Jarosław Wilk

Wydział Cybernetyki
Wojskowa Akademia Techniczna

Wykorzystanie teorii krat w modelowaniu procesów zarządzania bezpieczeństwem w platformach usług elektronicznych administracji publicznej

1. Wstęp

Postępująca informatyzacja wymusza wykorzystywanie danych pochodzących z wielu różnych źródeł. Konieczne staje się integrowanie niezależnych systemów, które historycznie były tworzone jako elementy odseparowane. Jednym ze sposób zapewnienia integracji systemów udostępniających usługi elektroniczne jest budowanie platform integracyjnych. Wraz z ich powstaniem pojawiły się nowe problemy związane m.in. z określeniem i zapewnieniem odpowiedniego poziomu bezpieczeństwa wdrażanych systemów.

W niniejszym artykule omówiono rolę platform integracyjnych w budowaniu cyfrowej administracji ze szczególnym uwzględnieniem wymogu bezpieczeństwa. Zaprezentowano również koncepcję wykorzystania teorii krat do rozwiązania problemu sterowania bezpieczeństwem w środowiskach zintegrowanych.

2. Rola platform integracyjnych w administracji publicznej

Ministerstwo Administracji i Cyfryzacji w raporcie *Państwo 2.0. Nowy start dla e-administracji*[1] określa kierunek informatyzacji administracji państwowej. Jej celem „powinno być ułatwienie, uproszczenie funkcjonowania bądź obsługa tych dziedzin życia, gdzie konieczna jest bezpośrednia relacja państwo–obywatel, przy zagwarantowaniu najlepszej relacji nakładów do wyników przetwarzania informacji"[2]. Zadania publiczne, jeżeli jest to możliwe, powinny być realizowane drogą elektroniczną, jako elektroniczne usługi publiczne. Istnieje wiele warunków, które należy spełnić, aby osiągnąć zamierzony cel, czyli zbudować sprawną i świadczącą usługi najwyższej jakości e-administrację. Jednym z nich, wymienianym jako kluczowy, jest założenie, że „państwowe systemy teleinformatyczne i rejestry publiczne mają ze sobą płynnie współdziałać"[3]. Nie jest możliwe zastąpienie odizolowanych systemów administracji państwowej jednym, nowym systemem, konieczne więc jest budowanie pomiędzy nimi połączeń. Niezależne integrowanie systemów okazało się nieefektywne i kosztowne, dlatego zdecydowano się na integrację opartą na centralnych systemach integrujących.

Zasady integracji rejestrów i systemów państwowych zostały opisane w Krajowych Ramach Interoperacyjności (w rozporządzeniu 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. z 2012 r. Nr 64, poz. 565 z późn. zm.), na które składają się:

- „sposoby osiągania interoperacyjności;
- architektura systemów teleinformatycznych podmiotów realizujących zadania publiczne;
- repozytorium interoperacyjności na ePUAP".

Wymieniona w Krajowych Ramach Interoperacyjności platforma ePUAP (czyli Elektroniczna Platforma Usług Administracji Publicznej) jest podstawową integracyjną platformą usług elektronicznych polskiej administracji. Opisywana jest jako „system teleinformatyczny, w którym instytucje publiczne udostępniają

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

[2] Ibidem, s. 70.

[3] Ibidem, s. 78.

usługi przez pojedynczy punkt dostępowy w sieci Internet". Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565 z późn. zm.) w pkt 13 mówi: „Dzięki niej obywatele mogą załatwiać sprawy urzędowe za pośrednictwem Internetu, natomiast przedstawiciele podmiotów publicznych bezpłatnie udostępniać swoje usługi w postaci elektronicznej"[4]. Główne cele ePUAP to:

- zapewnienie dostępności usług publicznych,
- obniżenie kosztów usług publicznych, przez ich elektroniczną realizację (odciążenie urzędów i urzędników, którzy realizowali usługi publiczne drogą tradycyjną),
- integracja usług, czyli budowanie usług wyższego poziomu, na których realizację składają się usługi podstawowe pochodzące z wielu różnych systemów i rejestrów publicznych,
- klasyfikacja usług, czyli opisanie ich w jednolity sposób, co pozwoli je łatwo katalogować, wyszukiwać, integrować i realizować.

