A C T A U N I V E R S I T A T I S L O D Z I E N S I S
FOLIA OECONOMICA 12, 1981

Elżbieta Woźniakowska*

ZAGADNIENIA OCHRONY INFORMACJI W OSOBOWYCH SYSTEMACH INFORMATYCZNYCH ZARZĄDZANIA REGIONEM

Istotą systemu ochrony informacji jest zbudowanie barier zabezpieczających przed niewłaściwym wykorzystaniem, względnie zniszczeniem informacji. Ochrona informacji dysponuje szeregiem środków prawnych, socjologicznych, organizacyjnych i technicznych umożliwiających spełnienie jej funkcji. Rozpatrując to zagadnienie, należy widzieć dwie przyczyny zajmowania się budową systemów zabezpieczających:

- zagrożenie niewłaściwego użycia informacji,
- zagrożenie utraty informacji, w wyniku której może wystąpić niebezpieczeństwo niewykonania zadań przez organizacje.

Informacje, dla których występuje niebezpieczeństwo pierwszego typu, określamy jako poufne lub wręcz tajne, do których bezwzględnie dostęp powinny mieć tylko upoważnione jednostki. Informacje te mogą dotyczyć spraw ogólnospołecznych (gospodarczych, politycznych itp.) oraz poszczególnych członków społeczeństwa. Gdy rozważamy zagadnienie ochrony informacji w osobowych zbiorach danych, wtedy mówimy o konieczności zapewnienia "prywatności".

Istota drugiego typu niebezpieczeństw odnosi się głównie do zagadnienia czasu. Konieczność natychmiastowego podjęcia decyzji lub realizacji nawet zrutynizowanych funkcji może wymagać, by informacja była dostępna natychmiast lub z niewielkim opóźnieniem w stosunku do czasu wystąpienia żądania. Może wystąpić

*Mgr, st. asystent Zakładu Organizacji Przetwarzania Danych UŁ.

trudność dostarczania informacji, gdyż uległa ona zniszczeniu, a odtworzenie jest kłopotliwe ze względu na:

- wiele różnorodnych źródeł pochodzenia informacji;
- dużą liczebność utraconych informacji, która powoduje, że odtworzenie poprzez źródło pierwotne pochodzenia informacji jest bardzo kosztowne i wymaga długiego czasu;
- uzyskanie informacji w żądanej postaci wymaga wielu bardzo skomplikowanych procedur przekształcania.

W systemie przetwarzania informacji zarówno środkami tradycyjnymi, jak i przy wykorzystaniu EMC należy zaplanować i realizować przemyślany system zabezpieczenia, który umożliwiłby prawidłowe działanie we wszystkich warunkach nieprawidłowości.

Wszystkie informacje występujące w systemach informacyjnych czy informatycznych należy zabezpieczać, choć w różnym stopniu. Jeżeli informacja nie wymaga żadnego zabezpieczenia, to znaczy że jest ona zbędna w systemie, i nie ma do spełnienia żadnego zadania.

W systemach informacyjnych (a co się z tym wiąże i w systemach informatycznych) władzy i administracji terenowej zbierane są liczne informacje wymagające zabezpieczenia, stwarzające różne problemy od tych, jakich można oczekiwać w systemach innych jednostek.

Komputeryzacja systemów informacyjnych przebiega także i w sferze zarządzania regionem, stąd należałoby się zastanowić nad niebezpieczeństwami istniejącymi dla informacji. Na to, z jakiego typu niebezpieczeństwami mamy do czynienia, rzutuje rodzaj informacji zbieranej, przechowywanej i wykorzystywanej w jednostce.

Przeprowadzone badania systemu informacyjnego urzędów administracji terenowej[1] wykazały, że zbierane są często bardzo szczegółowe informacje o zasobach i działaniu w regionie.

Dla rozważań nad zagadnieniem ochrony informacji w systemie zarządzania regionem, wybrano informacje o ludności. System informacji o ludności w regionie jest jednym z podstawowych zagadnień, które powinno stać się w pierwszej kolejności przedmiotem

---

[1] Badania w urzędach administracji terenowej stopnia podstawowego i wojewódzkiego prowadził ZOPD UŁ w woj. łódzkim, włocławskim, sieradzkim.

systemu informatycznego. Wynika to chociażby z celu, jaki postawiono przed organami władzy i administracji terenowej, które zgodnie z Konstytucją PRL mają troszczyć się o codzienne potrzeby i interesy ludności oraz zabezpieczać prawa obywateli.

