Jarosław Wilk

Comparex Poland Sp. z o.o.

Wydział Cybernetyki
Wojskowa Akademia Techniczna w Warszawie

Leopold Żurek

Wydział Zarządzania
Wyższa Szkoła Ekonomiczno-Humanistyczna w Skierniewicach

Mechanizmy sterowania bezpieczeństwem informacyjnym w modelu usługowym infrastruktury informacyjnej państwa

1. Wstęp

Zgodnie z założeniami *Programu Zintegrowanej Informatyzacji Państwa*[1], infrastruktura informacyjna państwa polskiego powinna zostać przebudowana na podstawie modelu usługowego. Ten strategiczny dokument wskazuje „działania rządu zmierzające do dostarczenia społeczeństwu wysokiej jakości elektronicznych usług publicznych. Celem Programu jest stworzenie spójnego, logicznego i sprawnego systemu informacyjnego państwa, dostarczającego e-usługi na poziomie krajowym i europejskim, w sposób efektywny pod względem jakości i kosztów. Program zapewni współpracę istniejących oraz nowych systemów teleinformatycznych administracji publicznej, eliminując jednocześnie powielające się dotychczas funkcjonalności”[2].

Systemy informacyjne budowane zgodnie z modelem usługowym mają wiele zalet, jednak wiążą się z nim nowe wyzwania. Jednym z nich, które zostało omówione w niniejszym artykule, jest zagadnienie bezpieczeństwa. Ochrona złożonych usług elektronicznych, które stały się fasadą dostępu do danych dla użytkowników, jest trudna lub wręcz niemożliwa przy wykorzystaniu dostępnych do tej pory modeli sterowania

[1] *Program Zintegrowanej Informatyzacji Państwa*, Ministerstwo Administracji i Cyfryzacji, Warszawa, listopad 2013.

[2] Ibidem, s. 4.

bezpieczeństwem. Dodatkowym utrudnieniem jest fakt, iż coraz częściej są wykorzystywane usługi złożone powstałe w wyniku łączenia wielu systemów, np. przez cyfrowe platformy integracyjne.

W artykule omówiono autorski model sterowania bezpieczeństwem dla systemów administracji publicznej zbudowanych zgodnie z modelem usługowym. Kluczowym jego elementem jest matematyczny model systemu składającego się z usług elektronicznych i danych, na których są wykonywane operacje elementarne.

2. Model usługowy infrastruktury informacyjnej państwa

Usługowy model systemu informacyjnego można opisać, bazując na definicjach architektury SOA (ang. *service oriented architecture* – architektura zorientowana na usługi). Poniżej zostały przytoczone dwie z nich opisujące model architektury zorientowanej na usługi jako:

- „Paradygmat organizacji i wykorzystania rozproszonych usług (możliwości), które mogą być pod kontrolą różnych domen. Zapewnia jednolite środki do oferowania, wyszukiwania, współpracy i wykorzystania usług (możliwości) tak, aby osiągać pożądane efekty zgodne z mierzalnymi uwarunkowaniami i oczekiwaniami”[3].
- „Lekkie środowisko umożliwiające dynamiczne odkrywanie i korzystanie z usług w sieci. Najważniejszą cechą architektury zorientowanej na usługi jest oddzielenie implementacji usługi od jej interfejsu”[4].

„SOA wnosi przede wszystkim takie własności niefunkcjonalne jak: ponowne użycie elementów oprogramowania, enkapsulację funkcjonalności, precyzyjną definicję interfejsów oraz elastyczność aplikacji tworzonych na drodze kompozycji”[5]. Podstawową cechą w kontekście nowego modelu, która wyróżnia podejście usługowe w stosunku do uprzednio stosowanych rodzajów architektury, jest „zapewnienie enkapsulacji funkcjonalności”[6]. W rozpatrywanych dotychczas modelach bezpieczeństwa najczęściej stosowanym podejściem był dostęp użytkownika bezpośrednio do danych za pomocą określonych operacji elementarnych, np. zapis, odczyt. W modelu architektury usługowej

---

[3] *Reference Model for Service Oriented Architecture 1.0*, Committee Specification 1, Oasis Open, 2006, s. 8–7.