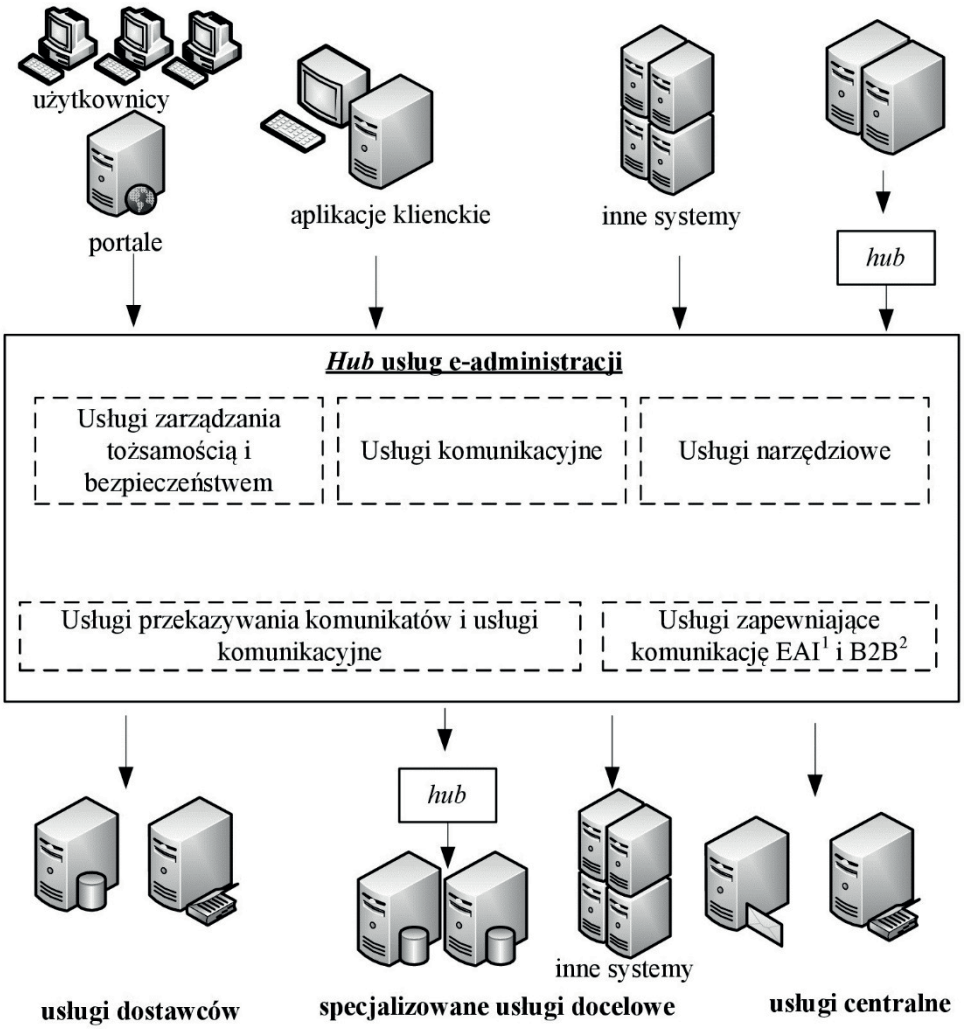
Platformy integracyjne są budowane na podstawie architektury wielostronnych ram interoperacyjności z centralnym systemem nazywanym „hubem". Umożliwia on dostęp usługobiorców do systemów dziedzinowych (np. przez portal lub aplikacje klienckie) i pozwala na komunikację systemów dziedzinowych między sobą (zarówno inne systemy, jak i inne huby mogą występować w roli klientów platformy integracyjnej). „Hub działa także jako klient, uzyskując dostęp do innych usług (wewnętrznych lub zewnętrznych), wśród których można wyróżnić następujące typy:

- usługi dostawców zewnętrznych (np. usługa weryfikacji tożsamości),
- specjalizowane usługi docelowe (podstawowe usługi świadczone przez urzędy),
- usługi centralne (usługi ogólnego przeznaczenia świadczone na zewnątrz huba, ale zarządzane w oparciu o infrastrukturę techniczną huba centralnego np. usługi poczty elektronicznej)"[5].

Schemat takiej interakcji został przedstawiony na rysunku 1.

[4] Ministerstwo Administracji i Cyfryzacji, *Czym jest ePUAP?*, http://epuap.gov.pl/wps/portal/E2_OePUAP (data odczytu 11.2012).

[5] Microsoft, *Ramy interoperacyjności systemów administracji publicznej*, 2008, s. 35.



Silniki usług integracyjnych:
[1]EAI (*Enterprise Application Integration*)
[2]B2B (*Business-to-Business*)

Rysunek 1. Kontekst i interakcje zewnętrzne huba usług dla sektora publicznego
Źródło: Microsoft, *Ramy interoperacyjności systemów administracji publicznej*, 2008, s. 34.

Zaprezentowana architektura platform integracyjnych jest wdrażana lub już została zaimplementowana w wielu różnorodnych systemach i rejestrach państwowych. Oprócz zaprezentowanej platformy ePUAP można wymienić inne, obejmujące węższy zakres integrowanych systemów, m.in.:

- Geoportal – „zakładający integrację i harmonizację usług oraz informacji przestrzennej poprzez wykorzystanie rejestrów referencyjnych/bazowych, a także koordynację działań zgodnie z modelem infrastruktury informacyjnej państwa oraz założeniami dyrektywy INSPIRE”[6];
- Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania Zasobów Cyfrowych o Zdarzeniach Medycznych – integracja systemów z obszaru ochrony zdrowia;
- Infrastruktura e-Usług Resortu Finansów (e-deklaracje, e-podatki, e-rejestracja, e-cło) – integracja usług systemów celnych i podatkowych.

