** - SC=(H, H, H).

3.2.4 Poziom SCCO4: Informacje niejawne

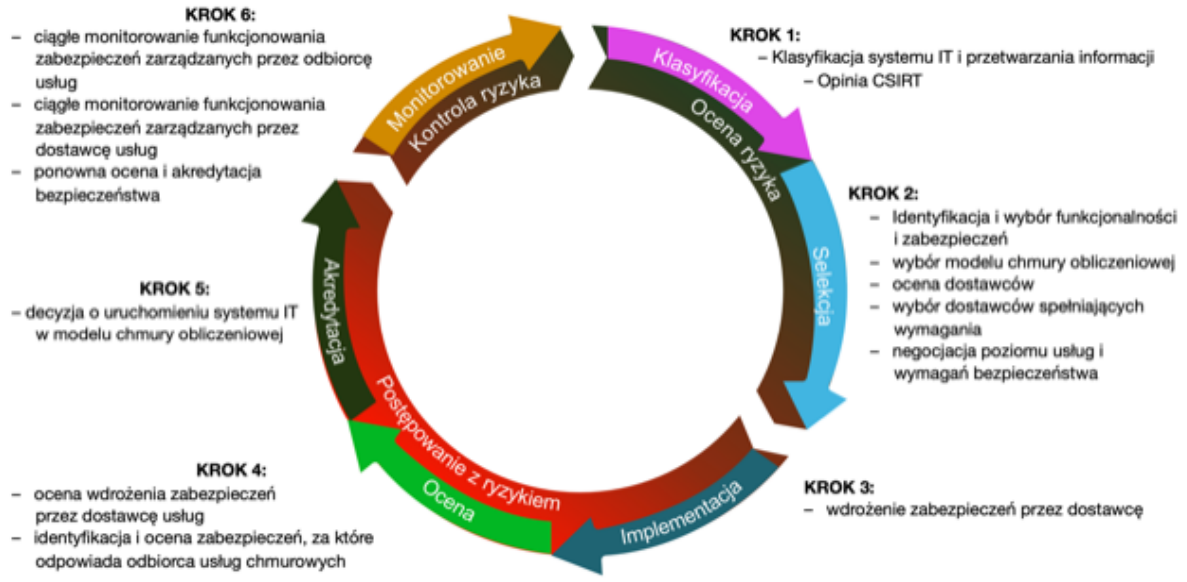
Obejmuje informacje klasyfikowane jako niejawne zgodnie z Ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.
Obecnie brak możliwości przetwarzania informacji niejawnych w formalnie nieakredytowanych środowiskach chmur obliczeniowych.

4 Proces przygotowania do przetwarzania informacji w modelach chmur obliczeniowych

Przetwarzanie informacji modelach chmur obliczeniowych wymaga dostosowania procesów zarządzania ryzykiem, które zazwyczaj dotyczą lokalnych zasobów fizycznych, systemów i aplikacji. Bardzo istotne jest określenie zakresu odpowiedzialności za realizację poszczególnych usług przetwarzania przy założeniu, że świadczone są one przez zewnętrzne podmioty. Dodatkowo, niezbędne jest spełnienie wymagań bezpieczeństwa i kontroli w stosunku do krytyczności informacji przetwarzanych w modelach chmur obliczeniowych, w sposób opłacalny i wydajny, przy jednoczesnym zapewnieniu bezpieczeństwa realizacji zadań statutowych.

Proces oceny ryzyka przy migracji informacji do przetwarzania w modelach chmur obliczeniowych koncentruje się na ocenie wymagań dla poziomów potencjalnego wpływu na bezpieczeństwo informacji. Potencjalni odbiorcy usług przy wyborze oferty dostawcy usług chmur obliczeniowych kierują się potrzebami operacyjnymi i funkcjonalnymi oraz weryfikują ich zgodność z wymaganiami SCCO na poziomie odpowiadającym klasyfikacji systemu i informacji, które mają być przetwarzane z wykorzystaniem usług chmur obliczeniowych.

Proces zarządzania ryzkiem związanym z przetwarzaniem informacji w modelach chmur obliczeniowych został opisany w poniższym cyklu RMF[8].



Rysunek 1 Ramy zarządzania ryzykiem zastosowane w ekosystemie chmury - perspektywa Odbiorcy usług w chmurze.

Działania potencjalnych odbiorców usług chmur obliczeniowych związane z zarządzaniem ryzykiem obejmują następujące kroki:

1. Ocena ryzyka – (analiza środowiska modelu chmur obliczeniowych w celu zidentyfikowania potencjalnych podatności dla bezpieczeństwa informacji)

[8] Ang. Risk Management Framework

Krok 1: Klasyfikacja

- Klasyfikacja systemu teleinformatycznego i przetwarzanych informacji, przechowywanych i przesyłanych przez ten system na podstawie analizy wpływu systemu na realizację zadań statutowych,
- Opinia właściwego CSIRT poziomu krajowego, w przypadku planowanego wykorzystania usług publicznych chmur obliczeniowych. zgodnie z § 8 uchwały WIIP.

Krok 2: Selekcja

- Identyfikacja i wybór możliwości funkcjonalnych dla całego systemu teleinformatycznego, powiązanych z nim podstawowych zabezpieczeń[9] w oparciu o poziom potencjalnego wpływu na bezpieczeństwo informacji, kontrole prywatności i rozszerzone kontrole bezpieczeństwa,
- Identyfikacja i wybór najlepiej dopasowanego modelu chmury obliczeniowej dla danego systemu teleinformatycznego,
- Ocena dostawców usług chmur obliczeniowych spełniających kryteria zdefiniowane przez potencjalnego odbiorcę usług chmur obliczeniowych (w tym architektura, możliwości funkcjonalne, zarządzanie i monitorowanie usług),
- Wybór dostawców usług chmur obliczeniowych, którzy najlepiej spełniają wymagania funkcjonalne oraz wymagania bezpieczeństwa (najlepiej wybrać dostawcę, który stosuje więcej zabezpieczeń organizacyjnych i technicznych, tak, aby minimalizować liczbę dodatkowych zabezpieczeń, które muszą być stosowane po stronie odbiorcy usług chmur obliczeniowych. Na tym etapie określa się zabezpieczenia, które zostaną wdrożone przez odbiorcę usług chmur obliczeniowych, zabezpieczenia wdrożone przez dostawców usług chmur obliczeniowych w ramach oferowanych usług oraz zabezpieczenia, które należy dostosować (poprzez stosowanie zamiennych zabezpieczeń i wybór określonych parametrów dla tych zabezpieczeń),
- Negocjacja umowy definiującej poziom świadczonych usług chmur obliczeniowych[10] SLA oraz wymagania bezpieczeństwa. Udokumentowanie wszystkich stosowanych zabezpieczeń. Przegląd i zatwierdzenie dokumentu polityki bezpieczeństwa. W przypadku wykorzystania w procesie sytemu ZUCH (usługa świadczona przez Ministra Cyfryzacji) etap negocjacji realizowany jest dla całego katalogu usług PChO, zaś odbiorca otrzymuje standardową umowę zgodną z niniejszymi standardami.

2. Postępowanie z ryzykiem (projektowanie, mitygacja, polityki i plany)

Krok 3: Implementacja

- Wdrożenie zabezpieczeń, za które odpowiedzialny jest odbiorca usług chmur obliczeniowych.

Krok 4: Ocena

- Ocena wdrożenia zabezpieczeń przez dostawcę usług chmur obliczeniowych,
- Identyfikacja i ocena wszelkich dziedziczonych i zależnych relacji między zabezpieczeniami stosowanymi przez dostawcę i odbiorcę usług chmur obliczeniowych.

Krok 5: Akredytacja

- Decyzja kierownika jednostki organizacyjnej o uruchomieniu systemu teleinformatycznego korzystającego z usług w modelach chmur obliczeniowych.

[9] ang. Security Controls
[10] ang. Service Level Agreement - SLA

3. Kontrola ryzyka (monitorowanie ryzyka, przegląd zdarzeń, korekty w polityce bezpieczeństwa)
   Krok 6: Monitorowanie
   - Ciągłe i w czasie rzeczywistym monitorowanie funkcjonowania zabezpieczeń zarządzanych przez odbiorcę usług chmur obliczeniowych,
   - Ciągłe i w czasie rzeczywistym monitorowanie funkcjonowania zabezpieczeń zarządzanych przez dostawcę usług chmur obliczeniowych,
   - Ponowna ocena i ponowna akredytacja (okresowa lub ciągła) bezpieczeństwa usług świadczonych przez dostawcę usług chmur obliczeniowych.