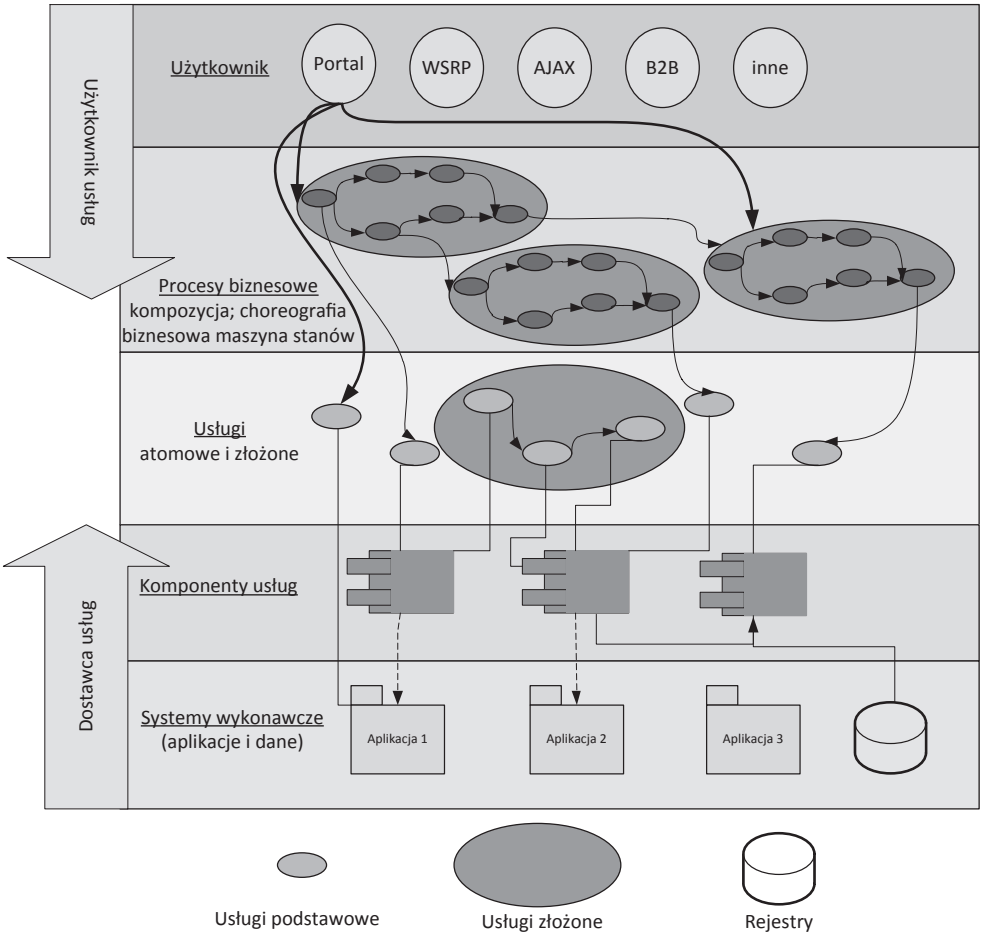
[4] J. Mc Govern, S. Tyagi, M. Stevens, M. Sunil, *Java Web Services Architecture*, Morgan Kaufmann Publishers, San Francisco 2003 (rozdział 2: *Service Oriented Architecture*), s. 24.

[5] D. Radziszowski, K. Zieliński, *Nowe technologie informacyjne dla elektronicznej gospodarki i społeczeństwa informacyjnego oparte na paradygmacie SOA*, Katedra Informatyki AGH, Kraków 2011, s. 1.

