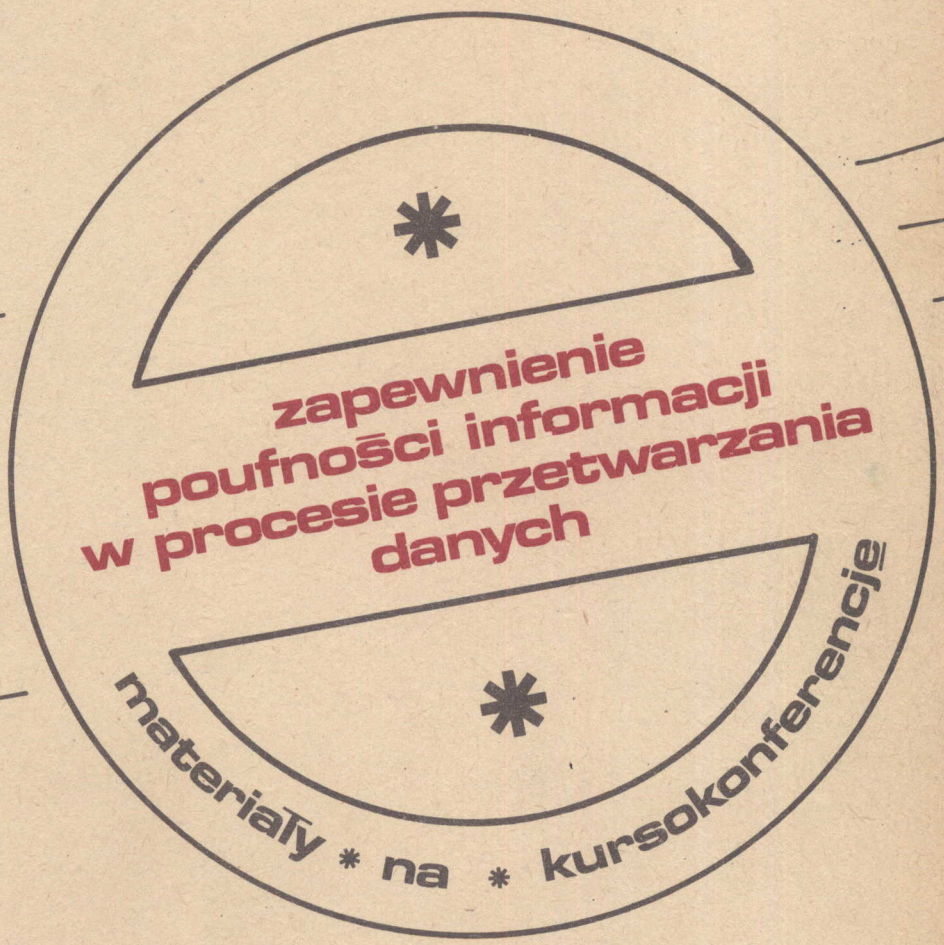
Towarzystwo Naukowe
Organizacji i Kierownictwa
ODDZIAŁ WARSZAWSKI



warszawa 1978

TOWARZYSTWO NAUKOWE ORGANIZACJI I KIEROWNICTWA

ODDZIAŁ WARSZAWSKI

TNOiK

ZAPEWNIENIE POUFNOŚCI INFORMACJI W PROCESIE PRZETWARZANIA DANYCH

(Materiały na kursokonferencję naukową)

Warszawa 1978

I. RADA NAUKOWO-PROGRAMOWA KURSOKONFERENCJI

Przewodniczący - mgr Janusz KOWALSKI
Instytut Organizacji Zarządzania i Doskonalenia kadr,
Wiceprzewodniczący Sekcji Informatyki Oddziału Warszawskiego TNOiK,

Z-ca Przewodniczącego - dr Bronisław OBIREK
Uniwersytet Warszawski
Przewodniczący Komisji Informatyki ZG TNOiK,

Sekretarz Naukowy - mgr Krzysztof MARCINIAK
Ministerstwo Spraw Wewnętrznych
Sekretarz Komisji Informatyki ZG TNOiK,

Członkowie - mgr inż. Zbigniew KOŚCIOŁEK
Centrum Elektroniczne NBP

- dr Stefan SEMCZUK
Ośrodek EPD GUS

- dr Andrzej SOKOŁOWSKI
Wojskowa Akademia Polityczna

- mgr inż. Zdzisław BOGDANOWICZ
Centrum Informatyki HZiGM
Przewodniczący Sekcji Informatyki Oddziału Warszawskiego TNOiK

- inż. Tadeusz JAEGERMANN
Zarząd Mechanizacji i Automatyzacji Obliczeń Statystycznych.