Podejście opisane powyżej (schemat sześciu kroków) umożliwia organizacjom systematyczne stosowanie i monitorowanie zabezpieczeń wspólnych, hybrydowych i specyficznych dla systemów teleinformatycznych oraz formułowanie wymagań bezpieczeństwa uwzględnianych w postępowaniach o zamówienia publiczne na dostawę usług w modelach chmur obliczeniowych.

Odbiorca usług chmur obliczeniowych odpowiada za prowadzenie oceny ryzyka, identyfikację wszystkich wymagań bezpieczeństwa wobec usług w wybranych modelach chmur obliczeniowych oraz potwierdzenie zabezpieczeń stosowanych przez dostawcę usług chmur obliczeniowych przed zawarciem umowy o świadczenie usług.

Dostawcy usług chmur obliczeniowych, którzy w największym stopniu spełniają potrzeby odbiorcy usług chmur obliczeniowych, powinni być wybierani z katalogu usług w ramach Systemu Zapewniania Usług Chmurowych – ZUCH, lub bezpośrednio w przypadku zamawiania usług poza Wspólną Infrastrukturą Informatyczną Państwa. Katalog usług ZUCH dostępnych jest online pod adresem: chmura.gov.pl.

Dostawcy usług publicznych chmur obliczeniowych będą podlegali certyfikacji w ramach europejskiego programu certyfikacji cyberbezpieczeństwa opracowanego na postawie projektu CSP CERT Europe (www.cspcert.eu).

Umowa o świadczenie usług chmur obliczeniowych musi zawierać część szczegółowo określającą rodzaje usług i poziomy usług (SLA), które mają być świadczone, w tym między innymi czas dostawy, dostępność i parametry wydajnościowe.

Odbiorca usług chmur obliczeniowych musi zwrócić szczególną uwagę na postanowienia w umowie odnoszące się do poziomów bezpieczeństwa świadczonych usług, również korzystać z opinii zespołów CSIRT i zewnętrznych ekspertów, aby upewnić się, że warunki umowy pozwolą organizacji na realizację zadań statutowych i spełnienie wymagań dotyczących wydajności.

Jednym z wyzwań przy wyborze ofert usług chmur obliczeniowych jest to, że dostawcy usług chmur obliczeniowych mogą oferować domyślną umowę napisaną z perspektywy dostawcy. Takie domyślne umowy mogą w niewystarczającym stopniu zaspokajać potrzeby odbiorców usług chmur obliczeniowych.

Podsumowując, podjęcie decyzji o migracji systemu teleinformatycznego do modelu chmur obliczeniowych wymaga od organizacji dokładnej identyfikacji własnych wymagań bezpieczeństwa oraz oceny adekwatności zakresu i zabezpieczeń usług oferowanych przez danego dostawcę usług chmur obliczeniowych, wynegocjowania warunków umowy

uwzględniających wymagane poziomy bezpieczeństwa usług oraz budowania zaufania z dostawcą usług chmur obliczeniowych przed akredytacją uruchamianych w nich usług przetwarzania informacji.

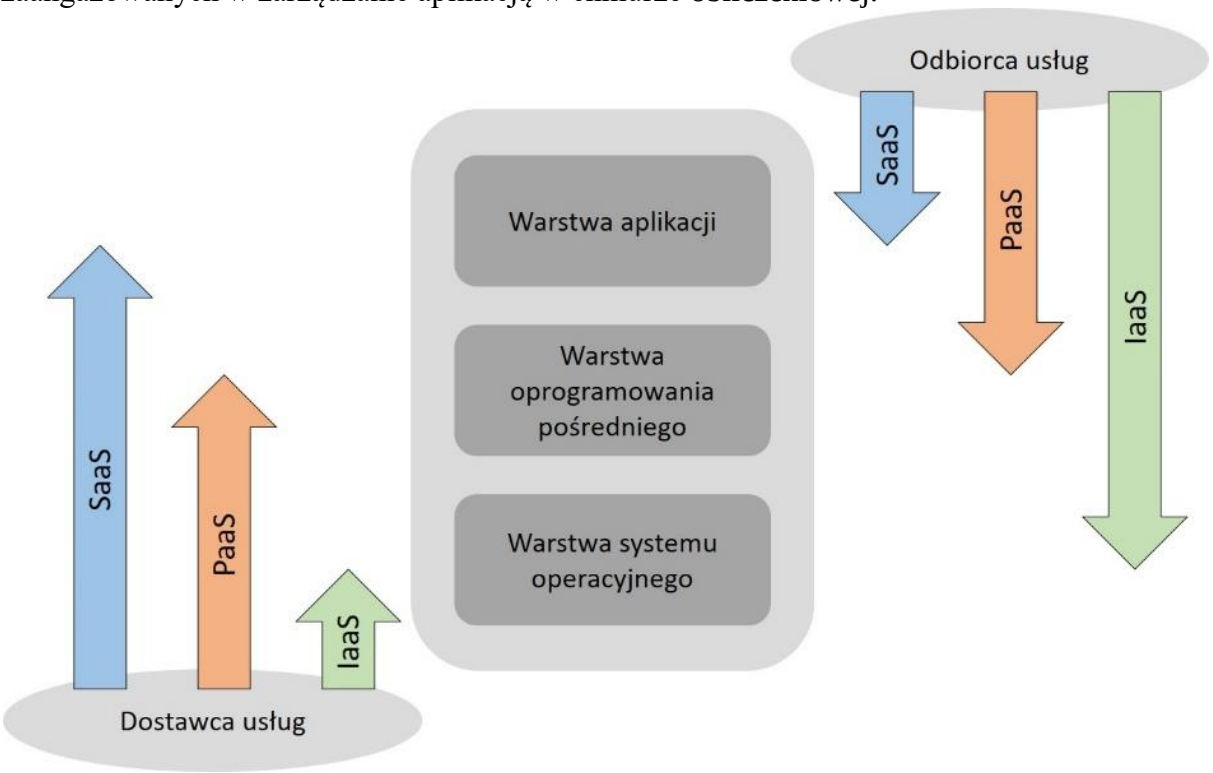
Szczegółowe szacowanie ryzyka w połączeniu z bezpieczną organizacją ekosystemu chmur obliczeniowych spełniającego wymagania SCCO, wraz z odpowiednimi wskazówkami dotyczącymi negocjowania umów ma wspierać odbiorców usług chmur obliczeniowych w zarządzaniu ryzykiem i podejmowaniu świadomych decyzji w zakresie wykorzystania modeli chmur obliczeniowych, które z założenia powinny zapewniać wyższy poziom bezpieczeństwa od systemów korzystających z lokalnej, dedykowanej infrastruktury teleinformatycznej.

Korzystając z ekosystemu chmur obliczeniowych, odbiorcy usług, jako właściciele informacji powiązanych, pozostają odpowiedzialni za ich zabezpieczenie proporcjonalnie do klasyfikacji informacji. Poziom kontroli i bezpośredniego zarządzania usługami w chmurach obliczeniowych różni się w zależności od wykorzystywanego modelu usług chmur obliczeniowych.

4.1 Współdzielona odpowiedzialność za ochronę zasobów modelach chmur obliczeniowych

Dostawca i odbiorca usług chmur obliczeniowych współdzielą kontrolę nad zasobami środowiska. Jak pokazano na środowiska. Jak pokazano na

Rysunek 2, różne modele usług w chmurach obliczeniowych wpływają na kontrolę organizacji nad zasobami obliczeniowymi, a tym samym na to, jakie działania możliwe są w środowisku chmury obliczeniowej. Rysunek pokazuje te różnice za pomocą klasycznej notacji stosu oprogramowania złożonej z warstw aplikacji, oprogramowania pośredniego i systemu operacyjnego. Analiza kontroli nad stosem aplikacji pomaga zrozumieć obowiązki stron zaangażowanych w zarządzanie aplikacją w chmurze obliczeniowej.



Rysunek 2: Zakres podziału odpowiedzialności pomiędzy dostawcą a odbiorcą usług chmur obliczeniowych

(Na podstawie NIST SP 500-292)

Warstwa aplikacji obejmuje aplikacje skierowane do użytkowników końcowych lub programów korzystających z usług chmur obliczeniowych. Aplikacje są:

- używane przez odbiorców usług typu SaaS[11] („oprogramowanie jako usługa")
- instalowane/zarządzane/obsługiwane przez odbiorców usług typu PaaS[12] („platforma aplikacyjna jako usługa"), odbiorców usług typu IaaS[13] („infrastruktura jako usługa") oraz dostawców usług typu SaaS.