Obecnie nowoczesne państwo nie może funkcjonować bez sprawnej i zinformatyzowanej administracji publicznej. Informatyzacja administracji publicznej nie jest możliwa bez integracyjnych platform usług elektronicznych budowanych na podstawie założeń interoperacyjności. Temat przedstawiony w niniejszym punkcie został szerzej rozwinięty w artykule *Rola platform integracyjnych w standaryzacji i podnoszeniu efektywności usług administracji publicznej*[7], w którym omówiono wpływ ePUAP na efektywność realizacji zadań publicznych przez państwo.

3. Bezpieczeństwo – podstawy wymóg platform integracyjnych

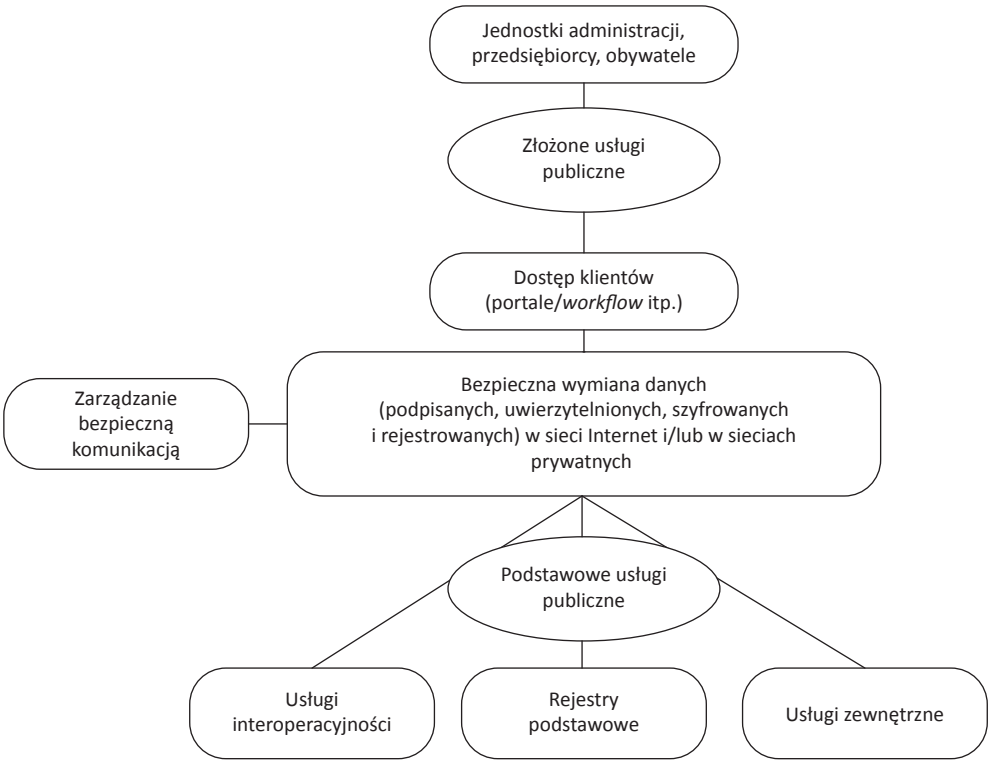
Podstawą funkcjonowania platform integracyjnych i wytwarzanych za ich pomocą usług złożonych jest zapewnienie odpowiedniego poziomu bezpieczeństwa. Dostęp z jednego portalu do wielu usług pochodzących z różnych systemów jest ogromnym wyzwaniem zarówno technologicznym, jak i organizacyjnym. Poza zapewnieniem bezpieczeństwa w warstwie technicznej (zapory ogniowe, aktualizacje, systemy wykrywania i przeciwdziałania włamaniom sieciowym itp.) kluczowe jest zintegrowanie bezpieczeństwa na poziomie logicznym. Często integrowane systemy podlegają innym resortom, przetwarzają informacje o różnych poziomach tajności, funkcjonują na podstawie innych aktów prawych. Różnorodność taka powoduje problem ze zbudowaniem jednego, wspólnego modelu bezpieczeństwa, który obejmowałby wszystkie składowe elementy złożonej platformy.

---

[6] M. Boni et al., op.cit., s. 30.

[7] J. Wilk, *Rola platform integracyjnych w standaryzacji i podnoszeniu efektywności usług administracji publicznej*, „Nowoczesne Systemy Zarządzania” (przyjęty do druku – 11.2013).