II. KOMITET REDAKCYJNY

1. mgr Janusz Kowalski
2. dr Bronisław Obirek
3. mgr Krzysztof Marciniak

SPIS TREŚCI

WSTĘP

OCHRONA DANYCH I ZAPEWNIENIE POUFNOŚCI INFORMACJI W PROCESIE PRZETWARZANIA DANYCH jest zadaniem tych, którzy zajmują się gromadzeniem danych, ich przygotowaniem do przetwarzania, przetwarzaniem danych, przechowywaniem informacji wynikowych, ich transportem, jak również wykorzystywaniem informacji w zarządzaniu przedsiębiorstwem.

Centralizacja danych i informacji w procesach przetwarzania, wymaga ochrony danych i informacji przed umyślnym lub przypadkowym zniekształcaniem danych lub informacji wynikowych. Potrzeba ta wzrasta wraz ze wzrostem grona użytkowników komputerów, szczególnie w zastosowaniu wielodostępności w przetwarzaniu danych. Wielodostępne systemy informatyczne wymagają wzmożonej, wielostronnej ochrony danych i informacji gromadzonych, przechowywanych, przetwarzanych itp., znajdujących się zarówno w komputerze jak i poza nim.

Zakres ochrony danych i informacji jest bardzo rozległy, a właściwie nie jest jeszcze zdeterminowany, jak również nie jest doceniany.

Komisja Informatyki ZG TNOiK doceniając ten problem zleciła przeprowadzenie wstępnych prac studialnych w zakresie zapewnienia użytkownikom poufności informacji w procesie przetwarzania danych. Mając pierwsze opracowanie o charakterze studialnym, Komisja Informatyki uznała za słuszne przekazanie tych informacji szerokiemu gronu praktyków do wykorzystania w pracy zawodowej.

W tym celu została powołana Rada Naukowo-Programowa Kursokonferencji, która zajęła się organizacją kursokonferencji pozwalającej na wymianę doświadczeń z tego zakresu.

W wyniku pierwszych kontaktów z osobami zajmującymi się omawianą tematyką, udało się przygotować niektóre materiały w formie koreferatów, a to:

1/ Ochrona środowiska informacji - Rola człowieka
2/ Ochrona danych w Głównym Urzędzie Statystycznym
3/ Kontrola danych jako element zabezpieczenia w procesie przetwarzania danych
4/ Prawne aspekty zabezpieczenia informacji.

Rada Naukowo-Programowa Kursokonferencji zdaje sobie sprawę z tego, że zaprezentowany materiał nie wyczerpuje całokształtu zagadnień związanych z zapewnieniem poufności informacji w procesie przetwarzania danych,

ale spodziewa się, że podczas Kursokonferencji można będzie dokonać oceny zaawansowania prac w praktyce.

Ta Kursokonferencja przyczyni się do wymiany doświadczeń między Uczestnikami, a przede wszystkim stanie się przyczynkiem do dalszego, bardziej wnikliwego i kompleksowego zajęcia się sprawami ochrony danych.

Doceniając bogate doświadczenie praktyków i naukowców, Rada Naukowo-Programowa Kursokonferencji zaprasza chętnych do współpracy w tym zakresie /z Komisją Informatyki ZG TNOiK lub pośrednio przez Sekcje Informatyki poszczególnych Oddziałów TNOiK w terenie/.

Żywimy nadzieję, że na Regionalnych Konferencjach Informatyki AMPIG-79 /które będą organizowane przez Oddziały TNOiK w terenie/ lub Krajowej Konferencji Informatyki AMPIG-80 można będzie zaprezentować przedyskutowane w kraju wnioski do realizacji przez poszczególne Ośrodki EPD.

Na zakończenie Rada Naukowo-Programowa Kursokonferencji składa serdeczne podziękowanie inspiratorom tej tematyki, autorom materiałów zaprezentowanych Uczestnikom Kursokonferencji oraz Uczestnikom Kursokonferencji za włączenie się do dyskusji nad problemami nurtującymi szeroki krąg informatyków i użytkowników informacji.

Krzysztof MARCINIAK

ZAPEWNIENIE UŻYTKOWNIKOM POUFNOŚCI INFORMACJI W PROCESIE ELEKTRONICZNEGO PRZETWARZANIA DANYCH

OD AUTORA

Komputeryzacja różnych dziedzin ludzkiej działalności przestała być hipotezą. Odpowiedź na pytanie: komputery - tak, czy nie ? - dawno już została sformułowana, i jest to odpowiedź twierdząca. Była ona efektem tzw. czystej przesłanki, a mianowicie konieczności. Gdyby sprawdzić w statystykach, to okazało by się, że przedziały czasowe w których liczba informacji na świecie podwaja się, wykazują stałą tendencję malejącą. Zbieranie, przetwarzanie, a następnie magazynowanie takiej liczby informacji za pomocą tradycyjnego zapisu, stało się po prostu niemożliwe.