Warstwa oprogramowania pośredniego zapewnia bloki konstrukcyjne oprogramowania (np. biblioteki, bazę danych i maszynę wirtualną) do wytwarzania oprogramowania w środowisku chmury obliczeniowej. Oprogramowanie pośrednie jest:

- używane przez odbiorców usług typu PaaS,
- instalowane/zarządzane/obsługiwane przez odbiorców usług typu IaaS lub dostawców usług typu PaaS i pozostaje niewidoczna dla użytkownika końcowego usług typu SaaS.

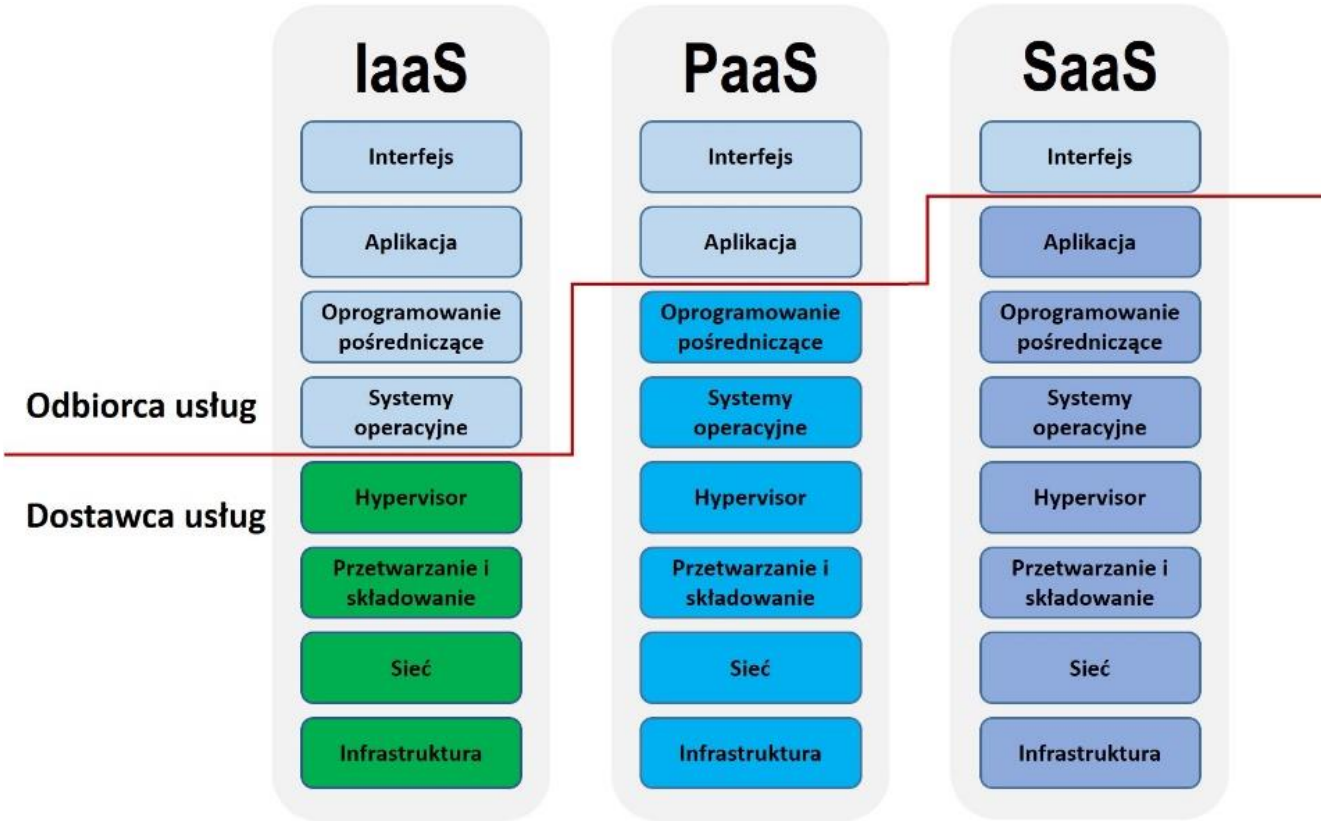
Warstwa systemu operacyjnego obejmuje system operacyjny oraz sterowniki i jest ukryta przed odbiorcami usług typu SaaS i PaaS. Usługa chmur obliczeniowych typu IaaS umożliwia uruchamianie wirtualizacji jednego lub wielu systemów operacyjnych na jednym hoście fizycznym. Zasadniczo odbiorcy usług chmur obliczeniowych mają dużą swobodę wyboru, który system operacyjny ma być hostowany spośród wszystkich systemów operacyjnych, które obsługiwane są przez danego dostawcę usług chmur obliczeniowych. Odbiorcy usług typu IaaS odpowiadają za utrzymanie, administrowanie i bezpieczeństwo systemu operacyjnego, a dostawca usługi typu IaaS odpowiada za utrzymanie, administrowanie i bezpieczeństwo system operacyjny środowiska hosta.

Modele usługowe chmur obliczeniowych definiowane są w ramach stosu SPI – Software, Platform, Infrastructure as a Platform, Infrastructure as a service. Pozwala on w uproszczony sposób zilustrować, jakie elementy usługi są dostarczane elementy usługi są dostarczane przez dostawcę, a za jakie elementy danego modelu usługowego odpowiada odbiorca usług odpowiada odbiorca usług chmur obliczeniowych. Ma to istotne znaczenie w zrozumieniu, jakie ryzyka są związane z jakie ryzyka są związane z poszczególnymi modelami oraz pomaga określić, kto jest odpowiedzialny za minimalizację tych odpowiedzialny za minimalizację tych ryzyk i zastosowanie odpowiednich zabezpieczeń.

Rysunek 3 przedstawia typowy układ stosu SPI.

Odbiorca usług chmur obliczeniowych musi rozumieć zakres swojej odpowiedzialności przy korzystaniu z usług i uwzględnić to w ocenie ryzyka i zakresie działań zabezpieczających

[11] ang. Software as a Service - SaaS
[12] ang. Platform as a Service - PaaS
[13] ang. Infrastructure as a Service - IaaS



Rysunek 3: Stos SPI

4.2 Wymagania bezpieczeństwa dla usług publicznych chmur obliczeniowych (PChO)

Bazując na definicji poziomów wymagań bezpieczeństwa SCCO przedstawionych w Rozdziale 3.2 stosowane są następujące zasady oceny usług świadczonych przez dostawców usług publicznych chmur obliczeniowych:

Poziom SCCO1: informacje na tym poziomie mogą być hostowane przez dostawcę usług publicznych chmur obliczeniowych. Odbiorca usług publicznych chmur obliczeniowych na poziomie SCCO1 odpowiada za sprawdzenie czy katalog usług danego dostawcy usług publicznych chmur obliczeniowych spełnia wymagania **podstawowych zabezpieczeń** dla **niskiego poziomu potencjalnego wpływu na bezpieczeństwo** zgodnie z Załącznikiem 5 do SCCO – bazującym na pełnym wykazie zabezpieczeń na podstawie NIST SP 800-53 Rev. 4.

***Poziom SCCO2*:** informacje na tym poziomie mogą być hostowane przez dostawcę usług publicznych chmur obliczeniowych, który deklaruje zgodność stosowanych **podstawowych zabezpieczeń** z wymaganiami na **umiarkowanym poziomie potencjalnego wpływu na bezpieczeństwo** zgodnie z Załącznikiem 5 do SCCO.

Deklaracja zgodności, dostarczana przez dostawcę usług chmurowych, powinna zawierać szczegółowe zestawienie stosowanych zabezpieczeń z ich odniesieniem do macierzy zabezpieczeń SCCO.

Pozytywna weryfikacja deklaracji zgodności przez Ministerstwo Cyfryzacji będzie podstawą do umieszczenia oferty usług chmur obliczeniowych danego dostawcy w katalogu usług publicznych chmur obliczeniowych PChO, dostępnym dla jednostek administracji publicznej.