Brak modelu bezpieczeństwa opisującego integracyjną platformę usług elektronicznych i zgodnego z wymogami bezpieczeństwa każdego z integrowanych systemów jest poważną przeszkodą w budowaniu interoperacyjnej infrastruktury informacyjnej państwa. „Trudność rozwiązywania problemów bezpieczeństwa rośnie wraz ze skalą rozproszenia platformy i jej heterogenicznością. Mimo wielu rekomendacji i dobrych praktyk oraz prób standaryzacji mechanizmów podnoszenia bezpieczeństwa, rozwiązania te wciąż nie są w pełni satysfakcjonujące”[8]. Raport Gartnera[9] wskazuje bezpieczną wymianę danych i sterowanie bezpieczną komunikacją jako bazę złożonych usług publicznych (co zostało zaprezentowane na rysunku 2).



Rysunek 2. Ramy narodowych usług publicznych

Źródło: Gartner Inc., *Preparation for Update European Interoperability Framework 2.0 – Final Report*, 4.06.2007 (rozdział 4.5. *Generic Public Services Framework*).

[8] T. Górski, *Platformy integracyjne – zagadnienia wybrane*, Wydawnictwo Naukowe PWN, Warszawa 2012, s. 189.

[9] Gartner Inc., *Preparation for Update European Interoperability Framework 2.0 – Final Report*.

Obecnie poziom bezpieczeństwa budowanych platform integracyjnych jest najczęściej określany na podstawie wiedzy eksperckiej. Polityka bezpieczeństwa dla systemu centralnego jest tworzona na zasadzie kompromisu specjalistów odpowiadających za integrowane systemy. Ze względu na trudność jednoznacznego wyliczenia parametrów bezpieczeństwa (m.in. poziomów tajności, zakresu dozwolonych operacji) w przypadku usług złożonych są one nadawane od nowa na podstawie analizy właściwości powstałej usługi. Oznacza to często przyjmowanie dla platformy integracyjnej najbardziej rygorystycznej polityki bezpieczeństwa ze wszystkich integrowanych systemów. W praktyce wybór najbardziej rygorystycznej polityki również jest dużym wyzwaniem ze względu na trudność w jednoznacznym porównaniu jej rodzajów. W rezultacie decyzja o wyborze odpowiedniej polityki jest podejmowana na podstawie oceny eksperckiej dysponentów systemów, a nie jasno określonych zasad. Krajowe Ramy Interoperacyjności określają to, kto jest odpowiedzialny za opracowanie modelu bezpieczeństwa dla budowanej platformy integracyjnej. Zgodnie z § 20 pkt 1 rozdziału IV rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności: „Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje, przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność". Niestety, poza odwołaniem do polskich norm dotyczących bezpieczeństwa teleinformatycznego (PN-ISO/IEC 27001 – zarządzania bezpieczeństwem informacji; PN-ISO/IEC 17799 – ustanawiania zabezpieczeń; PN-ISO/IEC 27005 – zarządzania ryzykiem; PN-ISO/IEC 24762 – odtwarzania po katastrofie) w dalszej części rozporządzenia skupiono się na aspektach bezpieczeństwa technicznego (m.in. aktualizacji oprogramowania, mechanizmach kryptograficznych, umowach serwisowych) i organizacyjnego (m.in. szkoleniach osób, zapewnieniu odpowiednich poświadczeń bezpieczeństwa). Brakuje jednoznacznych wytycznych do oceny tego, czy systemy opisane różnymi politykami bezpieczeństwa można zintegrować w ramach platformy integracyjnej (czy ich polityki bezpieczeństwa są ze sobą zgodne) i jak zbudować politykę bezpieczeństwa, która będzie wypadkową polityk integrowanych systemów.

4. Model kratowy

Według autora, rozwiązaniem omówionego w poprzednim punkcie problemu zarządzania bezpieczeństwem w integracyjnych platformach usług elektronicznych jest model zbudowany na podstawie teorii krat. Kratami (ang. *lattices*[10]) nazywamy „zbiory uporządkowane, dla których spełniony jest warunek, że dla każdej pary elementów danego zbioru istnieje kres górny i kres dolny"[11]. Kratę można przedstawić jako:

$$(K, \leq, \oplus, \otimes), \tag{1}$$

gdzie:
K jest zbiorem częściowo uporządkowanym,
$\leq$ jest relacją częściowego porządku,
$\oplus$ jest operacją wyznaczania kresu górnego (supremum) jego argumentów,
$\otimes$ jest operacją wyznaczania kresu dolnego (infimum) jego argumentów.

Na podstawie teorii krat powstał model kratowy przepływu danych, który opisany jest przez układ:

$$MPD = (K, \leq, \oplus, \otimes, 0, \rightarrow)^{12}, \tag{2}$$

gdzie:
zbiór K jest częściowo uporządkowanym zbiorem poziomów bezpieczeństwa, np. jawne, poufne, tajne, ściśle tajne;
zbiór O jest „zbiorem obiektów częściwo uporządkowanym ze względu na relację bezpiecznego przepływu informacji pomiędzy obiektami"[13];
operacja „$\rightarrow$" określa dozwolony bezpieczny przepływ informacji z obiektu a do obiektu b ($a \rightarrow b$), jeżeli poziom bezpieczeństwa obiektu a zapisany jako $\underline{a}$ nie jest wyższy niż poziom bezpieczeństwa obiektu b zapisanego jako $\underline{b}$. Oznacza to spełnienie relacji:

---

[10] G. Birkhoff, *Lattice theory*, „American Mathematical Society Colloquium Publications", vol. 25, New York 1948.