Skala komputeryzacji i charakter zastosowań elektronicznych maszyn cyfrowych zmusza dziś do zwrócenia uwagi na zagadnienie zabezpieczenia eksploatacji systemów informatycznych i ochrony danych przed nieupoważnionym dostępem, zniszczeniem lub sprzeniewierzeniem. Społeczeństwa krajów w których technika komputerowa jest wysoko rozwinięta doskonale znają wypadki oszustw oraz działań powodujących niszczenie informacji zmagazynowanej i przetwarzanej w elektronicznej maszynie cyfrowej. Wynika to między innymi z charakteru stosunków ekonomicznych, gdzie element konkurencyjności wymaga tajności informacji. W związku z tym wielu wybitnych teoretyków i praktyków z krajów zachodnich pracuje obecnie nad stworzeniem środków i metod zabezpieczających przetwarzanie danych. Oblicza się, że każde wyprzedzenie o rok prac badawczych nad tym problemem skróciłoby dystans między rozwojem maszyn cyfrowych, a metodami ochrony informacji o około 3 lata [1/].

W krajach socjalistycznych, w tym także w Polsce, nie prowadzi się praktycznie badań nad tym zagadnieniem. Upoważnia to do stwierdzenia, że jesteśmy dopiero na etapie przekonywania użytkowników i producentów o celowości podjęcia takiej pracy. Dla ośrodków obliczeniowych dużych przedsiębiorstw przemysłowych, ośrodków bankowych, wojskowych, urzędów centralnych, problem bezpieczeństwa danych stanowi jedno z ważniejszych zadań. Społeczeństwa będą budować systemy spełniające różne funkcje - intelektualne, ekonomiczne i społeczne, a systemy te z kolei wywrą głęboki wpływ na kształtowanie przebiegu ludzkiego życia. Sprzężenie między tymi przed -

1/ Por. O. W e i a m a n n, Sicherung in der Zukunft, Datenverarbeitung nr 5, 1976

miotem użyteczności publicznej, a społeczeństwem, jest tak silne, że samo społeczeństwo jest obecnie częścią tego systemu. Systemy maszyn łącznie z ludźmi stworzą nowe usługi, instytucje, środowisko i nowe problemy - np. problemy natury etycznej. W jaki sposób kontrolowany będzie dostęp do tego urządzenia ? Kto będzie regulował jego wykorzystanie ? Do jakich celów system będzie wykorzystywany i jak można zabezpieczyć się przed jego nadużywaniem ? 2/

2/ Por. Zbiór artykułów "Scientific American", Dziś i jutro maszyn cyfrowych, PWN, Warszawa 1960

1. Znaczenie zabezpieczenia zbiorów na tle rozwoju zastosowań systemów informatycznych

1.1. Istota zabezpieczenia informacji

Przez zabezpieczenie rozumieć należy zapewnienie dyspozycyjności, sprawności, nienaruszalności i poufności wszelkiego działania wykorzystującego ETO [3]. Inaczej, zabezpieczenie polega na stworzeniu skutecznych metod pozwalających na ochronę informacji nie tylko przed wypadkami losowymi, ale przede wszystkim przed świadomymi próbami zniekształcenia i niszczenia zbiorów danych.

System zabezpieczenia powinien stanowić integralną część każdego systemu informatycznego. Warto w tym miejscu przytoczyć wypowiedź przedstawiciela firmy IBM W.H.M u r r a y'a, który podczas obrad konferencji Europejskiego Programu Badawczego Diebolda w Wiedniu /marzec 1972/ powiedział: "Bezpieczeństwo to - zadania kierownictwa, obejmujące dbanie o dokładność i nienaruszalność informacji potrzebnej do prowadzenia przedsiębiorstwa, o poufność i niedostępność wrażliwych danych, o ochronę instalacji obliczeniowej przed katastrofami, niewłaściwym użyciem itp., o ustrzeżenie pracowników przed pokusą, a kierownictwa przed nieprzezornością. Bezpieczeństwo musi zapewniać przetrwanie przez przedsiębiorstwo wszelkich katastrof i kontynuację realizacji zadań. Bezpieczeństwo musi współzawodniczyć z innymi zadaniami kierownictwa o zasoby i musi być osiągalne w ten sam sposób jak zysk. Należy więc patrzeć na nie jako na funkcję operacyjną, liniową, a nie sztabową" [4].