Przy przetwarzaniu informacji na poziomie SCCO2 jednostki administracji publicznej nie mogą korzystać z ofert usług chmur obliczeniowych spoza katalogu usług publicznych chmur obliczeniowych PChO.

4.3 Wymagania bezpieczeństwa dla usług Rządowej Chmury Obliczeniowej (RChO)

***Poziom SCCO3*:** informacje na tym poziomie nie mogą być przetwarzane w ramach usług świadczonych przez dostawców usług publicznych chmur obliczeniowych i muszą być przetwarzane w ramach usług Rządowej Chmury Obliczeniowej RChO.

Usługi ujęte w katalogu usług RChO są dostarczane i obsługiwane przez operatora Rządowej Chmury Obliczeniowej. Usługi RChO są objęte takim samym zakresem podstawowych zabezpieczeń jak usługi dostawców publicznych chmur obliczeniowych, z dodatkowymi środkami ochrony wymaganymi na poziomie SCCO3, dotyczącymi w szczególności:

- zabezpieczeń organizacyjnych i technicznych dla Centrów Przetwarzania Danych przyłączonych do RChO,
- usług Rządowego Klastra Bezpieczeństwa,
- poświadczeń bezpieczeństwa dla personelu odpowiedzialnego za usługi świadczone w RChO.

5 Wymagania bezpieczeństwa

W tym rozdziale wskazane zostały wymagania bezpieczeństwa dotyczące korzystania z usług chmur obliczeniowych przez jednostki administracji publicznej.

5.1 Wymagania bezpieczeństwa przetwarzania informacji w chmurach obliczeniowych

Wymaga się, aby wszystkie systemy teleinformatyczne oraz informacje z jednostek administracji publicznej, które mają być przetwarzane z wykorzystaniem usług w modelu chmur obliczeniowych:

- zostały skategoryzowane zgodnie z załącznikiem 2 do Uchwały WIIP[14],
- sklasyfikowane pod kątem poziomu wymagań bezpieczeństwa SCCO, zgodnie z rozdziałem 3.2;

5.2 Jurysdykcja – uregulowania unijne dotyczące dostawców usług cyfrowych

Zgodnie z *Artykułem 18* dyrektywy UE 1148/2016[15]

1. Dostawca usług cyfrowych podlega jurysdykcji państwa członkowskiego, w którym posiada główną jednostkę organizacyjną. Uznaje się, że dostawca usług cyfrowych posiada główną jednostkę organizacyjną w państwie członkowskim, gdy ma siedzibę zarządu w tym państwie członkowskim.
2. Dostawca usług cyfrowych, który nie posiada jednostki organizacyjnej w Unii, ale oferuje usługi przetwarzania w chmurze w Unii, wyznacza przedstawiciela w Unii. Przedstawiciel musi posiadać jednostkę organizacyjną w jednym z tych państw członkowskich, w których oferowane są usługi. Uznaje się, że dostawca usług cyfrowych podlega jurysdykcji państwa członkowskiego, w którym przedstawiciel posiada jednostkę organizacyjną.

Zgodnie z załącznikiem 2 do Uchwały WIIP informacje administracji publicznej mogą być przetwarzane z wykorzystaniem usług w publicznych chmurach obliczeniowych znajdujących się w jurysdykcji polskiej (poziom SCCO2) lub w jurysdykcji państwa członkowskiego Unii Europejskiej (poziom SCCO1).

Dostawca usług przetwarzania w publicznych chmurach obliczeniowych umieszczanych przez Ministerstwo Cyfryzacji w katalogu usług PChO zobowiązany jest do przedstawienia listy wszystkich fizycznych lokalizacji centrów przetwarzania danych, w których dane mogą być przechowywane i przetwarzane.
Odnośnik do zabezpieczeń: SA-9 (Załącznik 5)

5.2.1 Wykorzystanie danych administracji publicznej przez dostawców usług publicznych chmur obliczeniowych

Wszystkie informacje/dane umieszczone lub utworzone przez administrację publiczną w chmurze dostawcy usług publicznych chmur obliczeniowych są własnością właściciela informacji, chyba, że została zawarta umowa z dostawcą usług, która stanowi inaczej. Dostawca usług publicznych chmur obliczeniowych nie ma żadnych praw do informacji / danych

[14] Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa" (Monitor Polski z dnia 24 września 2019 r. poz. 862).

[15] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. UE L 194/1 z 19.07.2016).

administracji publicznej. Informacje / dane obejmują także dzienniki i dane monitorowania utworzone przez aplikacje i systemy odbiorcy usług publicznych chmur obliczeniowych.

Dostawca usług publicznych chmur obliczeniowych nie może wykorzystywać informacji / danych odbiorców usług w żaden inny sposób aniżeli określony w umowie o świadczenie usług.

Dostawca usług publicznych chmur obliczeniowych zachowuje własność wszystkich dzienników i danych monitorowania związanych z wykorzystaniem i zarządzaniem świadczonymi usługami przetwarzania w publicznej chmurze obliczeniowej.

Dostawca usług publicznych chmur obliczeniowych nie może ujawniać danych odbiorców usług korzystających z jego oferty usług chmur obliczeniowych:

- organom państw, w których są przetwarzane dane tych odbiorców usług,
- organom państw sprawujących jurysdykcję nad dostawcą usług – o ile nie wynika to wprost z umowy zawartej pomiędzy odbiorcą i dostawcą usług.

Dostawca usług publicznych chmur obliczeniowych zobowiązany jest do niezwłocznego poinformowania odbiorcy usług o obowiązywaniu lub wprowadzeniu prawa uniemożliwiającego spełnienie powyższych warunków.
Odnośnik do zabezpieczeń: AC-23 (Załącznik 5)

5.3 Migracja i postępowanie z danymi po zaprzestaniu przetwarzania z wykorzystaniem usług w chmurze obliczeniowej

Niszczenie danych to zestaw działań, które mają miejsce, gdy jednostka administracji publicznej zaprzestanie korzystania z usług chmury obliczeniowej danego dostawcy. Proces przeniesienia jest wymagany, gdy Właściciel systemu migruje dane do innego dostawcy usług chmur obliczeniowych, wygasa umowa z dostawcą lub dostawca usług przestaje świadczyć usługi chmur obliczeniowych. Proces wyjścia z chmury jest podzielony na dwa etapy:

- pobieranie / migracja danych
- usuwanie lub zniszczenie danych.

Odbiorcy usług w chmurach obliczeniowych muszą przygotować się na ewentualne wycofanie usługi z oferty, a dostawcy usług zobowiązani są do niezwłocznego powiadomienia odbiorców usług o planowanym zaprzestaniu świadczenia usług chmur obliczeniowych.

5.4 Wycofanie z użycia, ponowne użycie i niszczenie nośników pamięci i sprzętu

Dostawca usług w chmurze obliczeniowej zobowiązany jest do upewnienia się, że nie pozostały żadne dane odbiorców usług na urządzeniach pamięci, które zostały wycofane z eksploatacji i zniszczone, ponownie wykorzystane w środowisku nieobjętym umową między dostawcą usług a odbiorcą usług lub przekazane osobom trzecim; zgodnie z wymaganiami zabezpieczeń MP-6 (Załącznik 5).

5.5 Kryptograficzna ochrona informacji

5.5.1 Polityka dotycząca stosowania procedur szyfrowania i zarządzania kluczami

Kryptograficzna ochrona informacji przetwarzanych z wykorzystaniem usług chmur obliczeniowych powinna uwzględniać następujące zasady i instrukcje stosowania organizacyjnych i technicznych zabezpieczeń:

- Korzystanie z silnych algorytmów szyfrowania (np. AES) i stosowanie najnowszych bezpiecznych protokołów sieciowych (np. TLS, IPsec, SSH):

- BSI TR-02102-2 Mechanizmy kryptograficzne: zalecenia i długości klucza część 2 - Korzystanie z Transport Layer Security (TLS)
- BSI TR-02102-3 Mechanizmy kryptograficzne: zalecenia i długości klucza Część 3 - Korzystanie z zabezpieczeń protokołu internetowego (IPSec) i Internet Key Exchange (IKEv2)
- BSI TR-02102-4 Mechanizmy kryptograficzne: zalecenia i długości klucza Część 4 - Korzystanie z bezpiecznej powłoki (SSH)

5.5.2 Szyfrowanie transmisji danych

Transmisja danych przetwarzanych w modelach chmur obliczeniowych powinna podlegać ochronie kryptograficznej polegającej na szyfrowaniu. Wymagania dotyczące mechanizmów kryptograficznych (algorytmów i długości kluczy) znajdują się w aktualizowanym okresowo dokumencie BSI TR-02102 Cryptographic Mechanisms[16].