[11] H. Rasiowa, *Wstęp do matematyki współczesnej*, Wydawnictwo Naukowe PWN, Warszawa 2005, s. 123.

[12] J. Stokłosa, T. Bilski, T. Pankowski, *Bezpieczeństwo danych w systemach informatycznych*, Wydawnictwo Naukowe PWN, Poznań 2001, s. 217.

[13] Ibidem.

$$a \to b \Leftrightarrow \underline{a} \leq \underline{b} \text{ gdzie } a, b \in 0 \text{ i } \underline{a}, \underline{b} \in K. \tag{3}$$

Możliwe jest realizowanie bezpiecznych przepływów z wielu obiektów i do wielu obiektów:

$$a_1, a_2, ..., a_n \to b \Leftrightarrow \underline{a_1} \oplus \underline{a_2} \oplus ... \oplus \underline{a_n} \leq \underline{b}^{14}, \tag{4}$$

$$a \to b_1, b_2, ..., b_n \Leftrightarrow \underline{a} \leq \underline{b_1} \otimes \underline{b_2} \otimes ... \otimes \underline{b_n}^{15}. \tag{5}$$

Na rysunku 3 został przedstawiony przykład krat bezpiecznego przepływu danych dla liniowego zbioru poziomów bezpieczeństwa od poziomu najniższego $N = 0$, np. jawne, do poziomu najwyższego $W = N - 1$, np. ściśle tajne.

Założenia

$K = \{0, 1, ..., n - 1\}$
$a \to b \Leftrightarrow \underline{a} \leq \underline{b}$
$\underline{a} \oplus \underline{b} = \max(\underline{a}, \underline{b})$
$\underline{a} \otimes \underline{b} = \min(\underline{a}, \underline{b})$
$N = 0, W = n - 1$

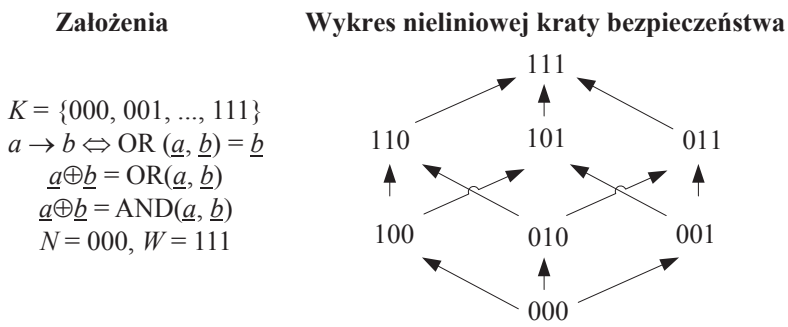
Wykres liniowej kraty bezpieczeństwa

Rysunek 3. Krata bezpiecznego przepływu danych dla liniowego zbioru poziomów bezpieczeństwa

Źródło: D.E. Denning, P.J. Denning, *Certification of Programs for Secure Information Flow*, Purdue University, 1976, s. 6.

Na rysunku 4 został przedstawiony przykład krat bezpiecznego przepływu danych dla nieliniowego zbioru poziomów bezpieczeństwa od poziomu najniższego $N = 000$ do poziomu najwyższego $W = 111$. Relacja porządkowania klas bezpieczeństwa, będących 3-bitowymi wektorami, została oparta na sumie logicznej (OR) i iloczynie logicznym (AND).

[14] Ibidem, s. 219.
[15] Ibidem.



Rysunek 4. Krata bezpiecznego przepływu danych dla nieliniowego zbioru poziomów bezpieczeństwa

Źródło: D.E. Denning, P.J. Denning, Certification of Programs for Secure Information Flow, Purdue University, 1976, s. 6.

Przedstawiona teoria krat była wykorzystywana wielokrotnie w modelach sterowania bezpieczeństwem. Znalazła zastosowanie w powszechnie używanych modelach Bella–LaPaduli[16] i Biby[17], w których krata poziomów bezpieczeństwa jest zbudowana na podstawie pary klasy i kategorii bezpieczeństwa (C, K), gdzie:

- C – jest zbiorem klasyfikacji klas bezpieczeństwa; zbiór $\{C_1, C_2, ..., C_n\}$ jest uporządkowany, tzn. $C_1 > C_2 > \cdots C_n$, np. jawne, poufne, tajne, ściśle tajne;
- K – jest zbiorem kategorii podmiotów, które muszą mieć dostęp do informacji; jego elementy odnoszą się do obszaru zastosowań, gdzie są wykorzystywane informacje $\{K_1, K_2, ..., K_q\}$; „przykładem kategorii są NATO, sztab, żandarmeria wojskowa"[18].