Podstawowym pytaniem przy podejmowaniu prac nad zabezpieczeniem systemu, jest pytanie: "Co chcemy chronić i jaką wartość stanowi dla nas zabezpieczona informacja" ? Upraszczając nieco problem - jakie nakłady opłaca się ponieść, żeby nasza informacja miała zagwarantowane bezpieczeństwo ? Rzadko w ośrodkach przeprowadza się sumienną analizę stopnia wrażliwości systemu informatycznego na możliwość jego infiltracji. Często kończy się tylko na przeprowadzaniu analizy. A przecież chodzi o to, aby wypracować racjonalny program ochrony określonego systemu. Jedną z istniejących przyczyn, utrudniającą stworzenie takiego programu jest brak świadomości, jakie to jest ważne. Systemy informatyczne stanowią jeszcze pewną

3/ Por.A.I d ź k i e w i c z Zabezpieczenie informacji oraz sprzętu jej przetwarzania przed zniszczeniem, uszkodzeniem i nieupoważnionym dostępem, Problemy Informatyki, Warszawa 1974

4/ Por.Europejski Program Badaczy Diebolda, Przeglądy kontrolne systemów, OBRI nr 40, 1973

nowość. W wielu wypadkach trwa jeszcze fascynacja sprzętem, potencjalnymi możliwościami jego wykorzystania. Powoduje to w efekcie zajmowanie takiego stanowiska, które eliminuje w instytucji wprowadzającej lub eksploatującej system informatyczny, niektóre techniki kontroli systemu, oparte na założeniu, że komputer się nie myli.

Informacja, począwszy od dokumentu źródłowego, przez nośnik maszynowy, a skończywszy na magnetycznym nośniku danych, przebywa w wielu miejscach i mają do niej dostęp różne osoby. W związku z tym nie wystarczy chronić tylko pomieszczenia komputera, łączy transmisji danych, lub wreszcie samego procesu przetwarzania danych, lecz należy uwzględnić cały system.

W przypadku eksploatacji systemu informatycznego na terenie jednego zamkniętego obiektu, elementami systemu, które mogą być potencjalnie narażone na infiltrację będą:

- budynek, w którym znajduje się EMC,
- pamięć operacyjna,
- pamięci zewnętrzne /dyski, taśmy, bębny, karty magnetyczne/,
- urządzenia wejścia /czytniki, konsole/,
- urządzenia wyjścia /drukarka, perforator taśmy/,
- biblioteka zbiorów danych,
- personel.

W warunkach systemu wielodostępnego, do wymienionych elementów dochodzą zupełnie nowe, takie jak:

- komputer telekomunikacyjny,
- linie transmisyjne,
- urządzenie końcowe /terminale/,
- użytkownicy.

Problem zabezpieczenia w warunkach systemu wielodostępnego nabiera szczególnego znaczenia, ponieważ potencjalny obszar infiltracji powiększa się o dodatkowe elementy. Szczególnie łatwo jest podłączyć się do linii transmisyjnych, a to dla odmiany jest bardzo trudne. Specjalnego zabezpieczenia wymaga terminal. Zainstalowany u użytkownika umożliwia dostęp do systemu nowej grupie osób. Nie jest sprawą tylko użytkownika, aby dostęp do końcówki miały upoważnione osoby. Jest to także sprawa kierownictwa ośrodka obliczeniowego.

Jak zatem widać ewolucja systemów komputerowych nakłada nowe zadania na służby zajmujące się ich zabezpieczeniem.

1.2. Rodzaje zabezpieczenia sprzętu i danych

Stosowane obecnie i będące przedmiotem najnowszych badań naukowych i eksperymentów metody zabezpieczeń można podzielić na cztery zasadnicze grupy:

- metody organizacyjne,
- metody techniczne,
- metody programowe,
- metody prawne.

Przedstawiony graficznie /rys. 1/ podział metod ochrony danych w porównaniu z innymi prezentowanymi w literaturze ma swoje istotne cechy 5/ Uwzględnia bowiem oprócz trzech grup podstawowych grupę czwartą - aspekt ochrony prawnej systemów informatycznych. Jest to wynik światowych tendencji w tej dziedzinie. Od niedawna w krajach Europy Zachodniej, Stanach Zjednoczonych i Związku Radzieckim prowadzi się prace nad objęciem działalności informatycznej przepisami prawnymi, sankcjonującymi tę działalność i dbającymi o prawidłowe jej funkcjonowanie. Z zadowoleniem należy przyjąć fakt, że w maju 1976 r. odbyła się we Wrocławiu konferencja naukowa poświęcona tym zagadnieniom 6/.

