STUDIA INFORMATICA 2002
Volume 23 Number 2B (49)

Grzegorz FILIPCZYK
Politechnika Śląska, Instytut Informatyki

WSTĘP DO ANALIZY BEZPIECZEŃSTWA SYSTEMU KOMPUTEROWEGO JEDNOSTKI ADMINISTRACJI SAMORZĄDOWEJ

Streszczenie. W artykule przedstawiono wyniki kolejnego etapu długofalowych badań nad bezpieczeństwem systemu komputerowego jednostki administracji samorządowej. Pokazany został model formalny systemu utworzony do badań z wykorzystaniem metod formalnych HAZOP i IT Grundschutz. Opisany został tryb prowadzenia badań, ich wyniki oraz wynikające z nich wnioski.

THE INTRODUCTION TO THE ANALYSIS OF TOWN OFFICE COMPUTER SYSTEM SECURITY

Summary. In this paper next part of the long-term researches over the security of the town office computer system is presented. Formal model, that has been prepared for the purpose of HAZOP and IT Grundschutz methodologies, is shown. Author describes the flow of researches, results and conclusions.

1. Prawne podstawy budowy systemu

Badanie bezpieczeństwa dużego systemu komputerowego wymaga zastosowania metod formalnych działających na jego modelu. Z punktu widzenia systemu komputerowego administracji samorządowej szereg aktów prawnych traktować należy jako specyfikację jego budowy, czyli inaczej mówiąc – specyfikację modelu. Ograniczeniem, jakie zostało nałożone w trakcie badań, których wyniki są tu prezentowane, było przeprowadzenie ich dla jednostki samorządu na poziomie powiatu grodzkiego, a jako przykład posłużył Urząd Miasta Piekary Śląskie. Niektóre aspekty takiego systemu określone są w omówionych niżej przepisach.

1.1. Funkcje jednostki administracji samorządowej

Urząd miasta jest podstawową komórką administracji. Za jego pomocą realizowane są zadania ustanowione przez Radę Miasta, Zarząd Miasta, a także zadania zlecone z zakresu administracji rządowej. Różnorodność i ilość funkcji ujmowana jest w znany schemat podziału na wydziały i referaty, z których najpowszechniej występujące realizują wymienione zadania:

- Wydział finansowy: sporządza sprawozdania rachunkowe, prowadzi wymiar i pobór podatków, ewidencjonuje i windykuje należności z tytułu dzierżawy i użytkowania wieczystego,
- Wydział spraw obywatelskich: wydaje dokumenty tożsamości, prowadzi ewidencję ludności, organizuje pobór wojskowy,
- Wydział architektury: prowadzi rejestr miejscowych planów zagospodarowania przestrzennego, wydaje pozwolenia na budowę,
- Wydział geodezji: prowadzi ewidencję nieruchomości i gruntów, prowadzi miejską bazę danych wchodzącą w ogólnopolski system informacji o terenie,
- Wydział komunikacji: prowadzi rejestrację i ewidencję pojazdów, wydaje uprawnienia do kierowania pojazdami.

Do realizacji wymienionych i pozostałych zadań konieczne jest stworzenie mechanizmów usprawniających proces gromadzenia i przetwarzania danych. Naturalnym narzędziem stwarzającym takie możliwości jest system komputerowy.

1.2. Informatyka w urzędzie miasta

Zgodnie z [14], możliwe jest stosowanie w pracy urzędu miasta technik komputerowych. Rozdział XVI *wykorzystanie informatyki w czynnościach kancelaryjnych* przewiduje m.in. następujące zakresy wykorzystania technik komputerowych:

- poczta elektroniczna,
- elektroniczny obieg dokumentów,
- komputerowe rejestry dotyczące obiegu dokumentów,
- tworzenie i eksploatacja baz danych, w szczególności ewidencji prawa miejscowego,
- monitorowanie zaleceń Prezydenta Miasta oraz załatwiania spraw urzędowych,
- realizacja prawa dostępu do informacji publicznej.

Należy zaznaczyć, że rozporządzenie reguluje również zakres eksploatacji urządzeń teleinformatycznych (§.54.1 aktu).

Istnieją także inne akty prawne wskazujące na zakres wykorzystania informatyki w urzędzie. Są to np.:

- Ustawa o rachunkowości,

- Ustawa o ewidencji ludności,
- Ustawa o ewidencji gruntów i nieruchomości,
- Ustawa prawo o ruchu drogowym.

Przewidują one tworzenie i eksploatację baz danych na potrzeby zadań, jakie opisują. Zawarte w nich zapisy, dotyczące wzajemnych zależności informacyjnych pomiędzy dedykowanymi dla nich systemami komputerowymi, mają fundamentalny wpływ na bezpieczeństwo pracy urzędu jako całości.