[6] G. Bieber, J. Carpenter, *Introduction to Service-Oriented Programming (Rev 2.1)*, 2011, s. 6.

pomiędzy użytkownikiem a jednostkami danych musi występować usługa elektroniczna, która za pomocą wbudowanego w nią programu przetwarza dane i przekazuje je do użytkownika. Przetwarzanie danych może być prostym mechanizmem przekazania ich w uzgodnionej formie za pomocą zdefiniowanego interfejsu lub polegać np. na ich obróbce statystycznej lub połączeniu z innymi danymi.

Dodatkowo enkapsulacja funkcjonalności i modułowość przejawiają się w udostępnianiu użytkownikowi usług (opisywanych dalej jako złożone) składających się z innych usług (opisywanych dalej jako atomowe lub proste). Schemat takiej architektury został przedstawiony na rysunku 1.



Rysunek 1. Architektura referencyjna SOA

Źródło: M.H. Dodani, *SOA 2006: State of the Art*, „Journal of Object Technology" 2006, vol. 2, s. 44.

Omówiony model usługowy został wskazany przez Ministerstwo Administracji i Cyfryzacji jako wzorcowe podejście do informatyzacji państwa: „Celem MAC jest dążenie do tego, by administracja była sprawna, przez co rozumiemy administrację jako sieć instytucji powiązanych Systemem Informacyjnym Państwa, wspierających obywatela w sposób dla niego »niewidoczny«. Sprawne państwo oznacza, że instytucje administracji publicznej i sektora usług publicznych oferują niezbędne usługi o jak najlepszej jakości, efektywnie, z wykorzystaniem nowoczesnych technologii informacyjnych i działają w oparciu o ideę otwartego rządu”[7]. Państwo w miarę możliwości ma udostępniać usługi złożone, które „zostaną wytworzone dzięki zapewnieniu współdziałania (tzw. interoperacyjności) różnych systemów”[8].

Podstawą złożonych usług publicznych jest bezpieczna wymiana danych i sterowanie bezpieczną komunikacją, szerzej opisane w innym artykule J. Wilka[9]. W *Programie Zintegrowanej Informatyzacji Państwa* również podkreśla się wagę bezpieczeństwa w całym procesie informatyzacji, wskazując jako jedno z zadań średniookresowych „opracowanie reużywalnej metodyki oraz wzorcowej dokumentacji systemów zarządzania bezpieczeństwem informacji wraz z dokumentacją i udostępnienie tych systemów podmiotom publicznym prowadzącym rejestry publiczne. Zakłada się przy tym wykorzystanie doświadczeń instytucji posiadających certyfikowane systemy zarządzania bezpieczeństwem informacji”[10].

3. Podstawowe pojęcia modelu usługowego

Poniżej zostały opisane podstawowe pojęcia dla systemu informacyjnego administracji państwowej zbudowanego zgodnie z modelem usługowym.

3.1. Usługa elektroniczna

e_l jest to najmniejszy rozpatrywany zasób wykonywalny, który przetwarza (korzystając ze składających się na usługę algorytmów) dane z jednostek danych. Algorytmy

---

7 M. Boni et al., *Państwo 2.0. Nowy start dla e-administracji*, Ministerstwo Administracji i Cyfryzacji, Warszawa 2012, s. 1.

8 *Program…*, op.cit., s. 7.

9 J. Wilk, *Wykorzystanie teorii krat w modelowaniu procesów zarządzania bezpieczeństwem w platformach usług elektronicznych administracji publicznej*, „Roczniki” Kolegium Analiz Ekonomicznych, z. 33, Oficyna Wydawnicza SGH, Warszawa 2014, s. 5.