Ważnym zagadnieniem dla rozpatrzenia w przypadku budowy systemu informatycznego o ludności w regionie jest funkcjonowanie systemu informacyjnego w tym zakresie, a następnie sformułowanie koniecznych do rozwiązania problemów dotyczących ochrony informacji.

System informacji o ludności, służący organom władzy i administracji terenowej, charakteryzują następujące własności:

- duże rozproszenie informacji,
- liczne źródła pochodzenia informacji,
- duża liczebność informacji.

Cechy te powodują niejednokrotnie sprzeczności w samych informacjach wynikające z błędów informacji wejściowych, niejednakowego okresu aktualizacji zbiorów.

W systemie informacyjnym urzędów występują informacje rzeczowe i finansowe o ludności charakteryzujące ją jako:

- członków społeczeństwa objętych działalnością odpowiedniego organu władzy i administracji terenowej,
- przedstawicieli urzędu działających w imieniu organów władzy i administracji terenowej i rozliczających się z tymi organami,
- pracowników urzędów administracji terenowej.

Jest sprawą jasną, że informacja o tej samej osobie może znaleźć się w więcej niż w jednej grupie i gromadzona jest przez szereg komórek organizacyjnych urzędu. Komplikuje to system informacyjny, gdyż istotne jest wtedy określenie i realizacja stałych powiązań informacyjnych. Brak powiązań między różnymi dysponentami informacji o tej samej osobie, którzy gromadzą je uwzględniając własne zadania, może być prostą drogą do wystąpienia sprzeczności w informacjach.

Pierwszy typ informacji o ludności stanowią przede wszystkim informacje zbierane w wydziałach (referatach):

- spraw wewnętrznych - podstawowe informacje o całej ludności regionu oraz ludności, która ze względu na typ zadań tych komórek jest tam rejestrowana (sprawy socjalne, sprawy karne);

- oświaty i wychowania - informacje o dzieciach, młodzieży i ich opiekunach;

- komunikacji - informacje o kierowcach różnego typu pojazdów;

- gospodarki mieszkaniowej i spraw lokalowych - informacje o osobach, które w sprawach pomieszczeń kontaktowały się z pracownikami urzędu;

- zatrudnienia i spraw socjalnych - informacje o ludności poszukującej pracy w sektorze uspołecznionym, kadrach wysoko kwalifikowanych;

- rolnictwa, leśnictwa, skupu - informacje o ludności prowadzącej działalność w wymienionym zakresie.

Z przytoczonych informacji wynika, że zbiory dotyczące ludności przewijają się w wielu wydziałach (referatach urzędów). Wrażenie to spotęguje się wówczas, gdy rozpatrzymy pozostałe typy informacji o ludności.

Drugi typ informacji zbierany jest w następujących wydziałach (referatach) urzędów:

- oświaty i wychowania - informacje o kadrze nauczycielskiej szkół ogólnokształcących, podstawowych, szkół zawodowych;

- rolnictwa - informacje o nauczycielach w szkołach rolniczych;

- zdrowia - informacje o nauczycielach w średnich szkołach medycznych;

- kultury, sztuki - informacje o osobach prowadzących działalność w tym zakresie, nie związanych z placówkami o zasięgu ponadregionalnym;

- handlu i usług - informacje o osobach zajmujących się prywatnym handlem lub działalnością usługową;

- komunikacji - informacje o instruktorach prawa jazdy.

Trzeba zwrócić uwagę na bogaty asortyment informacji o ludności znajdujący się w zbiorach komórek zajmujących się finansami w regionie. Prócz wyżej wymienionych informacji o ludności zbierane są także dane o kierownictwie zakładów i instytucji związanych ze sferą gospodarczą. Wynika to z uprawnień o mianowaniu i odwoływaniu kierowników placówek terenowych, które posiadają organa władzy terenowej. W urzędach znaleźć też można podstawowe rejestry dotyczące kierowników placówek o zasięgu ponadregional-

nym, lecz zlokalizowanych na terenie regionu. Głównym dysponentem tego typu informacji są komórki zajmujące się planowaniem, gdyż one wypracowują koncepcję rozwoju regionu ujmującą także zadania jednostek nie podlegających władzom terenowym.

Informacje zbierane o pracownikach nie różnią się niczym od informacji, które posiadają np. jednostki gospodarcze o swych pracownikach i gromadzone są zwykle centralnie w urzędach administracji lub w przypadku wyodrębnienia finansów i księgowości przez odpowiednie komórki.