1.3. Tajemnice w prawie polskim, ochrona informacji

Podstawową funkcją systemu w urzędzie miasta jest gromadzenie, przetwarzanie i ochrona informacji. Warto poświęcić nieco więcej uwagi pewnemu specjalnemu ich rodzajowi, który wymaga szczególnej ochrony. Są to tzw. informacje niejawne. Kwestie dostępu do informacji stanowiących tajemnicę państwową i służbową reguluje [23]. Informacje wymagające ochrony przed nieuprawnionym ujawnieniem mogą stanowić tajemnicę państwową bądź też tajemnicę służbową. Definicje tajemnic są następujące:

- **tajemnica państwowa** – jest to informacja niejawna, której nieuprawnione ujawnienie może spowodować istotne zagrożenie dla podstawowych interesów Rzeczypospolitej Polskiej, a w szczególności dla niepodległości lub nienaruszalności terytorium, interesów obronności, bezpieczeństwa państwa i obywateli, albo narazić te interesy na co najmniej znaczną szkodę ([23] art. 2, ust. 1),
- **tajemnica służbowa** – jest to informacja niejawna nie będącą tajemnicą państwową, uzyskana w związku z czynnościami służbowymi, której nieuprawnione ujawnienie mogłoby narazić na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej ([23] art. 2, ust. 2).

Z przeprowadzonej w trakcie badań analizy wynika, że w przypadku informacji gromadzonych w urzędzie miasta mamy do czynienia z tajemnicą służbową.

Zarówno tajemnicom państwowym, jak i tajemnicom służbowym przydziela się tzw. klauzule tajności. Tajemnicom służbowym przypisuje się klauzule wynikające z art. 23:

- **poufne** - w przypadku gdy ich nieuprawnione ujawnienie spowodowałoby szkodę interesu publicznego lub prawnie chronionego interesu obywateli ([23] art. 23.2, ust. 1),
- **zastrzeżone** - w przypadku gdy ich nieuprawnione ujawnienie mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli albo jednostki organizacyjnej ([23] art. 23.2, ust. 2).

[23] reguluje również kwestie bezpieczeństwa sieci komputerowych używanych do gromadzenia i przetwarzania informacji niejawnych. Szczególne wymagania bezpieczeństwa systemu lub sieci teleinformatycznej powinny być kompletnym i wyczerpującym opisem ich

budowy, zasad działania i eksploatacji wraz z procedurami bezpieczeństwa, które muszą być spełnione w fazie projektowania, wdrażania i funkcjonowania systemu lub sieci. Dla każdego systemu lub sieci, w której mogą być przetwarzane informacje niejawne, opracowuje się je na etapie projektowania oraz każdym z późniejszych etapów. Wydane na mocy [23] rozporządzenie [16] w §2.2 precyzuje pojęcie bezpieczeństwa w aspekcie prawnym i dzieli je na:

- ochronę fizyczną,
- ochronę elektromagnetyczną,
- ochronę kryptograficzną,
- bezpieczeństwo transmisji,
- kontrolę dostępu.

Kwestie bezpieczeństwa systemu komputerowego w jednostce administracji państwowej porusza także [14]. W §55 znajduje się szereg zaleceń dotyczących zabezpieczania danych, z których wynika m.in. następujący fakt: **korzystanie z dostępu do Internetu może odbywać się tylko ze stanowisk komputerowych nie podłączonych do wewnętrznej sieci komputerowej**.

Przytoczone wyżej przepisy wraz z innymi aktami dotyczącymi szczególnych zakresów działania urzędu, stanowią „rozproszoną" specyfikację systemu komputerowego. Zostały one tutaj przedstawione, aby pokazać, jak szeroki musi być zakres i jak wiele czynników należy uwzględnić w trakcie analizy bezpieczeństwa systemu komputerowego jednostki administracji samorządowej. Z tego powodu w procesie tym wykorzystano metody działające na modelu formalnym, którego specyfikację stanowią te właśnie akty. Wybrane zostały dwie metody: HAZOP i IT Grundschutz. Zastosowanie dwóch odmiennych metod pozwalało mieć nadzieję na zwiększony obiektywizm rezultatów. Jak się okazało, w efekcie uzyskano, w sposób niezależny, zbliżone wyniki analizy.

2. Metody badania bezpieczeństwa

2.1. HAZOP

W trakcie badań wykorzystano metodę HAZOP (*ang. hazard and operability*) [5,4] przeznaczoną do badania bezpieczeństwa systemów komputerowych. Za pomocą metody rozpatrywane są możliwe zagrożenia (hazardy) prawidłowego działania systemu, a także ich konsekwencje. Przedmiotem jej działania jest wyszukiwanie możliwości wystąpienia zdarzeń naruszenia bezpieczeństwa. Tryb prowadzenia analizy systemu zakłada ustaloną proceduralnie dyskusję nad poszczególnymi elementami formalnego modelu systemu.

HAZOP nie jest ściśle formalną, matematyczną metodą oceny bezpieczeństwa. W literaturze nazywa się ją czasem półformalną inspekcją dokumentową [9].

Zakłada się istnienie formalnej reprezentacji badanego systemu w postaci modelu zrozumiałego dla członków zespołu analitycznego. Identyfikacja możliwych hazardów polega na ich wyszukiwaniu w toku ustalonej proceduralnie dyskusji miedzy członkami zespołu ekspertów. Dyskutowane są podatności elementów widocznych w modelu formalnym oraz związane z nimi możliwości zagrożeń, a także wydawane są zalecenia potrzebnych zmian lub dodatkowych badań. HAZOP może być stosowany na każdym z etapów w cyklu życia systemu komputerowego, zarówno do analizy projektu, jak i działającego produktu. Proces badania systemu wymaga, by powstał zespół ekspertów liczący do siedmiu osób. Przykładami możliwych narzędzi tworzenia modeli są:

- diagramy przepływu danych,
- diagramy przepływów sterowania,
- diagramy związków encji[1],
- diagramy przejść stanów.