Poziom bezpieczeństwa $L_1 = (C_1, K_1)$ jest wyższy niż $L_2 = (C_2, K_2)$ (relacja dominancji $L_1 > L_2$) lub równy mu wtedy i tylko wtedy, gdy spełnione są relacje:

$$C_1 > C_2 \text{ i } K_1 \supseteq K_2. \tag{6}$$

W przypadku obu relacji ostrych można powiedzieć, że poziom L_1 jest wyższy niż L_2 ($L_1 > L_2$). Poziomy są nieporównywalne, jeżeli nie zachodzi relacja:

---

[16] D.E. Bell, L.J. LaPadula, *Secure Computer Systems: Mathematical Foundations*, MTR-2547, vol. 1, MITRE Corporation, Bedford, MA 1973.

[17] K.J. Biba, *Integrity Considerations for Secure Computer Systems*, MTR-3153, The Mitre Corporation, 1977.

[18] J. Stokłosa, op.cit., s. 160.

$$L_1 > L_2 \text{ ani } L_1 < L_2. \tag{7}$$

Oba modele są zbudowane na podstawie wielu aksjomatów opisujących dozwolone warunki przepływu informacji w celu zapewnienia ich tajności (model BLP) i integralności (model Biby). Nie zostaną one tu omówione ze względu na brak bezpośredniego związku z tematem niniejszego artykułu.

Teoria krat znalazła również zastosowanie w biznesowym modelu bezpieczeństwa opartym na koncepcji muru chińskiego. Model Brewera–Nasha[19] zakłada istnienie klas konfliktów, do których należą konkurujące ze sobą organizacje. „Podmiot ma dostęp do dowolnej informacji (obiektu) dopóty, dopóki nie uzyska dostępu do informacji innej organizacji z tej samej klasy konfliktu interesów"[20]. Bezpieczny dozwolony przepływ informacji pomiędzy obiektami opisany za pomocą kraty muru chińskiego jest uzależniony od etykiety określającej, z jakich organizacji czerpał on informacje. Dopuszczalne są tylko takie etykiety, które nie naruszają zasady klas konfliktu. „Obiekt opisany jest n-elementowym wektorem $[i_1, i_2, ..., i_n]$, gdzie każde $i_k \in COI_k$ (COI_1, COI_2, ..., COI_n – zbiór klas konfliktu) lub $i_k = \perp$ dla $k = 1... n$ (symbol $\perp$ oznacza brak informacji pochodzącej z danej klasy konfliktu). [...] Przykładowo obiekt zawierający informacje z firmy 7 w klasie konfliktu COI_2 i informacje z firmy 5 w klasie konfliku COI_4 jest opisany wektorem $[\perp, 7, \perp, 5, \perp, ..., \perp]$"[21].

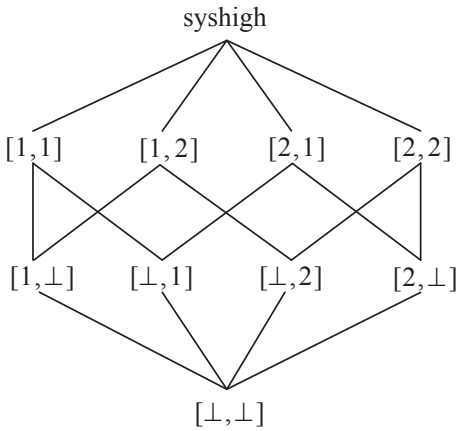
Rysunek 5 prezentuje przykładową kratę muru chińskiego, określającego możliwy bezpieczny przepływ informacji pomiędzy obiektami zawierającymi informacje pochodzące z dwóch klas konfliktu i dwóch organizacji. „Symbol $[\perp, \perp]$ oznacza informację dostępną powszechnie"[22] (niepochodzącą z żadnej organizacji), natomiast „syshigh" jest teoretyczną etykietą (wymaganą do prawidłowego zapisu modelu kratowego), która dominuje nad wszystkimi pozostałymi etykietami bezpieczeństwa.

[19] D.F.C. Brewer, M.J. Nash, *The Chinese Wall Security Policy*, Gamma Secure Systems Limited, Surrey, United Kingdom 2001.

[20] K. Liderman, *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012, s. 97.

[21] R.S. Sandhu, *Lattice-based access control models*, George Mason University, 1993, s. 18.

[22] Ibidem.



Rysunek 5. Krata bezpiecznego przepływu danych dla nieliniowego zbioru poziomów bezpieczeństwa

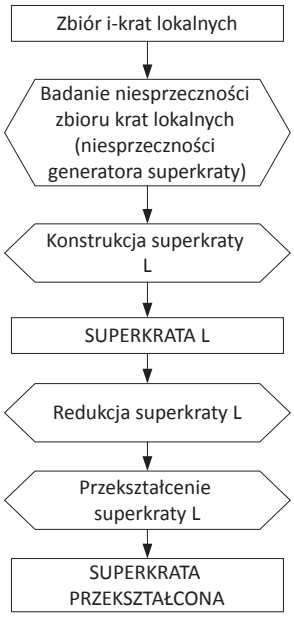
Źródło: R.S. Sandhu, *Lattice-based access control models*, George Mason University, 1993, s. 18.