1.2.1. Metody organizacyjne

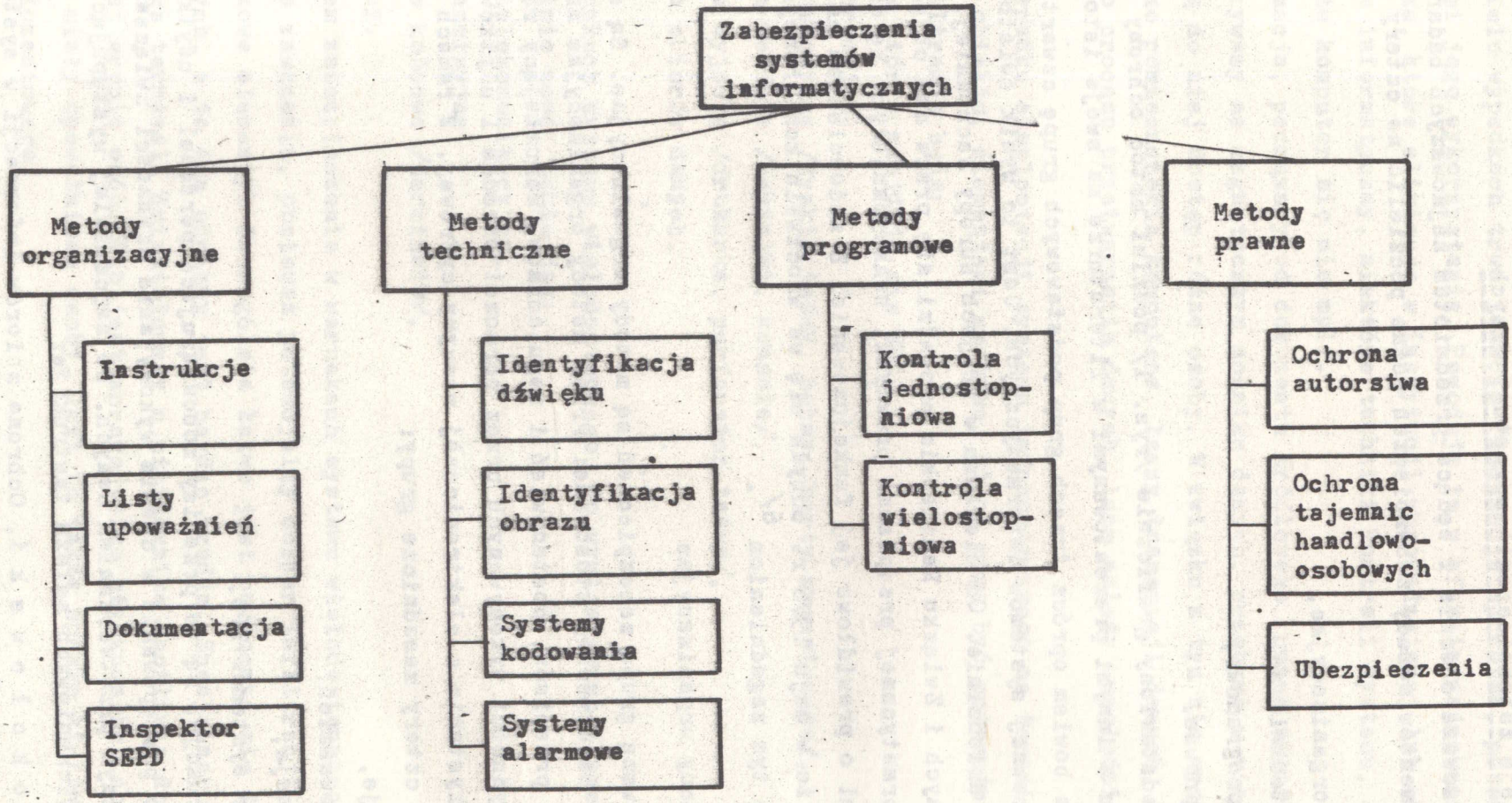
Pierwszą grupą zabezpieczeń są metody organizacyjne. Są one w chwili obecnej najczęściej stosowane. Przez metody organizacyjne należy rozumieć zbiór przepisów, postanowień i regulaminów, warunkujący realizację zespołu czynności wykonywanych przez personel ośrodka i użytkownika w czasie korzystania z elektronicznej maszyny cyfrowej. W ramach tej metody wyróżniamy cztery zasadnicze grupy:

- instrukcje,
- listy upoważnień,
- dokumentacja,
- inspektor systemów EPD.

Instrukcje, są to przepisy zobowiązujące personel i użytkownika do określonego postępowania w czasie wykonywania czynności związanych z elektronicznym przetwarzaniem danych. Do najczęściej występujących w ośrodkach obliczeniowych należą instrukcje:

5/ Por.A.S o k o ł o w s k i, Ochrona zbiorów informacji w systemach informatycznych, Informatyka nr 12, 1973

6/ Por.A.T a r g o w s k i, Polscy prawnicy o informatyce, Informatyka nr 9, 1976



Rys. 1 Podział metod zabezpieczenia danych

- eksploatacji i przechowywania materiałów magnetycznych,
- obsługi sprzętu komputerowego,
- postępowania z tajnymi wydrukami,
- prowadzenia dokumentacji systemowych,
- o trybie sporządzania raportów specjalnych,
- regulujące zasady transportu danych /jeśli są one przemieszczane między różnymi, oddalonymi od siebie obiektami/,
- awaryjne na wypadek zagrożenia pożarem, zalaniem itp.,
- prowadzenia archiwów.