Dobrą cechą reprezentacji systemu jest jej hierarchiczność, pozwalająca na przekrojowe spojrzenie na badany system komputerowy. Przykładem wykorzystania hierarchiczności może być zastosowanie diagramów przepływu danych równoważonych warstwowo (w górę lub w dół). HAZOP nadaje się do przeprowadzenie analizy na wysokich i średnich warstwach modelu. Im większy stopień szczegółowości, tj. im niższa warstwa modelu, tym wyższe są koszty prowadzenia analizy, a zarazem mniejsza zasadność wykorzystania metody HAZOP. Standard [4] zaleca dla niższych warstw stosowanie innych metod, np. metody FMEA [12].

Dla każdego elementu na modelu rozpatrywane są możliwe odstępstwa od zamierzonego działania. Odstępstwa te wyrażane są przez tzw. słowa kluczowe (*ang. guide words*), odniesione do atrybutów opisujących ten element. W metodzie, w zależności od rodzaju modelu formalnego, stosuje się pełny lub okrojony zbiór słów kluczowych. Podzbiór słów dla diagramów przepływu danych (*ang. DFD – data flow diagram*) jest przedstawiony w [4]. „Przyłożenie" słowa kluczowego do wybranego elementu w modelu ma w konsekwencji dać odpowiedź na pytanie „jakie są możliwe przyczyny występujących hazardów".

Nie jest jednak celem analizy HAZOP dokonywanie zmian w projekcie bądź działającym systemie. Z tego punktu widzenia HAZOP powinien być traktowany jako uzupełnienie innych form badania i osiągania bezpieczeństwa systemów. Więcej na temat metody znaleźć można np. w [6].

---

[1] ERD (*ang. entity relationship diagram*) – model sieciowy opisujący na wysokim poziomie abstrakcji układ danych przechowywanych w systemie.

2.2. IT Grundschutz

Druga z zastosowanych metod została opracowana przez instytucję BSI [3], niemiecki urząd ds. bezpieczeństwa teleinformatycznego. Przedstawiony tu opis pozwala zorientować się w ogólnych zasadach. W kontekście przeprowadzonych badań zwrócona została szczególna uwaga na etap określenia wymagań ochronnych dla składowych systemu. Przedstawienie całości zasad IT Grundschutz przekracza ramy tego artykułu, dlatego ograniczono się do ich ogólnego przedstawienia. Dokładniej opisane zostały tu te etapy, które w kontekście badań były najbardziej istotne. Szczegóły na temat metody znaleźć można np. w [2,3,28]. Na proces analizy systemu IT składają się:

- Analiza systemu:
  - Przygotowanie planu sieci. Jest to punkt startowy dla analizy struktury systemu IT. Stanowi graficzną reprezentację komponentów użytych w systemie oraz przedstawia sposób komunikacji poszczególnych elementów sieci.
  - Redukcja schematu. Polega ona na usunięciu ze schematu zbędnych informacji (o elementach, które są w identycznej konfiguracji lub są włączone w system w taki sam sposób), które komplikują dalszą analizę.
  - Zebranie informacji o elementach sieci. W tym etapie należy się skupić na technicznym wymiarze danego elementu systemu, tj. określić jego status, np. Windows NT Serwer, klient Novell z Windows 95, PC „stand alone" itp.
  - Zgromadzenie informacji o aplikacjach wykorzystywanych w systemie. Tutaj należy określić, jakie aplikacje są wykorzystywane w systemie. Zaleca się ograniczenie liczby rozpatrywanych aplikacji, tylko do najbardziej istotnych z punktu widzenia firmy. Uzyskanie w tym etapie informacje są niezbędne do rozpoczęcia procesu wyznaczania celu bezpieczeństwa.
- Wyznaczenie celu bezpieczeństwa. Etap ten, jako najbardziej znaczący w kontekście badań, opisany jest dokładniej w dalszej części.
- Modelowanie systemu modułami wzorcowymi. Tworzenie koncepcji bezpieczeństwa opiera się na zamodelowaniu istniejącego systemu IT tzw. *modułami wzorcowymi*, będącymi integralną częścią metodyki. Czynność ta nazywa się operacją mapowania, bowiem mamy do czynienia z sytuacją w której istniejący i działający system próbuje się zamodelować za pomocą gotowych „matryc". Następnie analizuje się każdy moduł i rozpatruje możliwe zagrożenia i zabezpieczenia. Pozwala to na ustalenie listy zabezpieczeń, które powinny znaleźć się w systemie. Mając gotową listę zabezpieczeń można przejść do etapu kompilacji, w którym porównuje się tę listę z istniejącymi zabezpieczeniami. W wyniku otrzymujemy kolejną listę – brakujących zabezpieczeń.