5. Model sterowania bezpieczeństwem w platformach integracyjnych

Teorię krat można również wykorzystać do zbudowania modelu sterowania bezpieczeństwem w platformach integracyjnych. Podstawą nowego rozwiązania jest kratowy model ochrony danych w systemach rozproszonych baz danych[23], opracowany przez B. Szafrańskiego. Zakłada on opisanie bezpieczeństwa bazy danych za pomocą kraty ochrony danych będącej złożeniem kraty przepływu i zakresu operacji, a następnie przy wykorzystaniu zbioru krat lokalnych zbudowanie z nich superkraty bezpieczeństwa[24], opisującej całe zintegrowane środowisko. Przekształcenia są realizowane zgodnie z metodyką przedstawioną na rysunku 6.

[23] B. Szafrański, *Modelowanie procesów ochrony baz danych ze szczególnym uwzględnieniem ich integracji*, Wojskowa Akademia Techniczna, Warszawa 1987.

[24] Ibidem, s. 104.



Rysunek 6. Szkic metodyki tworzenia i przekształcania superkraty

Źródło: B. Szafrański, *Modelowanie procesów ochrony baz danych ze szczególnym uwzględnieniem ich integracji*, Wojskowa Akademia Techniczna, Warszawa 1987, s. 106.

Zastosowanie przedstawionej powyżej metodyki zarówno pozwala zweryfikować to, czy integrowane systemy (w omawianym przypadku rozproszone bazy danych) można zintegrować, jak i umożliwia wyznaczenie kraty bezpieczeństwa, która opisuje całe zintegrowane środowisko.

W przypadku integracyjnych platform usług elektronicznych konieczne jest zdefiniowanie krat bezpieczeństwa, które opisują specyficzne parametry środowiska zorientowanego na usługi. Autor proponuje dwa możliwe podejścia do wskazanego problemu:

- Pierwsze, w którym operuje się na najniższym poziomie zbioru dostępów do danych składających się na usługę elektroniczną.
- Drugie, w którym operuje się na wyższym poziomie abstrakcji i w którym sterowanie bezpieczeństwem odbywa się w obszarze wywołań usług elektronicznych (bez analizowania dostępów do danych).

W obu przypadkach konieczne jest zdefiniowanie kraty zakresu operacji:

$$AL = < T, \Psi, \nabla, \Delta, t^{max}, t^{min} >^{25}, \tag{8}$$

[25] Ibidem, s. 82.

gdzie:
T – częściowo uporządkowany zbiór operacji, np. listuj ≤ czytaj ≤ zapisz ≤ wykonuj,
T – relacja zakresu działania operacji,
∇, Δ – operatory kresów górnego i dolnego,
t^{max}, t^{min} – ograniczenia górne i dolne zbioru operacji.

Zależnie od wybranego podejścia należy zdefiniować również kratę przepływu danych dla modelu operującego na poziomie danych lub kratę wywołania w przypadku modelu operującego na poziomie usług. Krata przepływu danych zdefiniowana jest jako:

$$CL = \quad < K, \rho, \oplus, \otimes, k^{max}, k^{min} >^{26}, \tag{9}$$

gdzie:
K – zbiór klas ochrony,
ρ – relacja przepływu,
$\oplus, \otimes$ – operatory kresów górnego i dolnego,
k^{max}, k^{min} – ograniczenia górne i dolne zbioru klas ochrony.

Zamiast kraty przepływu możliwe jest wykorzystanie „kraty wywołania", gdzie relacja przepływu informacji jest zastąpiona relacją wywołania usługi przez podmiot posiadający uprawnienia do powiązanej z usługą klasy ochrony. Jest ona zdefiniowana jako:

$$CL = \quad < K, \Omega, \oplus, \otimes, k^{max}, k^{min} >, \tag{10}$$

gdzie:
K – zbiór klas ochrony,
Ω – relacja wywołania,
$\oplus, \otimes$ – operatory kresów górnego i dolnego,
k^{max}, k^{min} – ograniczenia górne i dolne zbioru klas ochrony.

W wyniku złożenia dwóch krat – zakresu operacji i przepływu lub zakresu operacji i wywołania – powstanie krata ochrony danych, która jest „kratą bezpieczeństwa" systemu dziedzinowego. Korzystając z operacji kresu górnego i dolnego, można wyznaczyć graniczne wartości klas ochrony i zakresu działania dla wywoływanych usług elektronicznych lub przetwarzanych danych,

[26] Ibidem, s. 79.

a następnie porównać je z uprawnieniami, jakie posiada podmiot generujący żądania. Następnie po uzyskaniu lokalnych krat bezpieczeństwa dla systemów dziedzinowych (pierwszą lub drugą metodą) można utworzyć jedną superkratę, obejmującą pełną domenę bezpieczeństwa platformy integracyjnej.