Nie są to wszystkie instrukcje występujące w ośrodkach. Nazwa każdej z nich jednoznacznie wskazuje na zawartość treści i przeznaczenie. Chcemy zwrócić szczególną uwagę na fakt jak postępować, żeby instrukcja była dobra i spełniała cele dla jakich ją stworzono.

Przede wszystkim należy ustalić czego instrukcja ma dotyczyć. Dokładnie określić zasięg instrukcji, bo to pozwoli w przyszłości uniknąć nieporozumień związanych z lukami w instrukcji, wynikającymi ze zbytniego zawężenia lub nadmiernego jej rozszerzenia. Instrukcja powinna jednoznacznie uściślać co i w jakim trybie reguluje. Musi być napisana poprawnie stylistycznie, bez nazw obcego pochodzenia, tak aby była czytelna i zrozumiała dla kierownictwa i personelu zasadniczego. Instrukcja powinna dotyczyć tylko najistotniejszych zagadnień, Często instrukcje powodują biurokratyzowanie działalności. Nie mogą one komplikować pracy w centrum obliczeniowym i zmuszać do powoływania nowych służb administracyjnych, lecz muszą przyczyniać się do uproszczenia i ułatwienia postępowania w kwestiach, które regulują.

Przez listy upoważnień rozumieć będziemy podział kompetencji w odniesieniu do wykonywania poszczególnych czynności w przetwarzaniu danych. W praktyce oznacza to np., że osoba mająca dostęp do jednych zbiorów, będzie miała zabroniony dostęp do innych.

W systemie wielodostępnym, kiedy użytkownik zgłasza się do systemu przetwarzającego na bieżąco, bierze się pod uwagę jego upoważnienie. Będzie ono zależeć od przeszkolenia, stanowiska w przedsiębiorstwie oraz konieczności względu do zbiorów w związku z wykonywaną pracą. Upoważnienie może dawać mu prawo dostępu do zbiorów w celu ich aktualizacji, lub tylko w celu odczytania danych. Na przykład użytkownik może mieć zezwolenie na dostęp do zbioru zawierającego dane personalne, lecz nie na dokonywanie w nim zmian. Może on otrzymywać nazwiska i adresy określonych osób, lecz może być dla niego niedozwolone przeglądanie ich zawodów, lub

zarobków. Fakt wykorzystania upoważnienia powinien być odnotowany w rejestrze dostępów, łącznie z jego charakterystyką. Rejestr ten może być nieocenioną pomocą dla inspektora ochrony w czasie dokonywania przez niego inspekcji oraz w przypadku konieczności rekonstrukcji zbioru.

Listy upoważnień są bardzo istotnym elementem zabezpieczenia, ponieważ są związane z czynnikiem ludzkim będącym najczulszym miejscem ochrony każdego systemu.

Ważnym środkiem kontroli i zabezpieczenia każdego systemu jest właściwa dokumentacja. Największe niedociągnięcia zdarzają się w dokumentacji programów komputera. A właśnie te programy są najważniejszym elementem systemu, są częścią, w której mają miejsce bieżące transakcje, rejestracje, aktualizacje i które są najbardziej narażone na niepożądane działanie. Odtworzenie faktów warunkuje dobra dokumentacja.

Cała dokumentacja to w rzeczywistości księga, której poszczególne rozdziały interesują ludzi zajmujących się określonymi pracami. Każdy z rozdziałów powinien stanowić osobną całość, do której mają dostęp upoważnieni do tego pracownicy. Na przykład operator, mając własny rozdział lub podręcznik nie potrzebuje zaglądać do podręcznika programisty, a w zasadzie nawet nie powinien.

Stanowisko inspektora systemu do spraw zabezpieczenia jest praktycznie nieznane w polskich ośrodkach obliczeniowych. Czego można od niego oczekiwać i jakie powinien spełniać warunki ?

Inspektor zajmujący się zabezpieczeniem powinien udzielać porad dotyczących możliwych i niezbędnych technik ochrony, które mają być wprowadzone do systemu w czasie jego projektowania. Stąd wniosek, że inspektor systemów EPD powinien doskonale znać nie tylko techniki zabezpieczające, ale także powinien być programistą i projektantem. To pozwala wyczuć słabe punkty systemu już na etapie projektowania.

Siły powietrzne USA oraz przedsiębiorstwo AT nad T pierwsze w 1958r zaangażowały specjalistów APD zajmujących się zabezpieczeniem systemów i stworzyły odpowiednie komórki. AT and T utworzyło taką komórkę w ramach przedsiębiorstwa Bell Telephone Laboratories 7/. Specjaliści ci koncentrowali się na problemach ochrony i kontrolowania systemów EPD. Są oni specjalistami poszukiwanymi. W Polsce w związku ze wzrostem parku komputerowego i powszechnością dostępu do maszyn, działalność inspektora staje się obiektywną koniecznością.