10 *Program…*, op.cit., s. 59.

składające się na usługę elektroniczną z założenia są z nią związane na stałe i nie będą szczegółowo rozpatrywane. W przypadku występowania różnych kombinacji algorytmów powstają różne usługi elektroniczne.

$$E = \{e_1, e_2, \ldots, e_l, \ldots, e_L\} \text{ zbiór publicznych usług elektronicznych.} \quad (1)$$

3.2. Podmiot

p_r jest to usługobiorca korzystający z usług elektronicznych. Podmiotami są obywatele, urzędnicy lub jednostki publiczne różnych szczebli.

$$P = \{p_1, p_2, \ldots, p_r, \ldots, p_R\} \text{ zbiór podmiotów.} \quad (2)$$

Usługa elektroniczna uruchamiana jest przez wymuszenie w_n wyzwalane przez podmiot lub inną usługę elektroniczną.

$$W = \{w_1, w_2, \ldots, w_n, \ldots, w_N\} \text{ zbiór wymuszeń.} \quad (3)$$

Wymuszenie uruchamia jedną usługę elektroniczną i może uruchomić zbiór kolejnych wymuszeń z danej usługi – funkcja g.

$$g : W \to E \times 2^W . \quad (4)$$

Usługa elektroniczna uruchamia zbiór operacji T na jednostkach danych D – funkcja h.

$$h : E \to 2^{T \times D} . \quad (5)$$

3.3. Jednostka danych

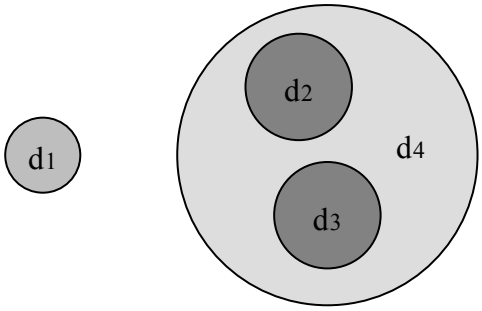
d_i jest to rozpatrywany obiekt informacyjny służący do przechowywania danych, np. plik, rekord bazy danych, tabela, baza danych, parametr funkcji.

$$D = \{d_1, d_2, \ldots, d_i, \ldots, d_I\} \text{ – zbiór jednostek danych.} \quad (6)$$

Granulacja jednostek danych zależy od poziomu, na jakim rozpatrywane są uprawnienia dostępu dla konkretnego systemu, i może być różna dla poszczególnych jednostek w ramach zbioru D. Pokazuje to poniższy schemat (rysunek 2), na którym dla

przykładowego systemu są rozpatrywane następujące jednostki danych (w kontekście uprawnień dostępu):

- d_1 – plik funkcji przykład_pliku_1;
- d_2 – tabela przykład_tabeli_1;
- d_3 – tabela przykład_tabeli_2;
- d_4 – baza danych przykład_bazy_danych_1.



Rysunek 2. Przykład granulacji jednostek danych $\mathbf{d}_i$

Źródło: opracowanie własne.

Baza danych d_4 może zawierać więcej tabel niż d_2 i d_3, ale mogą one nie być istotne w kontekście bezpieczeństwa danego systemu. Granulacja uprawnień dla omawianego przykładowego systemu pozwala na ich przypisanie do pliku, dwóch tabel i całej bazy danych.

3.4. Zbiór operacji

T składa się z operacji elementarnych realizowanych na jednostkach danych d_i. Są to operacje uniwersalne i ich zbiór można określić dla każdego systemu. Przykładem takiego zbioru są operacje: zapisz, odczytaj, wyszukaj, usuń, modyfikuj.

$$T = \{t_1, t_2, \ldots, t_m, \ldots, t_M\} \text{ zbiór operacji.} \tag{7}$$

Operacja może dotyczyć bezpośrednio jednostki danych najniższego poziomu, np. operacja „odczytaj" dla pliku, lub jednostki danych będącej obiektem wyższego poziomu, np. operacja „odczytaj" dla bazy danych określająca odczyt z dowolnej tabeli, dowolnego rekordu konkretnej bazy danych.

$$f : T \times D \to D \text{ funkcja działania operacji na jednostkach danych.} \tag{8}$$

W wyniku wykonania operacji t_m na jednostce danych d_i następuje zmiana jej stanu s_j. Zmiana stanu może mieć wymiar fizyczny (np. w wyniku operacji „zapisz" w jednostce danych d_i znajduje się nowa wartość) i formalny (np. w wyniku operacji „czytaj" nadal w jednostce danych d_i znajduje się ta sama wartość, ale już w stanie odczytanym).