Wdrożenie tych zabezpieczeń gwarantuje osiągniecie ustalonego poziomu zabezpieczeń wg IT Grundschutz.

Wyznaczenie celu bezpieczeństwa. Istotą wyznaczania celu bezpieczeństwa jest określenie wymagań ochronnych. Ze względu na rozległość tego procesu można go podzielić na cztery obszary, których dotyczy:

- aplikacje,
- systemy IT,
- łącza komunikacyjne,
- pomieszczenia.

Najbardziej istotne jest prawidłowe określenie wymagań ochronnych dla aplikacji. Wymagania dla systemów IT, komunikacji oraz pomieszczeń definiuje się bazując na wynikach otrzymywanych dla aplikacji. W celu określenia wymagań ochronnych należy sprecyzować stopień protekcji[1] dla poufności, integralności i dostępności. Aby dobrze określić stopień protekcji dla aplikacji wykorzystywanych w systemie IT, należy rozpatrzyć każdą aplikację pod kątem poufności, integralności, i dostępności do danych, na których operuje. Cały ten proces można podzielić na trzy etapy:

- Zdefiniowanie kategorii szkód:
  - naruszenie praw, regulaminów, warunków umów,
  - utrata zdolności do samookreślania,
  - osłabienie fizycznej integralności osoby,
  - zafałszowanie informacji o swych zobowiązaniach lub wynikach,
  - negatywne efekty na zewnątrz (np. kompromitacja firmy),
  - straty finansowe.
- Rozpatrzenie możliwych zagrożeń.
- Analiza wyników.

Każdy z etapów wymaga systematycznego podejścia, co pozwoli zagwarantować, że system zostanie prawidłowo oceniony pod kątem podatności na zagrożenia. Przeoczenie jakiejkolwiek podatności może w znacznym stopniu obniżyć poziom bezpieczeństwa całego systemu.

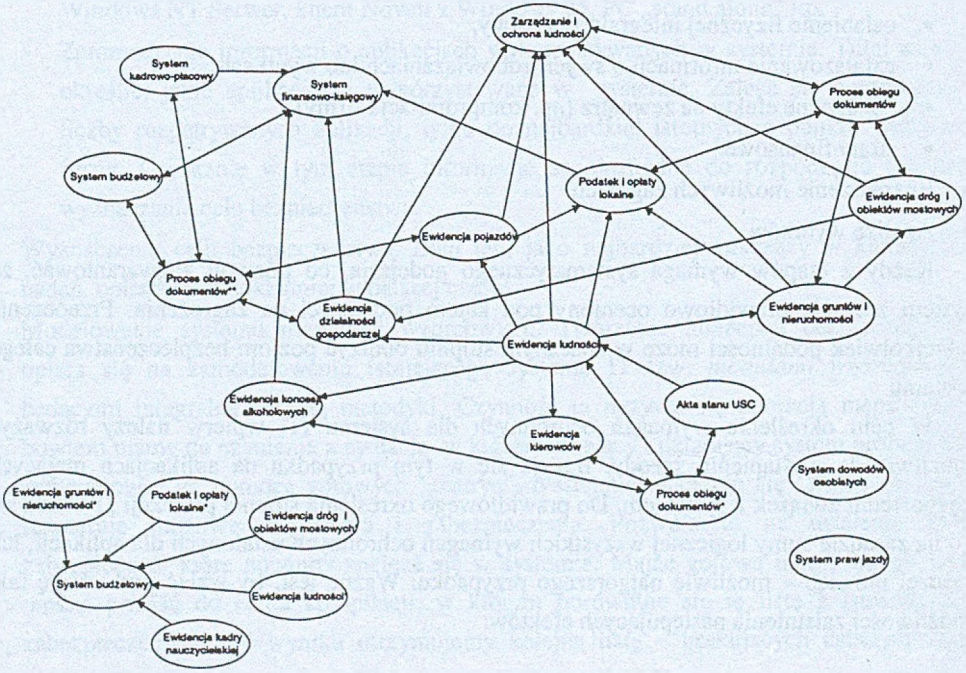
W celu określenia wymagań ochronnych dla systemu IT, wpierw należy rozważyć możliwie do wystąpienia szkody. Bazuje się w tym przypadku na aplikacjach mających bezpośredni związek z systemem. Do prawidłowego określenia stopnia protekcji IT ustala się go na zasadzie sumy logicznej wszystkich wymagań ochronnych ustalonych dla aplikacji, lub inaczej mówiąc – możliwie najgorszego przypadku. Ważne jest, by wziąć pod uwagę fakt możliwości zaistnienia następujących efektów:

[1] Definicja pojęcia „stopień protekcji" znajduje się np. w [8].

- związek zależny: analizując potencjalne zagrożenia oraz ich skutki należy wziąć pod uwagę fakt, że aplikacja działająca w systemie może używać na wejściu danych opracowanych przez inną aplikację,
- efekt kumulacji: jeśli w systemie działa kilka aplikacji o mniejszym znaczeniu, to należy wziąć pod uwagę fakt, że działanie kilku mniejszych przyczyn daje w rezultacie większy efekt – w naszym przypadku większe skutki uszkodzeń,
- efekt dystrybucji: jest to proces odwrotny do efektu kumulacji – zachodzi w przypadku gdy aplikacja o wysokich wymaganiach ochronnych jest uruchamiana w systemie tylko częściowo i niewielkie uszkodzenia mogą mieć znaczący wpływ na całość systemu.