7/ Por. Europejski Program Badawczy Diebolda, wyd.cyt.

Do zalet metod organizacyjnych zaliczyć należy:
- niekomplikowanie zasadniczego procesu przetwarzania danych,
- niewydłużanie czasu pracy komputera,
- niestosowanie nakładów finansowych,
- łatwość przyswojenia zasad przez personel.

Natomiast do wad tych metod zaliczamy:
- brak zabezpieczenia w czasie pracy maszyn,
- mała skuteczność wyłącznego jej stosowania.

1.2.2. Metody techniczne

Przez zabezpieczenia techniczne rozumieć będziemy stosowanie urządzeń technicznych i układów technicznych, sprzężonych z komputerem, mających możliwość skutecznego działania przeciwko ingerencji osoby nieupoważnionej [8/].

Układy techniczne można podzielić na następujące urządzenia:
- identyfikujące dźwięk,
- identyfikujące obrazy,
- do procesu kodowania i dekodowania,
- alarmujące.

Zespół urządzeń i środków przeznaczonych do rozpoznawania mowy przyjęto nazywać systemem automatycznego rozpoznawania mowy /ARM/. Zadaniem tego systemu jest rozpoznanie informacji zawartej w sygnale mowy oraz zidentyfikowanie osoby wysyłającej sygnał. Jakkolwiek uniwersalne systemy ARM powinny w zasadzie rozpoznawać mowę ludzką, przekazywaną do urządzenia przez różne osoby bez ograniczeń dotyczących liczby rozpoznawanych wyrazów i sposobów wymawiania, to z punktu widzenia zabezpieczenia można zrezygnować z pewnych wymagań. W naszym przypadku mogą być przydatne systemy rozpoznające pewien ograniczony zbiór haseł, natomiast bezbłędnie rozróżniające autora hasła.

Nie będziemy tutaj omawiać ani sposobu działania takiego urządzenia, ani przykładów kto i gdzie stosował tego typu urządzenia. Zainteresowanych odsyłamy do konkretnych publikacji [9/].

Wystarczy powiedzieć, że w chwili obecnej możliwe jest skonstruowanie urządzenia rozpoznającego ograniczoną liczbę słów /kilkadziesiąt do kilkuset/ z dokładnością zbliżoną do 100 %. Ze względu jednak na duże koszty budowy takich urządzeń oraz ich małą elastyczność /przystosowanie

8/ Por.A.S o k o ł o w s k i, wyd.cyt.

9/ Por.E.S a w i c k a, Automatyczne rozpoznawanie mowy, Elektroniczna Technika Obliczeniowa nr 4, 1974

urządzenia do jednej osoby mówiącej/ nie są one dotychczas rozpowszechnione.

Niektórzy specjaliści zachodni przewidują skonstruowanie pod koniec lat siedemdziesiątych systemu zdolnego do rozpoznawania prawie wszystkich słów języka angielskiego z dokładnością zbliżoną do 100 %. Dalszy postęp jest uzależniony od rozwiązania następujących problemów:

- wyboru cech wyróżniających /dystynktywnych/,
- normalizacji i segmentacji sygnału,
- opracowania optymalnych wzorów rozpoznawczych sygnałów,
- wyboru najbardziej optymalnych algorytmów porównania podejmowania decyzji.

Urządzenia utożsamiające obrazy graficzne są właściwie, tak samo jak identyfikujące mowę, w fazie eksperymentów. Szczególnym zainteresowaniem cieszą się propozycje budowy urządzenia identyfikującego linie papilarne. Działa ono na podobnych zasadach jak urządzenie utożsamiające znaki alfanumeryczne, obrazy figur i rysunków. Skonstruowanie urządzenia dopuszczającego człowieka do komputera dopiero po uprzednim zidentyfikowaniu jego linii papilarnych zrewolucjonizowałyby techniki zabezpieczenia. Zainteresowanych tym problemem odsyłamy do literatury zajmującej się tym zagadnieniem.

Trzecią grupę urządzeń należącą do technicznych metod zabezpieczenia systemów stanowią urządzenia kodujące i dekodujące. Są to najczęściej specjalne układy sprzężone z komputerem, działające jako urządzenia wejścia lub wyjścia. Kodery i dekodery /bo tak należy je nazywać/ powodują, że informacje wprowadzane lub wyprowadzane z maszyny zmieniają swoją notację na zupełnie nieczytelną dla jej odbiorcy. Prawdziwy odbiorca, dysponujący dekoderem, ma możliwość prawidłowego ich odczytu. Dla osoby nieuprawnionej pozostaną one niewiele znaczącym ciągiem niezidentyfikowanych znaków.