Trzeba zwrócić uwagę na fakt, że urząd może korzystać nie tylko z informacji zbieranych i przechowywanych we własnych zbiorach, lecz także ze zbiorów nadzorowanych jednostek. Zbiory jednostek podporządkowanych władzom terenowym mogą posiadać bardzo szczegółowe informacje.

Prócz sprawy rodzaju zbieranych informacji istotne są także źródła pochodzenia informacji. Informacje gromadzone w urzędach pochodzą od:

- ludności,
- jednostek podporządkowanych i współpracujących z urzędami,
- pracowników urzędów.

Wymienione są trzy grupy źródeł, lecz kryje się pod tymi hasłami wiele różnorodnych możliwości zasięgania informacji.

Jak widać z przytoczonych informacji, w systemie informacyjnym urzędów zbierane są różnorodne informacje o ludności, które charakteryzują się cechami wymagającymi zabezpieczenia przed zniszczeniem informacji, jak i jej nieprawidłowym użyciem Cechami tymi są: duża szczegółowość informacji, objęcie wielu problemów życia prywatnego ludzi, trudności w odtworzeniu informacji pochodzących z różnych źródeł. Zbierane informacje są podstawą podjęcia decyzji mających wpływ na życie jednostek, a także rozwój społeczno-gospodarczy regionu.

Zbudowanie systemu informatycznego o ludności dla rozwiązywania problemów w tym zakresie przez organa władzy i administracji terenowej wywoła powstanie szeregu problemów z zakresu ochrony informacji specyficznych dla tego systemu i typowych dla systemów także i o innej tematyce.

Ujęcie w systemie informatycznym informacji o ludności wywoła

- skoncentrowanie informacji w jednym miejscu,

- możliwość zbierania informacji bardziej szczegółowo o poszczególnych osobnikach,

- możliwość przechowywania informacji raz zarejestrowanych przez długi czas i stosunkowo łatwy dostęp do nich.

Skutki informatyzacji rozpatrywane są tutaj tylko w aspekcie wpływu na ochronę informacji. Skoncentrowanie informacji wzmaga niebezpieczeństwo zarówno zagubienia informacji, jak i jej niewłaściwego użycia. Grozi to naruszeniem sfery "prywatności" życia jednostek. Zbieranie bardziej szczegółowych informacji pozwoli na dokładniejszą charakterystykę określonego osobnika, ale także nastąpi wzrost niebezpieczeństwa naruszenia granic określonych dla prawa ingerencji w życie prywatne. Na charakterystykę jednostek może wpływać informacja pochodząca z ubiegłego okresu, która w systemach informatycznych jest z reguły (jeżeli istnieje) łatwiej dostępna niż w systemach tradycyjnych. Trzeba jednak zastrzec, że nie wszyscy, którzy mają prawo do uzyskania informacji o jednostce w zbiorach aktualnych, mają także prawo do sięgania do informacji historycznych. Tego typu zastrzeżenia stwarzają dodatkowe problemy dla systemu ochrony informacji.

Stanem idealnym byłoby zabezpieczenie wszystkich informacji w 100%, ale jest to niemożliwe choćby ze względu na koszty rozwiązania. W wielu publikacjach określa się wysokość tych kosztów bardzo różnie[2]. Trzeba niejednokrotnie zrezygnować z rozwiązania idealnego. Różne informacje w systemie będą wymagać różnego zabezpieczenia, np. ze względu na poufność informacji dane o kolizji z prawem będą wymagać staranniejszego zabezpieczenia niż informacja o adresie zamieszkania określonej osoby. Łatwiejsze do odtworzenia mogą być np. informacje o stanie cywilnym osoby niż informacje o opłatach podatkowych. Widać stąd konieczność różnicowania metod zabezpieczających w stosunku do różnych informacji (sięgając aż do informacji elementarnych).

Przy rozważaniach nad kwestią zabezpieczenia informacji w systemie informatycznym o ludności istotne jest rozważanie, które zbiory, a nawet informacje elementarne, należy zabezpieczyć i w

---

[2] J. M a r t i n, Security, accuracy, privacy in computer systems, Englewood Cliffs N. Y. 1973, określa je jako max. ok. 5% kosztu budowy całego systemu informatycznego.

jakim stopniu. Panuje przekonanie[3], że potrzeby zabezpieczenia może wskazać tylko kierownictwo instytucji, dla której jest ten system budowany, gdyż tylko ono zna prawdziwą wartość informacji.

W systemie administracji terenowej istotne jest określenie, kto to kierownictwo stanowi, czy tylko prawnie ustanowiony organ administracji terenowej - wojewoda (prezydent, naczelnik gminy, oraz upoważnione do podejmowania decyzji osoby), czy także kierownicy poszczególnych komórek urzędu. Wydaje się, że ze względu na specyfikę urzędów, szeroki zakres załatwianych spraw - należy przyjąć koncepcję rozszerzonego składu kierownictwa.