3. Model systemu

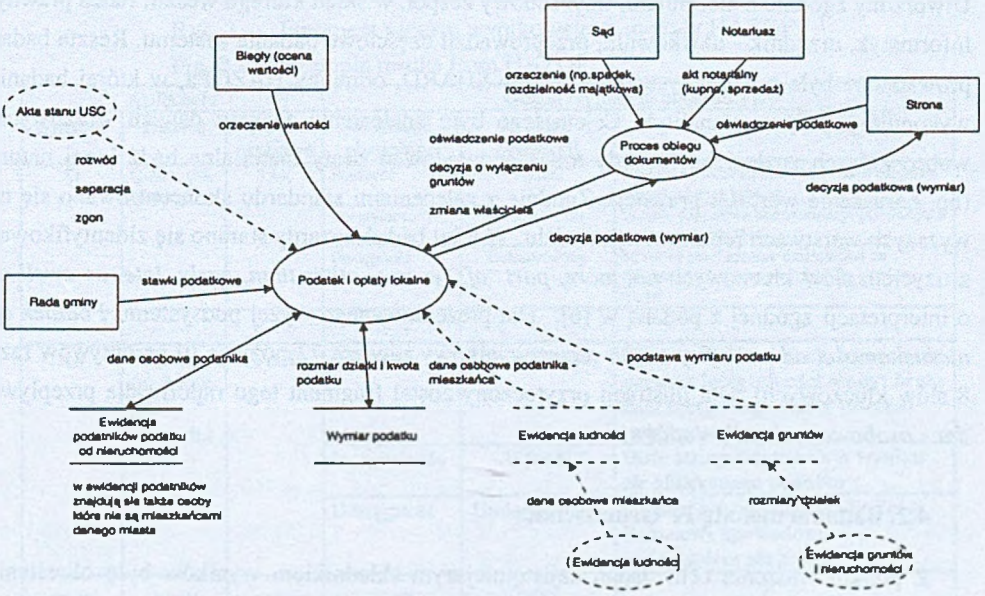
Traktując sygnalizowane wcześniej akty prawne jak specyfikację podsystemów składających się na system urzędu miasta, sporządzono model formalny opierając się na diagramach przepływu danych. Wybór DFD (*ang. data flow diagram*) podyktowany był względami praktycznymi. W trakcie wcześniejszych badań metodą HAZOP okazało się, że jest to najlepiej zrozumiała reprezentacja dla członków zespołu badawczego nie będących informatykami.



Rys. 1. Diagram przepływu danych systemu urzędu miasta
Fig. 1. Data flow diagram model for town office computer system

Na system urzędu składa się 18 podsystemów. Ogólny kształt systemu urzędu przedstawiony jest na Rys. 1. Z diagramu usunięto magazyny i etykiety przepływów celem zwiększenia jego czytelności. W modelu każdemu przedstawionemu tu procesowi odpowiada pojedynczy diagram. Przykładowy diagram dotyczący podsystemu *Podatek od nieruchomości od osób fizycznych* przedstawiony jest na Rys. 2. Kropkowaną linią zaznaczono przepływy i podsystemy, których połączenie z przedstawionym podsystemem nie ma postaci jawnego wymagania prawnego, jest natomiast wynikiem logicznej analizy. Specyfikacja podsystemu oparta została na [26,20,24,18,25,19,21,23,22,15,16,13].

Działanie podsystemu jest następujące. Gromadzone są dane ewidencyjne podatników zarówno będących mieszkańcami miasta, jak i zamieszkałych poza nim (magazyn *Ewidencja podatników podatku od nieruchomości*). Razem z danymi ewidencyjnymi gromadzone są dane o podlegających opodatkowaniu zasobach posiadanych przez podatników (magazyn *Wymiar podatku*) i wartościach tych podatków. Dane do obydwu magazynów pochodzą z oświadczeń składnych przez stronę (osoba fizyczna) zawierających dane osobowe i majątkowe podatnika.



Rys. 2. Model DFD podsystemu podatek od nieruchomości
Fig. 2. DFD model for local taxes subsystem

Konkretny wymiar podatku obliczany jest na podstawie ustalonych przez Radę Miasta stawek. W przypadku zaistnienia rażącej niezgodności co do wartości opodatkowanego zasobu, zasób wyceniany jest przez biegłego rzeczoznawcę (terminator *Biegły*). Celem działania podsystemu jest wydanie właściwej decyzji administracyjnej nakładającej konieczność wykonania obowiązku podatkowego przez podatnika (przepływ *decyzja*

podatkowa (wymiar)). Powinno występować zasilanie danymi z podsystemu *Urząd Stanu Cywilnego* w celu uwzględnienia informacji na temat zgonów, rozwodów, separacji itp. Wskazana jest weryfikacja danych osobowych podatników z danymi z podsystemu *Ewidencja ludności*. W odniesieniu do danych dotyczących podstawy wymiaru podatku potrzebna jest weryfikacja z danymi z podsystemu *ewidencji gruntów i nieruchomości*. Zbudowany model posłużył do badań w metodzie HAZOP oraz IT Grundschutz.