Silne szyfrowanie transmisji realizowane jest obecnie z wykorzystaniem protokołu TLS 1.2 w połączeniu z Perfect Forward Secrecy.

5.5.3 Szyfrowanie wrażliwych danych na pamięci masowej

W celu przetwarzania i przechowywania wrażliwych informacji odbiorca usług chmur obliczeniowych powinien ustanowić procedury i wybrać techniczne zabezpieczenia do ich szyfrowania. Wyjątki dotyczą informacji, które nie mogą być zaszyfrowane w celu świadczenia usługi w chmurze obliczeniowej ze względów funkcjonalnych.

Klucze prywatne używane do szyfrowania powinny być znane tylko odbiorcy usług chmur obliczeniowych. Wyjątki (np. użycie klucza głównego przez dostawcę usług chmury obliczeniowej) opierają się na kontrolowanej procedurze i muszą być uzgodnione z odbiorcą usług chmury obliczeniowej.

5.5.4 Bezpieczne zarządzanie kluczami

Procedury i zabezpieczenia techniczne dla bezpiecznego zarządzania kluczami obejmują, co najmniej, następujące aspekty:

- generowanie kluczy dla różnych systemów kryptograficznych i aplikacji
- wydawanie i uzyskiwanie certyfikatów klucza publicznego
- obsługa i aktywacja kluczy dla odbiorców usług chmur obliczeniowych
- bezpieczne przechowywanie kluczy kryptograficznych
- wymiana lub aktualizacja kluczy kryptograficznych, w tym zasad określających, w jakich warunkach i w jaki sposób wymiana i / lub aktualizacja ma być realizowana
- wycofanie i usunięcie kluczy, na przykład w przypadku naruszenia bezpieczeństwa lub zmiany personelu
- przechowywanie kluczy odbiorców usług chmury publicznej poza środowiskiem dostawcy usług (np. u zaufanej strony trzeciej).

5.5.5 Szyfrowanie danych w chmurach obliczeniowych

Odbiorców usług w chmurach obliczeniowych muszą mieć możliwość szyfrowania informacji / danych podczas ich przechowywania i transmisji z zapewnieniem wyłącznej kontroli odbiorcy usług nad procesami generowania i zarządzania kluczami.

[16] https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/tr02102/index_htm.html

Dostawcy usług w chmurach obliczeniowych mogą oferować dedykowane sprzętowe kryptograficzne moduły bezpieczeństwa[17] lub oferować generowanie i zarządzanie kluczami kryptograficznymi, jako jedną z usług bezpieczeństwa.
Szyfrowanie informacji / danych przechowywanych w środowisku chmury obliczeniowej przy użyciu kluczy kontrolowanych i zarządzanych przez odbiorcę usługi daje następujące korzyści:

- chroni integralność publicznie udostępnianych informacji i zawartość stron internetowych na poziomie SCCO1, gdzie poufność zachowanie poufności nie jest głównym wymaganiem,
- chroni poufność i integralność na poziomie SCCO2 i SCCO3, dodatkowo:
  – ogranicza zagrożenia wewnętrzne związane z uzyskaniem nieuprawnionego dostępu przez pracowników dostawcy usług w chmurze obliczeniowej
  – ogranicza zagrożenia zewnętrzne związane z uzyskaniem nieuprawnionego dostępu przez zewnętrznych atakujących
  – umożliwia wysoce niezawodne zabezpieczenia dostępu do informacji przy konieczności migracji i/lub zakończenia korzystania z usług przetwarzania w chmurze obliczeniowej danego dostawcy bez konieczności udziału lub współpracy z tym dostawcą.

5.5.6 Kasowanie kryptograficzne

Kasowanie kryptograficzne jest techniką kasowania, która może być stosowana w niektórych sytuacjach, gdy dane przechowywane na nośniku są zaszyfrowane. W tym przypadku kasowanie nośników odbywa się poprzez kasowanie kluczy kryptograficznych używanych do szyfrowania danych, w przeciwieństwie do kasowania pamięci na nośnikach zawierających same zaszyfrowane dane. *[NIST SP 800-88]*

Szyfrowanie przechowywanych informacji, w połączeniu z wyłączną kontrolą odbiorcy usług w chmurze obliczeniowej nad zarządzaniem kluczami kryptograficznymi, zapewnia możliwość kryptograficznego usuwania danych w spoczynku bez pomocy i współpracy z dostawcą usług.

5.6 Kopia zapasowa

Dostawcy usług w chmurach obliczeniowych wykorzystywanych przez administrację publiczną są odpowiedzialni za tworzenie kopii zapasowych danych zgodnie z zabezpieczeniem CP-9 (Załącznik 5). Odbiorcy usług w chmurach obliczeniowych są również odpowiedzialni za zapewnienie kopii zapasowej ich danych zgodnie z zabezpieczeniem CP-9.

Dodatkowe kopie zapasowe przechowywane u więcej niż jednego dostawcy usług w chmurach obliczeniowych zmniejszają ryzyko utraty / uszkodzenia informacji / danych w przypadku zaprzestania działalności lub katastrofalnego zdarzenia, które wpływa na całą infrastrukturę dostawcy usług. Decyzja dotycząca liczby dodatkowych kopii zapasowych i miejsca ich przechowywania powinna być podejmowana na podstawie analizy ryzyka w ramach planowania awaryjnego wymaganego przez zabezpieczeniem CP-2.

UWAGA: W przypadku kopii zapasowych w usługach typu IaaS / PaaS kopie zapasowe obejmują konfiguracje maszyn wirtualnych lub obrazy w pełni skonfigurowanych maszyn wirtualnych, w tym ich wirtualnych dysków twardych, dzięki czemu odtworzenie bazy obliczeniowej i informacji jest łatwiejsze. Zabezpieczenia: CP-2, CP-9.

[17] ang. Hardware Security Module - HSM

6 Obsługa incydentów przy korzystaniu z usług w modelach chmur obliczeniowych

Wymagania dotyczące obsługi incydentów zostały zawarte w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa [uKSC].

Dostawcy usług w modelach chmur obliczeniowych są dostawcami usług cyfrowych i podlegają obowiązkom opisanym w rozdziale 4 uKSC (art. 17-20), w tym „podejmuje właściwe i proporcjonalne środki techniczne i organizacyjne określone w rozporządzeniu wykonawczym 2018/151 w celu zarządzania ryzykiem, na jakie narażone są systemy informacyjne wykorzystywane do świadczenia usługi cyfrowej. Środki te zapewniają cyberbezpieczeństwo odpowiednie do istniejącego ryzyka oraz uwzględniają:

1) bezpieczeństwo systemów informacyjnych i obiektów;
2) postępowanie w przypadku obsługi incydentu;
3) zarządzanie ciągłością działania dostawcy w celu świadczenia usługi cyfrowej;
4) monitorowanie, audyt i testowanie;
5) najnowszy stan wiedzy, w tym zgodność z normami międzynarodowymi, o których mowa w rozporządzeniu wykonawczym 2018/151.”

Podmiotami administracji publicznej będące odbiorcami usług w chmurach obliczeniowych będący podlegają obowiązkom określonym w rozdziale 5 uKSC (art. 21-25). Każdy podmiot publiczny realizujący zadanie publiczne zależne od systemu informacyjnego:

1) zapewnia zarządzanie incydentem w podmiocie publicznym;
2) zgłasza incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;
3) zapewnia obsługę incydentu w podmiocie publicznym i incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;
4) zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej;
5) przekazuje do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV dane osoby, o której mowa w art. 21, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

7 Załącznik 1 – Wykaz przepisów i norm związanych bezpieczeństwem przetwarzaniem informacji w modelach chmur obliczeniowych

[1] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005 nr 64 poz. 565).
[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000).
[3] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. 2004 nr 171 poz. 1800).
[4] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).
[5] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010 Nr 182 poz. 1228, t. jedn. Dz.U. 2019 poz. 742).
[6] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 Nr 89 poz. 590, t. jedn. Dz.U. 2019 poz.1398).
[7] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. 1994 Nr 24 poz. 83, t. jedn. Dz.U. 2019 poz. 1231).
[8] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. 2001 Nr 112 poz. 1198, t. jedn. Dz.U. 2019 poz. 1429).
[9] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002 nr 144 poz. 1204, t. jedn. Dz.U. 2019 poz. 123, 730).
[10] Ustawa z dnia 5 września 2016 o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 poz. 1579, t. jedn. Dz.U. 2019 poz.162, 1590).
[11] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012 poz.526, t. jedn. Dz.U. 2017 poz. 2247).
[12] Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa" (Monitor Polski z dnia 24 września 2019 r. poz. 862).
[13] Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–20 (Monitor Polski z dnia 30 października 2019 r. poz. 1037).
[14] Rozporządzenie Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników (Dz.U. 2016 poz.1627).
[15] Rozporządzenie Wykonawcze Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz.U. UE L 26 z 31.01.2018 s.48)
[16] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) (Dz.U. UE L 257/73 z 28.08.2014).
[17] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie (Dz.U. UE L 151/15 z 07.06.2019).
[18] Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.U. L 241/1 z 17.9.2015).
[19] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. UE L 194/1 z 19.07.2016).