Przy rozważaniu sprawy koniecznych zabezpieczeń należy rozpatrzeć kwestię dostarczenia choćby nieco zobiektywizowanych miar i procedur dla określenia wymagań w zakresie ochrony poszczególnych informacji. Przy określeniu wymagań w zakresie ochrony informacji za podstawę przyjmuje się zwykle wielkość ewentualnych strat. W przypadku rozpatrywania systemów o ludności są to straty ponoszone przez instytucję gromadzącą informacje oraz straty osoby, której informacja dotyczy. Część z tych strat (szkód) jest niewymierna, lecz część daje się ująć w jednostkach miary.

Dla (choćby częściowego) rozwiązania problemu określenia wymagań dotyczących stopnia zabezpieczenia poszczególnych informacji w zbiorach dotyczących ludności proponuje się przyjęcie:

- skali strat (A)
- skali czasu bezwładności (B)
- skali prawdopodobieństwa zajścia zdarzenia (ingerencji, zniszczenia) informacji (C)[4].

Skala strat ujmować będzie straty, jakie w jednostkach pieniężnych poniesie osobnik i instytucja w wyniku zagubienia informacji, czy też wykorzystania jej niezgodnie z celem, ze względu na który była zbierana. Przyjmujemy pewne przedziały strat oraz przyporządkowujemy któremuś z nich określoną informację. Na wymagania w stosunku do ochrony informacji wpływa także okres czasu, w jakim system bez ubocznych skutków oczekuje

---

[3] M a r t i n, op. cit.; A. I d ź k i e w i c z, Zabezpieczenie informacji oraz sprzętu jej przetwarzania przed zniszczeniem, uszkodzeniem i nieupoważnionym dostępem, Warszawa 1974.

[4] Zobacz załącznik 1.

na informacje, które w tym czasie mogą być odtworzone. Czas ten niewątpliwie wpływa na rodzaj wybranej metody i co się z tym wiąże - na jej kosztowność. Dla tego zagadnienia można również zbudować skalę czasu bezwładności systemu (okresu, w którym nie ponosimy strat). W skali B przyporządkowujemy każdej informacji jeden z przyjętych przedziałów bezwładności. Ponieważ może wystąpić różny stopień zagrożenia dla informacji (zarówno prawdopodobieństwo zniszczenia, jak i ingerencji w dane) , stąd należy również określić dla każdej informacji prawdopodobieństwo wystąpienia niekorzystnych działań. Można przyjąć pewną skalę, w której jednemu z przyjętych przedziałów zostanie przyporządkowana określona informacja. Przedziały mogą być określone w jednostkach czasowych. Przyporządkowanie do poszczególnych przedziałów może nastąpić np. przez analizę zagrożeń podobnych informacji w innych systemach lub subiektywne odczucie decydenta w sprawie ochrony. Prawdopodobieństwo wystąpienia zagrożenia może w tym przypadku być jednakowe dla wielu informacji, gdy możemy je określić dla całych zbiorów.

Każda z informacji systemu byłaby charakteryzowana przez trzy wielkości ze skal A, B, C. Na podstawie ich można ułożyć listę priorytetową w zakresie ochrony informacji. O pozycji na liście decyduje suma numerów pozycji skal A, B, C. Można oczywiście preferować którąś ze skal, jeżeli wynika to z charakterystyki systemu. Przyjmujemy wtedy wyróżnik dla pozostałych skal 0 (zero), układamy listę dla skali wyróżnionej i dopiero w ramach równych pozycji dokonujemy modyfikacji dla pozostałych skal.

Korzyścią takiego rozważania zagadnienia wymagań w stosunku do ochrony informacji jest rozważenie przynajmniej trzech istotnych elementów wpływających na wybór rozwiązania problemu. Przyjęcie z góry określonych przedziałów pozycji w ramach poszczególnych skal pozwala na porównywalność otrzymanych wyników. Oczywiście trzeba przyjąć skale dające możliwość porównywań, to znaczy że każda skala budowana będzie tak, że wzrastającym numerom pozycji odpowiadać będzie wzrastające wymaganie w stosunku do ochrony i większe straty w jednostkach pieniężnych, mniejszy okres bezwładności, większa częstotliwość występowania. Znaczenie tego typu rozważań wynika z konieczności ograniczenia możliwych zabezpieczeń informacji (chociażby ze względu na koszty). Może