4. Wyniki badań

4.1. Badania metodą HAZOP

W szczególności można metodę HAZOP zastosować do wyznaczania zasobów wrażliwych systemu, które podlegać powinny ochronie. W tym kontekście metod HAZOP dobrze nadaje się do znajdowania zbiorów danych o szczególnym znaczeniu w systemie. Utworzony zgodnie z zleceniami, trzyosobowy zespół, w skład którego weszli: radca prawny, informatyk, urzędnik - użytkownik, przeprowadził częściowe badania systemu. Reszta badań prowadzona była z wykorzystaniem metody SHARD, odmiany HAZOPa, w której badania wykonuje pojedynczy analityk. Celem tego było znalezienie zakresu danych wrażliwych, wobec których znalezione hazardy mogą spowodować straty materialne bądź innej natury (np. naruszenie wartości prawnej). Zgodnie z zaleceniami standardu skoncentrowano się na wyższych warstwach reprezentacji modelu. W toku badań hazardy starano się zidentyfikować z użyciem słów kluczowych *no, more, part of, reverse, other than, early, late, as awell as* o interpretacji zgodnej z podaną w [6]. Dla prezentowanego wyżej podsystemu *Podatek od nieruchomości od osób fizycznych* raport wynikowy zawiera 72 pozycje (9 przepływów razy 8 słów kluczowych). Dla ilustracji przytoczony został fragment tego raportu dla przepływu *dane osobowe podatnika (odczyt)*.

4.2. Badania metodą IT Grundschutz

Z punktu widzenia celu badań najistotniejszym składnikiem wyników było określenie wymagań ochronnych dla aplikacji. Przeprowadzony całościowy audyt dotyczył konkretnego systemu. Model systemu uzupełniony został o pewne dodatkowe składniki, charakterystyczne dla metody, a przedstawione szczegółowo w [28]. Badania prowadzone w UM Piekary Śląskie dotyczyły implementacji aplikacji dla których, jak to wspomniano wcześniej, specyfikacje stanowią akty prawne. W tym zakresie etapy audytu dotyczące określania aplikacji w systemie oraz wyznaczania celu bezpieczeństwa rozpatrywane były

Table 10 HAZOP Study for **Podatek od nieruchomości**							
HAZOP:		Procedura wydania wydania decyzji podatkowej				Description:	
Diagram:		08. Podatek i opłaty lokalne					
Date:							
Leader:		Grzegorz Filipczyk					
Recorder:							
Team Members:		Andrzej Oświęcimski, Teresa Kaszyca					
HAZOP ITEM	INTERCONNECTION	ATTRIBUTE	GUIDE WORD	CAUSE	CONSEQUENCE/ IMPLICATION	INDICATION/ PROTECTION	
9	dane osobowe podatnika, odczyt	data flow	no	brak bazy w wyniku uszkodzenia lub nieuprawnionej modyfikacji	nie można wydać decyzji podatkowej, strata finansowa	archiwum, kopie zapasowe, dziennik operacji	
10	dane osobowe podatnika, odczyt	data flow	more	kilka zapisów dla tej samej osoby	nie można wydać decyzji podatkowej, strata finansowa, ewentualne wydanie zawyżonej lub zaniżonej decyzji	unikalny indeks strukturalny na dane osobowe	
11	dane osobowe podatnika, odczyt	data flow	part of	niepełna informacja w bazie spowodowana nieuprawnioną modyfikacją	wydanie zaniżonej decyzji (na mniej działek niż w rzeczywistości posiada osoba)	podpis cyfrowy zapewnia wykrycie zmian, system kont dostępu	
12	dane osobowe podatnika, odczyt	data flow	reverse	nie występuje			
12	dane osobowe podatnika, odczyt	data flow	other than	informacja błędna, dane osobowe nieprawdziwe	strata finansowa (KPA-kara lub niemożność doręczenia decyzji), wysłanie decyzji do podatnika obcego	weryfikacja w ewidencji ludności	