Krajowe Ramy Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-1022 (Ministerstwo Cyfryzacji 2017).
Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej 2015 (BBN 22 stycznia 2015 r.).

NIST-US Government Cloud Computing Technology Roadmap Volume II [500-293]
NIST-US Government Cloud Computing Technology Roadmap Volume I [500-293]

NIST-Trusted Cloud Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (laaS) [1800-19B]
NIST-Trusted Cloud Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (laaS) [1800-19A]
NIST-Technical Guide to Information Security Tested and Assessment [800-115]
NIST-Security_Reference_Architecture_2013.05.15_v1.0 [500-299]
NIST-Security and Privacy Controls for Federal Information Systems and Organizations [800-53]
NIST-Risk Management Framework for Information Systems and Organizations [800-37]
NIST-Recommendation for the Triple Data Encryption Algorithm (TDEA) [800-67]
NIST-Mobile Device Security Cloud and Hybrid Builds Executive Summary How-to Guides [1800-4c]
NIST-Mobile Device Security Cloud and Hybrid Builds Executive Summary [1800-4a]
NIST-Mobile Device Security Cloud and Hybrid Builds Approach, Architecture, and Security Characteristics [1800-4b]
NIST-Mobile Device Security Cloud and Hybrid Builds [1800-4]
NIST-Managing Information Security Risk [800-39]
NIST-Identity and Access Management (IAM) [1800-2]
NIST-Guidelines on Security and Privacy i Public Cloud Computing [800-144]
NIST-Guidelines for Media Sanitization [800-88]
NIST-Guideline for Using Cryptographic Standards in the Federal Government-Directives, Mandates and Policies [800-175B]
NIST-Guideline for Using Cryptographic Standards in the Federal Government [800-175B]
NIST-Guide to Storage Encryption Technologies for End User Devices [800-111]
NIST-Guide to SSL VPNs [800-113]
NIST-Guide to Selecting Information Technology Security Products [800-36]
NIST-Guide to IPsec VPNs [800-77]
NIST-Guide for Security-Focused Configuration Management of Information Systems [SP 800-128]
NIST-Guide for Mapping Types of Information and Information Systems to Security Categories [800-60]
NIST-Definition of Cloud Computing [800-145]
NIST-Cybersecurity Framework Manufacturing Profile [NISTIR 8183]
NIST-Cybersecurity Framework [CSF]_rev. 1.1_2018.04.16
NIST-Contingency Planning Guide for Federal Information Systems [800-34]
NIST-Cloud Computing Synopsis and Recommendations [800-146]
NIST-Cloud Computing Standards Roadmap [500-291]
NIST-Cloud Computing Service Metrics Description [500-307]
NIST-Cloud Computing Reference Architecture [500-292]
NIST-Assessing Security and Privacy Controls in Federal Information Systems and Organizations [800-53A]
NIST-ABAC How-to Guides [1800-3C]
NIST-ABAC Executive Summary [1800-3A]

PN-ISO/IEC 15408-1:2016-10 Technika informatyczna – Techniki bezpieczeństwa – Kryteria oceny zabezpieczeń informatycznych – Część 1: Wprowadzenie i model ogólny.
PN-EN ISO 22301: 2014 - Systemy zarządzania ciągłością działania – Wymagania.
PN-EN ISO/IEC 27001: 2017 - Systemy zarządzania bezpieczeństwem informacji – Wymagania.
PN-EN ISO/IEC 27002: 2017 - Praktyczne zasady zabezpieczania informacji.
PN-ISO/IEC 27004: 2017 - Zarządzanie bezpieczeństwem – Monitorowanie, pomiary, analiza i ocena.
PN-ISO/IEC 27005: 2014 - Zarządzanie ryzykiem w bezpieczeństwie informacji.
PN-ISO/IEC 27017: 2017 - Praktyczne zasady zabezpieczenia informacji na podstawie ISO/IEC 27002 dla usług w chmurze.
PN-ISO/IEC 27018: 2017 - Praktyczne zasady ochrony danych identyfikujących osoby (PII) w chmurach publicznych działających jako przetwarzający PII.
PN-EN 50600 - seria norm dot. wyposażenia i infrastruktury centrów przetwarzania danych.
NCI – DCIS Cube Architecting Initiative.
CSA – Cloud Controls Matrix 3.01 (CSA CCM).

8 Załącznik 2 – Słownik pojęć

Nazwa	Skrót	Opis
Centrum Przetwarzania Danych	**CPD**	Z ang. **Data Center**. Serwerownia w zasobach administracji rządowej to obiekt budowlany wykorzystywany jako lokalizacja dla infrastruktury teleinformatycznej i związanych z nimi elementów, np.: systemów telekomunikacyjnych, zasobów przetwarzania. Ponadto, obejmuje nadmiarowe źródła zasilania, sieci teletransmisji, środki kontroli środowiska (np. klimatyzacja, systemy gaśnicze), urządzenia i systemy bezpieczeństwa oraz ochronę fizyczną obiektu.
Chmura hybrydowa		Z ang. **hybrid cloud**. Model wdrażania chmury obliczeniowej, w którym infrastruktura składa się z dwóch lub więcej odrębnych infrastruktur teleinformatycznych dostarczanych z chmury obliczeniowej (prywatnej, wspólnotowej lub publicznej), które pozostają odrębnymi jednostkami powiązanymi ze sobą znormalizowaną lub zastrzeżoną technologią, umożliwiającą przenoszenie danych i aplikacji między chmurami obliczeniowymi (np. w celu równoważenia obciążenia);
Przetwarzanie w chmurze obliczeniowej		ang. **cloud computing** to model przetwarzania umożliwiający powszechny i wygodny dostęp za pośrednictwem sieci do wspólnej puli konfigurowalnych zasobów przetwarzania (np. sieci, serwerów, pamięci masowych, aplikacji i usług), które mogą być szybko udostępniane przy minimalnym wysiłku ze strony zespołów zarządzania lub dostawcy usług. Chmura obliczeniowa poprzez **katalog usług** dostarcza usług w modelu chmurowym. Model chmurowy (model chmury obliczeniowej) składa się z pięciu zasadniczych cech (samoobsługi na żądanie, szerokiego dostępu do sieci, dynamicznego gromadzenia zasobów, szybkiego i elastycznego przydzielania i zwalniania zasobów, pomiarów i optymalizacji usług); trzech modeli usług (**SaaS**, **PaaS**, **IaaS**); oraz czterech modeli wdrażania usług (**chmura prywatna**, **chmura wspólnotowa, chmura publiczna**, chmura **hybrydowa**); kluczowe technologie wspomagające obejmują: szybkie i wydajne sieci rozległe, wydajne oraz relatywnie niedrogie serwery (uwzględniając ich liczbę) oraz wysokowydajną wirtualizację sprzętu; Cechą chmury obliczeniowej jest współdzielona odpowiedzialność pomiędzy dostawcę i odbiorcę usług chmurowych.
Chmura prywatna		ang. **private cloud**. Model wdrażania chmury obliczeniowej, w którym infrastruktura jest udostępniana do wyłącznego użytku przez jedną organizację obejmującą wielu **Odbiorców usług**, może być własnością organizacji, strony trzeciej lub ich kombinacji, bądź może być przez nie zarządzana i obsługiwana oraz zainstalowana w siedzibie tej organizacji lub poza nią.
Chmura publiczna		ang. **public cloud**. Model wdrażania chmury obliczeniowej, w którym infrastruktura jest udostępniana do użytku publicznego, może być własnością organizacji biznesowej, akademickiej lub rządowej lub ich kombinacji, bądź może być przez nie zarządzana i obsługiwana oraz jest zainstalowana w siedzibie dostawcy chmury.
Chmura wspólnotowa		Z ang. **community cloud.** Model wdrażania chmury obliczeniowej, w którym infrastruktura jest przeznaczona do wyłącznego użytku przez określoną grupę organizacji, mających wspólne założenia (m.in. misję, wymagania bezpieczeństwa, politykę, zgodność z regulacjami), może być własnością jednej lub więcej organizacji wchodzącej w skład grupy, strony trzeciej lub ich kombinacji, bądź może być przez nie zarządzana i obsługiwana i jest zainstalowana w siedzibie organizacji lub poza nią.