mieć znaczenie ułożenie listy mówiącej o preferencjach w zakresie zabezpieczenia także i wtedy, gdy rozpatrujemy zagadnienie poufności informacji i gdy skala bezwładności mówi o okresie, w którym reagujemy, by nie dopuścić do niekorzystnych sytuacji w przypadku przechwycenia informacji przez nieupoważnionego odbiorcę. W przypadku zniszczenia informacji skala B mówi nam o okresie czasu, w jakim można odzyskać informację bez ponoszenia wysokich strat. Skale te mogą się stać narzędziem kierownictwa komórek dla określenia wymagań w stosunku do zabezpieczenia. Przy rozpatrywaniu systemów o ludności trzeba dokonywać przyporządkowań, rozpatrując zagadnienie z punktu widzenia urzędów i z punktu widzenia rejestrowanych osób. Ponieważ mogą występować duże różnice w pozycjach, należy rozpatrzyć zagadnienie dwukrotnie, wykonać 2 listy priorytetowe i w stosunku do informacji o ludności przyjąć wymagania z punktu widzenia ludności jako podstawowe.

Budując system informatyczny o ludności należy mieć na uwadze wszystkie zasady określane przez W. H. Ware[5], który twierdzi że:

1) nie powinien istnieć system rejestrowania danych personalnych stanowiący tajemnicę;

2) jednostka powinna mieć możliwość ustalenia treści informacji na jej temat i sposobu jej wykorzystania;

3) informacja indywidualna może być użyta w innym celu niż została uzyskana tylko za zgodą osoby zainteresowanej, która powinna mieć możliwość zapobiegania nadużyciom w tym zakresie;

4) jednostka powinna mieć zapewnioną możliwość skorygowania lub zmiany informacji na jej temat;

5) organizacja tworząca i prowadząca rejestr danych personalnych powinna zapewnić ich rzetelność i zapobiegać niewłaściwemu wykorzystaniu informacji.

Duża liczebność i różnorodność zbiorów o ludności istniejących w systemie informacyjnym urzędów rzutuje na konieczność rozważenia wszystkich tych zagadnień. Przy podjęciu decyzji o informatyzacji, potrzeby zabezpieczeń informacji nie należy ograniczać tylko do sfery samego przetwarzania informacji, gdyż bez us-

---

[5] Za M. R. W e s s e l e m, Komputer i społeczeństwo, Warszawa 1976, s. 75-76.

taleń prawnych, zabezpieczenia organizacyjnego i kształtowania świadomości w tym zakresie, zapewnienie bezpieczeństwa procedurom przetwarzania będzie kroplą w morzu koniecznych działań.

Załącznik 1

Skala A

Straty / Informacje	Do 1000 zł	1001-1500 zł	...	...
	1	2	...	n
1. Karalność osoby		x		
.				
.				
.				

Skala B

Czas bezwładności / Informacje	2 miesiące	1 miesiąc	...	...
	1	2	...	n
1. Karalność osoby		x		
.				
.				
.				

Skala C

Częstotliwość występowania zagubienia informacji / Informacje	Raz w roku	Dwa razy w roku	...	...
	1	2	...	n
1. Karalność osoby	x			
.				
.				
.				

Wyróżnikiem dla informacji jest 5; określa on miejsce informacji na liście priorytetowej.

Elżbieta Woźniakowska

PROBLEMS OF INFORMATION PROTECTION IN PERSONAL INFORMATION SYSTEMS OF REGIONAL ADMINISTRATION

In computer-based information systems there is a danger of improper use or loss of information. The significance of this problem grows in the case of issues concerning the population since apart from dangers ensuing from it for institutions there exists a possibility of infringing the "privacy" sphere being ensured for the population.

Data files concerning the population of a given region include very numerous and diversified pieces of information. They of appear in all organizational units subordinated to the local administration organs.

Big quantity of information, its diverse sources, complicated procedures of obtaining output data pose additional requirements in the field of information systems protection. An ideal state (hardly attainable - at least due to high costs of such solution) would be full protection of all information. In the operating information systems the management staff of organizations should define the degree to which particular information should be safeguarded. There should be analyzed the problem of providing measures and procedures for determination of requirements concerning information protection. These requirements are determined by the following factors:

- level of losses incurred as result of drawbacks in the system,
- period of time in which we can counteract improper use of intercepted information or in which it can be made unavailable
- frequency of irregularities.

While discussing problems belonging to the area of information protection, they should not be reduced to data protection sphere alone since without legal provisions, organizational protection, and building proper awareness in this respect protection measures will never be fully effective.