Rys. 3. Fragment raportu wynikowego z metody HAZOP

Fig. 3. Example results from HAZOP

Aplikacje			Ocena wymagań ochronnych		
Symbol	**Nazwa**	**Dane osobowe**	**Wartość chroniona**	**Stopień protekcji**	**Uzasadnienie**
A1	Qwark, (FK edukacja)	TAK	Poufność	Wysoki	Przechowywane są kompletne dane osobowe objęte ochroną prawną.
			Integralność	Umiarkowany	Istnieje papierowa dokumentacja pozwalająca na korekcję błędów.
			Dostępność	Umiarkowany	Możliwe prowadzenie działalności na dokumentach papierowych przez pewien okres.
.....	.....	.....	.....	.....	.....
A8	**Mipon (podatek od nieruch.)**	**TAK**	**Poufność**	**Umiarkowany**	**Ujawnienie danych osobowych nie narusza integralności osoby; brak znaczącego zagrożenia interesu publicznego.**
			Integralność	**Wysoki**	**Duże straty finansowe w wyniku źle obliczonego podatku**
			Dostępność	**Umiarkowany**	**Istnieją jedynie niewielkie straty finansowe spowodowane opóźnieniem płatności.**
.....	.....	.....	.....	.....	.....
A12	Rejestr (ew. pojazdów)	TAK	Poufność	Umiarkowany	Ujawnienie danych osobowych nie stwarza szczególnego zagrożenia społecznego lub możliwości naruszenia integralności fizycznej osoby.
			Integralność	Umiarkowany	Istnieją mechanizmy kontroli poprawności danych pozwalające na korekcję błędów.
			Dostępność	Umiarkowany	Wszystkie dane przechowywane są w rejestrach pozainformatycznych – możliwe wyłączenia systemu IT na 1 dzień.

Rys. 4. Wymagania ochronne dla aplikacji

Fig. 4. Protection requirements for applications

w kontekście badań jako działanie na modelu logicznym systemu i potraktowane w oderwaniu od rzeczywistego systemu. (m.in. sprzętu i łącz komunikacyjnych). Można tak postąpić zakładając zgodność aplikacji z przepisami prawa, czyli prawdziwość realizowanych funkcji. Efektem przeprowadzonego audytu jest wiele dokumentów składających się na politykę bezpieczeństwa badanego podmiotu. Obszerność tych dokumentów nie pozwala na ich umieszczenie w niniejszym artykule. Powyżej przedstawiony jest fragment raportu z wynikami oceny wymagań ochronnych dla aplikacji, w tym dla podsystemu podatku od nieruchomości.

5. Wnioski

W wyniku badań wykonane zastało studium literaturowe – analiza aktów prawnych stanowiących podstawę działania systemu w urzędzie miasta. Na jej podstawie zbudowany został model strukturalny poddany następnie badaniu z wykorzystaniem metody półformalnej inspekcji dokumentowej HAZOP. Równolegle przeprowadzone zostało badanie metodą IT Grundschutz mające na celu, obok wykonania audytu rzeczywistego systemu UM Piekary Śląskie, określenie wymagań ochronnych dla aplikacji składowych. W toku prac wyodrębnione zostały opisane niżej cechy systemu komputerowego jednostki administracji samorządowej mające wpływ na jego poziom bezpieczeństwa:

- istnieje bardzo znacząca sieć powiązania danych między podsystemami,
- pierwotnym systemem (nie zasilanym danymi z żadnego innego) jest Podsystem Urząd Stanu Cywilnego,
- istnieją trzy kluczowe podsystemy, zasilające w dane większość z pozostałych, są to:
  - ewidencja ludności,
  - ewidencja gruntów,
  - podsystem obiegu dokumentów.

Ze względu na konieczność integracji baz danych i ilość wzajemnych zależności miedzy podsystemami kluczowe znaczenie w procesie zapewnienia bezpieczeństwa mają opisane wyżej efekty dystrybucji i kumulacji. Należy odpowiadać na fundamentalne pytanie o najlepszy z punktu widzenia poziomu bezpieczeństwa stopień integracji podsystemów. Kolejne prace autora dotyczyć będą m.in. tych zagadnień. W tym celu zbudowany model strukturalny posłuży do dalszych badań mających na celu znalezienie opisu ilościowego i jakościowego oraz przeprowadzenie próby stworzenia matematycznego modelu systemu i jego podsystemów. Istotą tych badań byłoby takie modelowanie systemu, by osiągany mierzalny poziom bezpieczeństwa był jak najwyższy.

Kolejną ważną cechą jest fakt, iż nie występują elementy składowe, dla których konieczny byłby bardzo wysoki stopień protekcji. Większość elektronicznych baz danych ma swoje manualne odpowiedniki. Możliwe jest czasowe wstrzymanie przetwarzania elektronicznego i praca „ręczna".

Rozpatrując zagadnienie informacji niejawnych (tajemnic), zauważyć można, że w systemie komputerowym nie przetwarza się informacji o klauzuli wyższej niż służbowa - poufna. Ogranicza to znacznie konieczność stosowania bardzo zaawansowanych mechanizmów bezpieczeństwa, jakie przewidziane są dla informacji z klauzulą tajemnica państwowa.

W odniesieniu do metody HAZOP, w kontekście przeprowadzonych badań, wyciągnąć można kilka ważnych wniosków. Po pierwsze, wyniki badań są tak dobre, jak dobry jest zespół ekspertów. Domniemywać można, że metoda ta powinna być stosowana przez specjalizowane podmioty audytorskie w porozumieniu z użytkownikami systemu. Drugim ważnym wnioskiem jest stwierdzenie faktu, że nie ma gwarancji, iż wszystkie hazardy zostaną wykryte. Nie wiadomo bowiem, czy znalezione zostały wszystkie możliwe interpretacje słów kluczowych w kontekście badanych atrybutów. Pomocne tu są różne reprezentacje formalne – różne spojrzenia na badany system. Poddając inspekcji różne modele zwiększa się możliwości metody. Trzecie spostrzeżenie, zgodnie z sugestiami standardu, wskazuje na potrzebę stosowania także innych metod badania bezpieczeństwa, np. FTA [11] lub FMEA [12], przy czym uznać należy, że badania metodą HAZOP powinny być ich uzupełnieniem, a nie na odwrót.