Nazwa	Skrót	Opis
Dostawca usługi w chmurze obliczeniowej		*(ang. Cloud Service Provider),* Podmiot, który oferuje/świadczy usługi w chmurze. Niekwalifikowane użycie terminu Dostawca usług odnosi się do dowolnego lub wszystkich dostawców usług w chmurze, Operator RChO lub innych niż Operator RChO.
Dostawca komercyjny		Komercyjny Dostawca usług: odnosi się do organizacji niebędących jednostkami administracji publicznej oferującej usługi w chmurze Odbiorca usługom publicznym i / lub rządowym w ramach przedsięwzięcia biznesowego, zwykle za opłatą z zamiarem osiągnięcia zysku. *[ang. Commercial-Cloud Service Provider]*
Dostawca usług cyfrowych	**DUC**	osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej mająca siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, świadcząca usługę cyfrową *[szczegółowa def. W Ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa]*
Elastyczność		Z ang. **rapid elasticity.** Usługi dostarczane z **chmury obliczeniowej** mogą być elastycznie konfigurowane i dostarczane, w niektórych przypadkach automatycznie, w celu szybkiego skalowania proporcjonalnie do popytu. Dla **Odbiorcy usług** udostępniane zasoby przetwarzania i usługi często wydają się być nieograniczone i mogą być przydzielane w dowolnej ilości i w dowolnym momencie.
Infrastruktura chmury		**Zasoby przetwarzania** stanowiące zbiór sprzętu i oprogramowania zgrupowanego w **pule zasobów**, który umożliwia pięć zasadniczych cech przetwarzania w chmurze (patrz **chmura obliczeniowa**) zawierające warstwę zarówno fizyczną (składającą się z zasobów sprzętowych, które są niezbędne do obsługi dostarczanych usług w chmurze obliczeniowej i zazwyczaj obejmują składniki serwera, pamięci masowej i sieci), jak i warstwę abstrakcji znajdującą się powyżej warstwy fizycznej (składającą się z oprogramowania rozmieszczonego w warstwie fizycznej, która posiada zasadnicze cechy chmury obliczeniowej);.
Infrastruktura jako usługa	**IaaS**	Z ang. **Infrastructure as a Service**. Usługa świadczona w **modelu chmurowym** zapewniająca **infrastrukturę chmury**, na której **Odbiorca usług** jest w stanie wdrożyć i uruchomić dowolne oprogramowanie (systemy operacyjne i aplikacje), nie zarządza ani nie kontroluje **infrastruktury chmury**, ale kontroluje systemy operacyjne, pamięć masową i wdrożone aplikacje oraz ewentualnie ma ograniczoną kontrolę nad wybranymi komponentami sieciowymi (np. zapór sieciowych).
Interoperacyjność		Zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy przez wspierane przez nie procesy biznesowe realizowane za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych.
Katalog usług		*(ang. Cloud Service Offering, CSO),* Lista predefiniowanych i ustandaryzowanych usług infrastruktury informatycznej typu **IaaS**, **SaaS**, **PaaS** itd. (dla RChO zabezpieczona usługami bezpieczeństwa dostępnymi w ramach **RKB)** prezentowana poprzez portal WWW umożliwiająca samodzielne ich wykorzystanie przez **Odbiorcę usług**.
Kategoria Bezpieczeństwa	**SC**	*(ang. Security Category),* Charakterystyka informacji/danych lub systemu informatycznego oparta na ocenie potencjalnego

Nazwa	Skrót	Opis
		wpływu utraty poufności, integralności lub dostępności takich informacji/danych lub systemu informatycznego na działania statutowe administracji publicznej, zasoby organizacyjne, osoby fizyczne, inne organizacje oraz bezpieczeństwo państwa.
Model chmury obliczeniowej		Model proaktywnego świadczenia usług informatycznych. W tym modelu **infrastruktura chmury** dostarczana jest do użytkowników, jako ustandaryzowana i prekonfigurowana usługa wymagająca od nich tylko niewielkiej, finalnej konfiguracji. Usługi dostępne są z **katalogu usług** w modelu samoobsługowym (patrz **self-service**) i rozliczane za ich użycie. Użytkownik nie kupuje infrastruktury informatycznej tylko ją użytkuje. Po stronie dostawcy usług pozostaje kwestia utrzymania określonego SLA, wydajności, dostępności oraz zabezpieczenia na wypadek awarii.
Model samoobsługowy	**Self-service**	Samoobsługa na żądanie. **Odbiorca usług** może samodzielnie użyć zasobów chmury, przygotowanych do automatycznej konfiguracji przez użytkownika, bez konieczności interakcji z obsługą techniczną dostawcy usług.
Network Operation Center	**NOC**	Centrum Zarzadzania Siecią. Dedykowany zespół specjalistów świadczący usługi zarządzania siecią **RChO**.
Szacowanie ryzyka		Proces identyfikowania zagrożeń dla operacji organizacyjnych (w tym działań statutowych, funkcji, wizerunku, reputacji), zasobów organizacyjnych, osób, innych organizacji i Narodu, wynikających z działania systemu *[NIST SP 800-30 risk assessment]*.
Odbiorca usług w chmurze obliczeniowej		1. Podmioty sektora finansów publicznych, o których mowa w art. 9 ust. 1-13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2019 r. poz. 869); 2. inne państwowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, banków i spółek prawa handlowego; 3. inne, niż określone w ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych, państwowe jednostki organizacyjne nieposiadające osobowości prawnej. Dotyczy podmiotów 1-3, które podpisały umowy o świadczenie usług **RChO**. Może wykorzystywać jeden lub wiele tenantów na potrzeby budowy systemów informatycznych.
Mitygacja ryzyka		Ustalanie priorytetów, ocena i wdrażanie odpowiednich zabezpieczeń / środków zaradczych zmniejszających ryzyko zalecanych w procesie zarządzania ryzykiem.
Operator RKB		Minister właściwy do spraw informatyzacji pełniący rolę Operatora Rządowego Klastra Bezpieczeństwa.
Oprogramowanie jako usługa	**SaaS**	Z ang. **Software as a Service**. Usługa świadczona w **modelu chmurowym** umożliwiająca **Odbiorcy usług** wykorzystanie aplikacji uruchomionej na **infrastrukturze chmury** dostarczanej przez dostawcę usług, dostępnej na różnych urządzeniach klienckich za pośrednictwem cienkiego Odbiorcy usługi np.: przeglądarka internetowa lub Odbiorca usług aplikacji, oraz w przypadku której **Odbiorca usług** nie zarządza ani nie kontroluje **infrastruktury chmury**, a nawet parametrów konfiguracyjnych aplikacji, z wyjątkiem ograniczonych ustawień konfiguracji aplikacji specyficznych dla użytkownika.
Platforma jako usługa	**PaaS**	Z ang. **Platform as a Service**. Usługa świadczona w **modelu chmurowym** umożliwiająca **Odbiorcy usług** wdrożenie na **infrastrukturze chmury** aplikacji stworzonych przez siebie lub nabytych, które zostały przygotowane przy użyciu języków programowania, bibliotek, usług i narzędzi obsługiwanych