$$S = \left\{s_1, s_2, \ldots, s_j, \ldots, s_J\right\} \text{ zbiór wszystkich stanów.} \tag{9}$$

$$gst : D \rightarrow 2^S \text{ generator stanów.} \tag{10}$$

$$gst\left(d_i\right) = S_i \quad dla\ d_i \in D\ gdzie\ S_i \subset S;\ S_i \neq \varnothing. \tag{11}$$

Stan całego systemu jest dowolnym podzbiorem stanów wszystkich jednostek danych tego systemu.

$$S_{system} = S_1 \times S_2 \times \ldots \times S_i \times \ldots \times S_I \text{ stan całego systemu.} \tag{12}$$

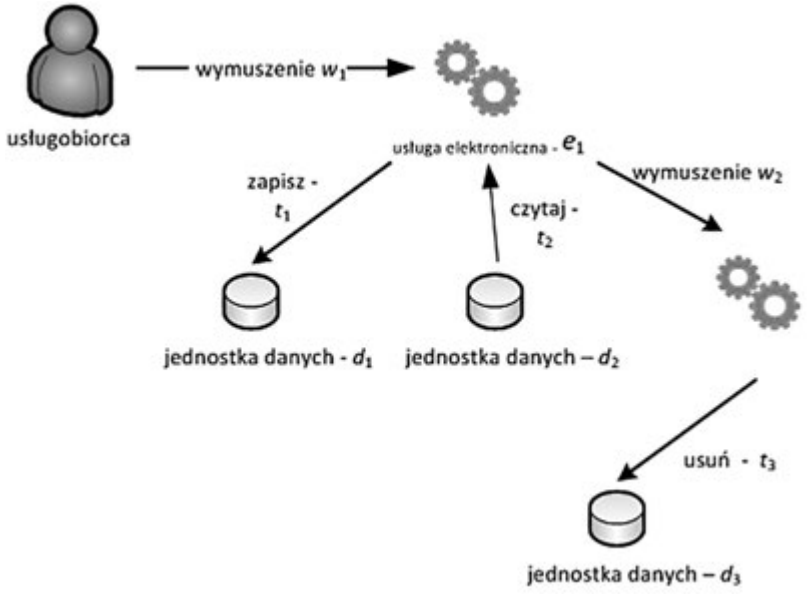
Weryfikacja tego, czy system jest bezpieczny, jest możliwa do wykonania za pomocą dwóch sposobów:

a) kontroli stanu systemu po jego każdej zmianie; jest to nierealne do wdrożenia w rzeczywistych systemach, gdyż wymagałoby przygotowania wszystkich kombinacji stanów wraz z opisem, czy jest ona dopuszczalna, czy niedopuszczalna w kontekście zachowania bezpieczeństwa;
b) opracowania zbioru funkcji sprawdzających, czy operacje, które prowadzą w konsekwencji do zmiany stanu, są dopuszczalne; rozwiązanie realnie stosowane w rzeczywistych systemach.

W omawianym modelu przejęto drugie podejście (b), zakładając, że dopuszczalna w kontekście zachowania bezpieczeństwa operacja przeniesie system do stanu dopuszczalnego. Pozwala to na stosowanie modelu do rzeczywistych systemów administracji państwowej (już istniejących i projektowanych) i upraszcza go o element stanów, które nie muszą być już dalej rozpatrywane.