Obie metody, IT Grundschutz i HAZOP, nie dają wyników w postaci wartości bezwzględnych poziomu bezpieczeństwa. Taka konsekwencja badań została na wstępie zaakceptowana. Należy zauważyć, że badanie dużych, skomplikowanych systemów jest w takim ujęciu zagadnieniem trudnym. Badania określiły kształt systemu w postaci modelu, a wyniki działania HAZOP i IT Grundschutz zaowocowały opisowym określeniem „co i gdzie" należy chronić.

LITERATURA

1. Adamski A.: Prawo karne komputerowe. Wydawnictwo C.H.Beck, Warszawa 2000.
2. Białas A.: Zarządzanie bezpieczeństwem informacji w systemach gospodarki elektronicznej. Studia informatica, Gliwice 2001.
3. Bundesamt fur Sichercheit in der Informationstehnik: IT Grundschutz, October 2000.
4. Defence Standard 00-58 HAZOP Studies on Systems Containing Programmable Electronics Part 2 General Application Guidance. Great Britain Ministry of Defence, 2000.

5. Defence Standard 00-58 HAZOP Studies on Systems Containing Programmable Electronics Part 1 Requirements. Great Britain Ministry of Defence, 2000.
6. Filipczyk G.: Badanie bezpieczeństwa systemu komputerowego metodą HAZOP. Studia informatica, Gliwice 2001.
7. Filipczyk G.: Wybrane zagadnienia ustawowej ochrony danych osobowych na przykładzie problemów występujących w urzędzie miasta. ZN Pol. Śl. s. Informatyka z. 36, Gliwice 1999.
8. Grzywak A.: Bezpieczeństwo systemów komputerowych. Wydawnictwo Pracowni Komputerowych Jacka Skalmierskiego, Gliwice 2000.
9. Jurkowlaniec M., Nowicki B., Redmil F.: Wprowadzenie do metody HAZOP. Informatyka 1997, nr 7-8, s. 24-29.
10. Polska norma PN-I-13335-1, Technika informatyczna: Wytyczne do zarządzenia bezpieczeństwem systemów informatycznych. Polski Komitet Normalizacyjny, 1999.
11. Polska norma PN-IEC 1025, Analiza drzewa niezdatności. Polski Komitet Normalizacyjny, 1994.
12. Polska norma PN-IEC 812, Procedura analizy rodzajów i skutków uszkodzeń. Polski Komitet Normalizacyjny, 1994.
13. Regulamin organizacyjny Urzędu Miasta w Piekarach Śląskich.
14. Rozporządzenie w sprawie instrukcji kancelaryjnej dla organów gmin i związków międzygminnych. Dz.U.1999.112.1319.
15. Rozporządzenie w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Dz.U.1998.80.521.
16. Rozporządzenie w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych. Dz.U.1999.18.162.
17. Trybicka K,. Ziębiński.: Zagadnienia bezpieczeństwa w systemie obiegu informacji multimedialnej Urzędu Miasta Pszów. ZN Pol. Śl. s. Informatyka z. 34, Gliwice 1998.
18. Ustawa dochody jednostek samorządu terytorialnego. Dz.U.1998.150.983.
19. Ustawa finanse publiczne. Dz.U.1998.155.1014.
20. Ustawa gospodarka komunalna. Dz.U.1997.9.43
21. Ustawa kodeks postępowania administracyjnego. Dz.U.2000.98.1071.
22. Ustawa o ochronie danych osobowych. Dz.U.1997.133.883.
23. Ustawa o ochronie informacji niejawnych. Dz.U.1999.11.95.
24. Ustawa o rachunkowości. Dz.U.1994.212.591.
25. Ustawa podatki i opłaty lokalne. Dz.U.1991.9.31.
26. Ustawa zmiana niektórych ustaw określających kompetencje organów administracji publicznej – w związku z reformą ustrojową państwa. Dz.U.1998.106.668.

27. Yourdon E.: Współczesna analiza strukturalna. WNT, Warszawa 1996.
28. Dubiel J.: Realizacja polityki bezpieczeństwa systemu komputerowego jednostki administracji samorządowej. Praca dyplomowa magisterska pod kierunkiem prof. dr hab. A.Grzywaka, Instytut Informatyki, Gliwice 2001.

Recenzent: Dr inż. Andrzej Białas

Wpłynęło do Redakcji 11 kwietnia 2002 r.

Abstract

Computer system security is a still growing problem. There is a need for evaluation of the safety level using formal methodologies. Author concentrates on the town office systems, using laws as the specification for the formal model. The descriptions of the HAZOP and IT Grundschutz methodologies are given. Article contains general model of the system (Fig. 1) and the particular example of one of the subsystems (Fig. 2). Two parts of reports from HAZOP (Fig. 3) and IT Grundschutz (Fig. 4) is given and conclusions made. The results of the researches give the opinion that the most important factor in security modeling is the problem of subsystems integration.