Nazwa	Skrót	Opis
		przez dostawcę w przypadku której **Odbiorca usług** nie zarządza ani nie kontroluje **infrastruktury chmury** oraz systemów operacyjnych i baz danych, ale ma kontrolę nad wdrożonymi aplikacjami i, ewentualnie, nad ustawieniami konfiguracji dla środowiska udostępniania aplikacji.
Prawo zamówień publicznych	**PZP**	Przepisy wynikające z Ustawy Prawo zamówień publicznych z dnia 29 stycznia 2004 r. z późniejszymi zmianami.
Publiczna Chmura Obliczeniowa	**PChO**	Chmura obliczeniowa dostępna w modelu **chmury publicznej** świadczona przez dostawców, spełniająca w szczególności wymagania w zakresie poufności, integralności i dostępności zdefiniowanych pod kątem zapewnienia bezpieczeństwa informacji administracji publicznej. Dostarcza usług infrastruktury informatycznej poprzez predefiniowany **Katalog usług** PChO.
Ramy Zarządzania Ryzykiem	**RMF**	(ang. Risk Management Framework) Ramy Zarządzania Ryzykiem to sześciostopniowe, oparte na ryzyku podejście do bezpieczeństwa systemu informatycznego, którego celem jest zgodność z różnymi przepisami publicznymi. RMF zastępuje tradycyjne procesy certyfikacji i akredytacji C&A (NIST SP 800-37).
Rejestr państwowy		Ewidencja, wykaz, lista, spis albo inna forma ewidencji, służąca do realizacji zadań publicznych, prowadzona przez podmiot publiczny na podstawie odrębnych przepisów ustawowych np.: PESEL, CEiDG, SRP, CEPIK.
Rozliczanie usług		System zarzadzania **chmury obliczeniowej** automatycznie kontrolują i optymalizują wykorzystanie **zasobów przetwarzania**. Poprzez systemy pomiarowe kolekcjonują dane o ich wykorzystaniu w podziale na rodzaj (np.: przechowywanie, przetwarzanie, przepustowość i aktywne konta użytkowników). Wykorzystanie zasobów jest monitorowane, kontrolowane i raportowane, zapewniając przejrzystość rozliczenia zarówno dostawcy usług, jak i **Odbiorcy usług**. Rozliczenie wykorzystanej usługi może nastąpić na podstawie np.: płatności za użycie z ang. pay-per-use.
Rządowa Chmura Obliczeniowa	**RChO**	Chmura obliczeniowa typu **chmura wspólnotowa** dedykowana jednostkom administracji publicznej budowana w oparciu o **zasoby przetwarzania** oraz infrastrukturę teleinformatyczną, która pozostaje w dyspozycji podmiotów administracji publicznej, dostępna z **katalogu usług**. W jej skład wchodzą **ISR**, **IDR** i **RKB**.
Rządowy Klaster Bezpieczeństwa	**RKB**	Usługi bezpieczeństwa oraz środki techniczne stosowane do zabezpieczenie **RChO** będące implementacją wymagań **SCCO**.
Security Operation Center	**SOC**	Operacyjne Centrum Bezpieczeństwa. Centrum zarządzania bezpieczeństwem i obsługi incydentów. Dedykowany zespół specjalistów świadczący usługi zarządzania bezpieczeństwem i obsługą incydentów **RChO**.
Sieci rządowe		Sieci teletransmisyjne umożliwiające wymianę komunikacji pomiędzy publicznymi podmiotami krajowymi (GovNet), Unii Europejskiej oraz NATO (TESTA-NG), pozostające w gestii Ministra właściwego do spraw wewnętrznych oraz jednostek przez niego nadzorowanych.
Standardy Cyberbezpieczeństwa Chmury Obliczeniowej	**SCCO**	Zbiór wymagań prawnych, organizacyjnych i technicznych zapewniających cyberbezpieczeństwo w modelach wdrażania chmur obliczeniowych opracowany w oparciu o normy, standardy i metodyki uznane w obrocie profesjonalnym oraz w oparciu o rekomendacje Pełnomocnika rządu ds. cyberbezpieczeństwa.

Nazwa	Skrót	Opis
Systemy Rejestrów Państwowych	**SRP**	System informatyczny łączący najważniejsze polskie rejestry. Dzięki połączeniu rejestrów można załatwiać wybrane sprawy urzędowe, nie wychodząc z domu. System łączy pięć rejestrów: PESEL, Rejestr Dowodów Osobistych, Rejestr Stanu Cywilnego, System Odznaczeń Państwowych, Centralny Rejestr Sprzeciwów. W dniu 1 marca 2015 r. weszły w życie 3 ustawy regulujące nowy sposób prowadzenia ewidencji ludności, wydawania dowodów osobistych oraz rejestracji stanu cywilnego, tj. ustawa o ewidencji ludności, ustawa o dowodach osobistych oraz Prawo o aktach stanu cywilnego. Ta ostatnia po raz pierwszy wprowadziła elektroniczny sposób prowadzenia rejestracji stanu cywilnego.
System Zapewnienia Usług Chmurowych	**ZUCH, System ZUCH**	System informatyczny pozwalający na klasyfikację systemu informatycznego administracji publicznej, wybór oraz zakup usług **PChO**, zgodnie z przepisami **PZP**.
Tenant		Architektura **chmury obliczeniowej** jest zbudowana w oparciu o tenanty (z ang. multi-tenant), które współdzielą **infrastrukturę chmury**. Każdy tenant to logicznie izolowana część **infrastruktury chmury** dedykowana do wyłącznego wykorzystania przez pojedynczego **Odbiorcę usług** i niedostępna dla innych **Odbiorców usług**. Tenant zawiera wszystkie usługi z **katalogu usług** wykorzystywane przez **Odbiorcę usług** wraz z ich konfiguracją oraz dane. Dostęp do tenantu jest możliwy dla uprawnionych użytkowników.
Wspólna Infrastruktura Informatyczna Państwa	**WIIP**	Definicja obejmuje 2 znaczenia. (1) **Projekt WIIP** obejmuje dostarczanie infrastruktury informatycznej, jako usługi w modelu chmury obliczeniowej oraz zapewnienie bezpieczeństwa systemów teleinformatycznych tam uruchomionych poprzez budowę **RKB, RChO** i **PChO oraz udostępnienie Systemu ZUCH**. Celem projektu jest inicjalne dostarczenie **infrastruktury chmury** na potrzeby budowy **RChO,** udostępnienie **katalogu usług** oraz osiągnięcie odpowiedniego poziomu gotowości organizacyjnej. (2) **Inicjatywa WIIP** (program WIIP) jest przedsięwzięciem szerszym, wykraczającym poza ramy projektu WIIP planowanego na lata 2019-2021.
Współdzielona odpowiedzialność		Z ang. **Shared Responsibility Model** - model bezpieczeństwa funkcjonowania **chmury obliczeniowej** opisujący ustalenia dotyczące odpowiedzialności dostawcy „Bezpieczeństwo chmury" i odpowiedzialności Odbiorca usługa „Bezpieczeństwo w chmurze" w zakresie infrastruktury teleinformatycznej, środowiska przetwarzania, przetwarzania danych oraz usług.
Zarządzanie ryzykiem		Program i procesy wspierające zarządzanie ryzykiem związanym z działaniami instytucji (w tym działaniami statutowymi, funkcjami, wizerunkiem, reputacją), aktywami instytucji, osobami fizycznymi, innymi organizacjami i narodem, obejmują: ustanowienie kontekstu dla działań związanych z ryzykiem; ocenę ryzyka; reagowanie na ryzyko raz określone; i monitorowanie ryzyka w czasie. *[NIST SP 800-37: risk management]*.
Zintegrowana Infrastruktura Rejestrów	**ZIR**	**Infrastruktura chmury** dedykowana do obsługi systemów teleinformatycznych administracji publicznej, które mają kluczowe znaczenie dla realizacji zadań państwa o fundamentalnym znaczeniu budowana w ramach realizacji projektu **WIIP**. ZIR obsługuje **Rejestry Państwowe** dostępne z sieci wydzielonych i sieci o wysokim poziomie zaufania np. dedykowanych dla poszczególnych instytucji lub dedykowanej

Nazwa	Skrót	Opis
		sieci. Ta część infrastruktury jest galwanicznie izolowana od **ISR**.

9 Załącznik 3 – Skróty

CSP	Cloud Service Provider (def. Dostawca usług)
DUC	Dostawca usług cyfrowych
IPsec	Internet Protocol Security
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
NIST	National Institute of Standards and Technology
RMF	Risk Management Framework (def. Ramy Zarządzania Ryzykiem)
SC	Security Category (def. Kategoria Bezpieczeństwa)
SP	Special Publication
VPN	Virtual Private Network

10 Załącznik 4 – Podstawowe Wymagania Bezpieczeństwa – Macierz zabezpieczeń

W osobnym pliku

11 Załącznik 5 – Katalog zabezpieczeń

W osobnym pliku