Schemat poniżej (rysunek 3) przedstawia przykład publicznej usługi złożonej (składającej się z dwóch usług atomowych) opisanej zgodnie z omówionym modelem. Problemów z opisaniem bezpieczeństwa usługi przedstawionej na rysunku 3 nie ma w przypadku statycznych (zdefiniowanych przy tworzeniu systemu i niezmieniających się) usług elektronicznych składających się ze wszystkich elementów (innych usług, jednostek danych i operacji) pochodzących z tego samego systemu. Wystarczy zdefiniować np. macierz uprawnień (z modelu Lampsona) użytkowników do złożonych

usług elektronicznych i na jej podstawie zezwalać lub nie zezwalać na ich uruchamianie. Problem z wykorzystaniem obecnie dostępnych modeli pojawia się w przypadku dynamicznie tworzonych i zmieniających się usług złożonych, które powstają w wyniku integracji wielu różnych systemów (usług elektronicznych, jednostek danych, operacji). W takim przypadku konieczna staje się analiza uprawnień na niższym poziomie, tzn. składających się na usługę elektroniczną elementów.



Rysunek 3. Przykład publicznej złożonej usługi elektronicznej

Źródło: opracowanie własne.

4. Mechanizmy sterowania bezpieczeństwem

Zaproponowany mechanizm sterowania bezpieczeństwem informacyjnym dla systemów usługowych infrastruktury informacyjnej państwa składa się z dwóch modeli sterowania:

- dostępem do danych (*access management* – AM);
- wykonywaniem usług elektronicznych (*execution management* – EM).

Jednostki danych *D* są opisane za pomocą klas ochrony danych ze zbioru *K*, np. jawne, poufne, tajne, ściśle tajne. Usługi elektroniczne *E* są opisane za pomocą kategorii uprawnień uruchamiania usług ze zbioru *B*, np. powszechne, specjalistyczne, zastrzeżone.

Każdy podmiot p_r ze zbioru *P* ma następujące parametry określające jego poziom dostępu:

- klasę ochrony ze zbioru *K*, np. poufne;
- zakres dopuszczalnych operacji z zbioru *T*, np. odczyt;
- kategorię uprawnienia uruchamiania usług ze zbioru *B*, np. specjalistyczne.

Model AM określa dozwolone dla podmiotu (*B*) operacje dostępu (*T*) do jednostek danych (*D*) na podstawie klasy ochrony i zakresu dopuszczalnych operacji.

$$AM = \langle P,\ D, K,\ T, \rho, \tau, HF \rangle, \tag{13}$$

gdzie:
P – zbiór podmiotów,
D – zbiór jednostek danych,
K – zbiór klas ochrony,
T – zbiór operacji,
ρ – relacja dostępu,
τ – relacja zakresu działania operacji,
HF – zbiór funkcji modelu, generator ograniczenia integralności modelu sterowania dostępem.

Relacja dostępu jest zbudowana na parach klas ochrony $\rho \subset K \times K$ i określa dozwoloną hierarchię dostępów do danych, np. ściśle tajne > tajne > poufne > jawne. Relacja zakresu działania operacji jest zbudowana na parach operacji $\tau \subset T \times T$ i określa hierarchię zdefiniowanych operacji, np. aktualizuj > usuń > pisz > czytaj > wyszukaj.

Podmiot może uzyskać dostęp do danych przez wywołanie na jednostce danych konkretnej operacji pod warunkiem, że jego klasa ochrony jest większa od klasy ochrony jednostki danych lub jej równa i zakres jego operacji jest większy od wykonywanej operacji lub jej równy (przy uwzględnieniu dodatkowo szczególnych przypadków, które nie zostały omówione w niniejszym artykule).

Model EM określa to, jakie wymuszenia usług (*E*) są dozwolone, tzn. jakie usługi mogą być uruchomione przez podmiot (*P*) i inne usługi (*E*) (w wyniku uruchomienia kolejnej usługi przez usługę, którą wywołał uprawniony podmiot).

$$EM = \langle P, E,\ B, \delta, BF \rangle, \tag{14}$$

gdzie:
P – zbiór podmiotów,
E – zbiór usług elektronicznych,
B – zbiór kategorii uprawnień uruchamiania usług,

δ – relacja uprawnionego uruchamiania usług,
BF – zbiór funkcji modelu, generator ograniczenia integralności modelu sterowania uruchamianiem usług.

Relacja uprawnionego uruchamiania usług jest określona na parach kategorii uprawnień $\delta \subset B \times B$ i określa hierarchię kategorii uprawnień uruchamiania usług: zastrzeżone > specjalistyczne > powszechne.