Superkrata platformy integracyjnej jest wykorzystywana w modelu sterowania bezpieczeństwem w integracyjnych platformach usług elektronicznych analogicznie do wykorzystania kraty bezpieczeństwa w systemach dziedzinowych. Pozwalana na określenie wymagań i parametrów bezpieczeństwa, jakie musi spełnić podmiot, aby wywołać złożoną usługę elektroniczną (zbudowaną z wielu usług prostych pochodzących z różnych systemów dziedzinowych).

6. Podsumowanie

Omówiona koncepcja wykorzystania teorii krat do sterowania bezpieczeństwem w platformach usług elektronicznych pozwala rozwiązać dwa podstawowe problemy:

- jednoznacznego określenia, czy dane systemy mogą być ze sobą integrowane na podstawie architektury platform integracyjnych,
- wyznaczenia modelu bezpieczeństwa dla zintegrowanej infrastruktury usługowej nawet w przypadku różnorodności modeli bezpieczeństwa opisujących systemy dziedzinowe.

Jak zostało wykazane, platformy integracyjne są obecnie podstawowym narzędziem wykorzystywanym w procesach informatyzacji administracji publicznej i dlatego zaproponowanie dobrego modelu sterowania bezpieczeństwem jest kluczowym czynnikiem warunkującym ich dalszy rozwój. Wraz ze zwiększaniem się liczby systemów dziedzinowych coraz trudniejsze staje się budowanie polityk bezpieczeństwa i określanie poziomów bezpieczeństwa złożonych usług publicznych tylko na podstawie wiedzy eksperckiej. Zaprezentowane rozwiązanie wymaga dalszych prac w celu doprecyzowania i weryfikacji wskazanego modelu. Konieczna jest ścisła współpraca administracji państwowej i ośrodków badawczych tak, aby tworzone modele mogły być wykorzystane w praktyce w budowaniu nowoczesnych i bezpiecznych elektronicznych usług publicznych.

Bibliografia

1. Bell D.E., LaPadula L.J., *Secure Computer Systems: Mathematical Foundations*, MTR-2547, vol. 1, MITRE Corporation, Bedford, MA 1973.
2. Biba K.J., *Integrity Considerations for Secure Computer Systems*, MTR-3153, The Mitre Corporation, 1977.
3. Birkhoff G., *Lattice theory*, „American Mathematical Society Colloquium Publications", vol. 25, New York 1948.
4. Boni M. et al., *Państwo 2.0 Nowy start dla e-administracji*, Ministerstwo Administracji i Cyfryzacji, Warszawa 2012.
5. Brewer D.F.C., Nash M.J., *The Chinese Wall Security Policy*, Gamma Secure Systems Limited, Surrey, United Kingdom 2001.
6. Denning D.E., Denning P.J., *Certification of Programs for Secure Information Flow*, Purdue University, 1976.
7. Gartner Inc., *Preparation for Update European Interoperability Framework 2.0 – Final Report*, 4.06.2007.
8. Górski T., *Platformy integracyjne – zagadnienia wybrane*, Wydawnictwo Naukowe PWN, Warszawa 2012.
9. Liderman K., *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012.
10. Microsoft, *Ramy interoperacyjności systemów administracji publicznej*, 2008.
11. Rasiowa H., *Wstęp do matematyki współczesnej*, Wydawnictwo Naukowe PWN, Warszawa 2005.
12. 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. z 2012 r. Nr 64, poz. 565 z późn. zm.).
13. Sandhu R.S., *Lattice-based access control models*, George Mason University, 1993.
14. Stokłosa J., Bilski T., Pankowski T., *Bezpieczeństwo danych w systemach informatycznych*, Wydawnictwo Naukowe PWN, Poznań 2001.
15. Szafrański B., *Modelowanie procesów ochrony baz danych ze szczególnym uwzględnieniem ich integracji*, Wojskowa Akademia Techniczna, Warszawa 1987.
16. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565 z późn. zm.).
17. Wilk J., *Rola platform integracyjnych w standaryzacji i podnoszeniu efektywności usług administracji publicznej*, „Nowoczesne Systemy Zarządzania" (przyjęty do druku – 11.2013).

Źródła sieciowe

1. Ministerstwo Administracji i Cyfryzacji, *Czym jest ePUAP?*, http://epuap.gov.pl/wps/portal/E2_OePUAP (data odczytu 8.11.2012).

* * *

The use of lattice theory in the modelling of safety management processes in public administration electronic services platforms

Summary

This article discusses the role of integration platforms in public administration. Particular attention was given to security, which is a basic requirement of integration platforms. Furthermore, a review of lattice models used to control security was presented. A new model of safety management for electronic services integration platform (based on the lattice theory) was introduced.

Keywords: security, integration platforms, electronic services, state administration, public services, interoperability, lattice access control