Podmiot może uruchomić usługę pod warunkiem, że jego kategoria uprawnień uruchamiania jest większa od kategorii usługi lub jej równa. Usługa może uruchomić inną usługę pod warunkiem, że jej kategoria uprawnień uruchamiania jest większa od kategorii uruchamianej usługi lub jej równa (przy uwzględnieniu dodatkowo szczególnych przypadków, które nie zostały omówione w niniejszym artykule).

Wskazane modele AM i EM ze względu na ich właściwości mogą zostać wyrażone za pomocą odpowiednio – kraty sterowania dostępem i kraty sterowania uruchamianiem. Pozwoli to na składanie uprawnień i skuteczne zarządzanie bezpieczeństwem dla elektronicznych usług złożonych, których jednostki danych i usługi atomowe pochodzą z rożnych systemów, np. z różnych rejestrów państwowych. Zagadnienie wykorzystania teorii krat w modelowaniu procesów zarządzania bezpieczeństwem dla integrowanych systemów administracji publicznej zostało opisane szczegółowo w innym artykule J. Wilka[11].

5. Podsumowanie

Zaprezentowany mechanizm sterowania bezpieczeństwem informacyjnym w modelu usługowym infrastruktury informacyjnej państwa jest odpowiedzią na nowe wymagania, jakie są stawiane przed nowoczesnym państwem. Zmiana architektury na systemy i aplikacje zorientowane na usługi wymaga również nowego podejścia do problemów bezpieczeństwa. Stosowane dotychczas modele były tworzone w innej rzeczywistości (programowania strukturalnego, wyłącznie relacyjnych baz danych i silosowo budowanych systemów) i trudno jest je stosować w świecie usług elektronicznych, chmur obliczeniowych i platform integracyjnych. Budowa społeczeństwa cyfrowego wymaga stworzenia usługowej infrastruktury informacyjnej państwa, a ta musi bazować na mocnych fundamentach, jakimi są bezpieczeństwo i interoperacyjność.

[11] J. Wilk, op.cit.

Bibliografia

Bieber G., Carpenter, J., *Introduction to Service-Oriented Programming (Rev 2.1)*, 2001.

Boni M. et al., *Państwo 2.0. Nowy start dla e-administracji*, Ministerstwo Administracji i Cyfryzacji, Warszawa 2012.

Dodani M.H., *SOA 2006: State of the Art*, „Journal of Object Technology" 2006, vol. 2.

Mc Govern J., Tyagi S., Stevens M., Sunil M., *Java Web Services Architecture*, Morgan Kaufmann Publishers, San Francisco 2003.

Program Zintegrowanej Informatyzacji Państwa, Ministerstwo Administracji i Cyfryzacji, Warszawa, listopad 2013.

Radziszowski D., Zieliński K., *Nowe technologie informacyjne dla elektronicznej gospodarki i społeczeństwa informacyjnego oparte na paradygmacie SOA*, Katedra Informatyki AGH, Kraków 2011.

Reference Model for Service Oriented Architecture 1.0, Committee Specification 1, Oasis Open, 2006.

Wilk J., *Wykorzystanie teorii krat w modelowaniu procesów zarządzania bezpieczeństwem w platformach usług elektronicznych administracji publicznej*, „Roczniki" Kolegium Analiz Ekonomicznych, z. 33, Oficyna Wydawnicza SGH, Warszawa 2014.

* * *

Mechanisms for the information security management in the service-oriented public information infrastructure

Summary

In the Integrated Digitalization Programme for Poland, the Polish government decided on creating a coherent, logical and efficient state information system to provide electronic services to citizens. It has to ensure the cooperation of existing and new information and communication systems of public administration. Interoperability and security are the key elements to achieve this goal. This article presents the new information security model designed specifically for the service-oriented public information infrastructure.

Keywords: information security, electronic service, service-oriented architecture, integration platform, public information infrastructure, public services