Metoda ta jest najczęściej stosowana. Jest stosunkowo prosta i nie wymaga dużych nakładów finansowych. Zasadniczym zarzutem stawianym tej metodzie jest fakt, że wydłuża proces przetwarzania danych. Wydaje się jednak, że w sytuacji kiedy wartość informacji wymaga specjalnych środków ochrony, warto ponosić tego typu kłopoty.

Czwartą grupą urządzeń są urządzenia alarmowe, sygnalizujące niebezpieczeństwo przez wywołanie sygnału świetlnego lub dźwiękowego.

Do grupy tej należą różnego rodzaju czujniki termiczne, które w wypadku podwyższonej temperatury uruchamiają urządzenie alarmowe informujące załogę ośrodka o grożącym niebezpieczeństwie.

W wielu ośrodkach na zachodzie, gdzie przechowuje się i przetwarza informacje wyjątkowo ważne, stosuje się także telewizję przemysłową. Dyżurujący personel sekcji zabezpieczenia danych obserwuje na monitorach czynności wykonywane w pomieszczeniu EMC. Specjalne czujniki elektryczne dbają o to, aby osoby przebywające w pobliżu komputera nie miały przy sobie przedmiotów wpływających na jego pracę /np. magnes/.

Urządzenia alarmujące przeciwpożarowe lub probierze wilgotności powietrza powinny stanowić podstawowe wyposażenie ośrodków obliczeniowych, natomiast telewizja przemysłowa i fotokomórki różnego typu mogą, ze względu na swoje wysokie koszty, być stosowane tylko tam gdzie są naprawdę niezbędne.

Do zalet układów technicznych możemy zaliczyć:
- skuteczność i ciągłość działania danego urządzenia w czasie ochrony informacji,
- objęcie działaniem wszystkich eksploatowanych systemów,
- "długowieczność" urządzeń.

Do wad zaliczamy:
- ochronę tylko na niektórych etapach przetwarzania,
- wysoki koszt urządzenia,
- wydłużenie czasu pracy komputera.

1.2.3. Metody programowe

Zabezpieczenie programowe definiuje się jako stworzenie w ramach programów systemowych lub użytkowych specjalnych procedur weryfikujących prawo dostępu do zbiorów danych w czasie przetwarzania. Zaletą tej metody jest fakt, że komputer sprawdza, czy dana osoba może, i w jakim zakresie, korzystać ze zbiorów danych.

Stosowane obecnie procedury programowe można podzielić na: jedno - stopniowe i wielostopniowe.

Włączenie do programu zasadniczego przetwarzania danych procedury jednostopniowej powoduje, że przed otwarciem zbiorów, na monitorze poja - wia się komunikat żądający podania hasła lub odpowiednich parametrów.

W czasie przerwania programu należy wprowadzić odpowiednie informacje z konsoli operatorskiej lub monitora. W wypadku kiedy hasło nie zostanie wprowadzone lub zostanie wprowadzone błędnie, nastąpi blokada programu uniemożliwiająca otwarcie zbiorów i przetwarzanie danych.

Procedury wielostopniowe działają na tej samej zasadzie z tą tylko różnicą, że częstotliwość ich występowania w programie jest większa. Wy-

gląda to tak, że program, ustaloną ilość razy sprawdza prawidłowość hasła w różnych częściach programu. Od programisty zależy, w którym miejscu pro gramu zadysponuje działanie tych procedur. Zbytnie przeciążenie takimi procedurami prowadzi do wydłużenia czasu przetwarzania i skomplikowania prostych programów.

Do zalet metod programowych zaliczyć możemy:

- łatwość ich konstrukcji,
- małe nakłady finansowe,
- możliwość częstych zmian haseł i parametrów,
- realizowanie czynności zabezpieczających przez komputer,
- działanie ochrony danych w czasie pracy maszyny cyfrowej.

Wady tych metod to przede wszystkim:

- wydłużenie czasu przetwarzania,
- niebezpieczeństwo zgubienia lub zapomnienia haseł i parametrów.

1.2.4. Metody prawne

Artykuł 23 kodeksu cywilnego mówi że: dobra osobiste człowieka, jak zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizeru nek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska pozostają pod ochroną prawa niezależnie od ochrony przewidzianej w innych przepisach /o środkach ochrony jest mowa w art. 24 KC/. Ponadto szkody wynikające z systemów ewiden cji osobowych mogą być regulowane przepisami artykułu 417 kodeksu cywilne go [10/].

Zagadnienia te budzą od dawna zainteresowanie na świecie. Liczne in formatyczne systemy osobowe, samorzutnie rozwijane, budzą obawę, że może być naruszone prawo swobód obywatelskich. Przykładowo, dane o zawarciu małżeństwa lub o rodzicach przysposobionego dziecka mają usankcjonowaną prawnie cechę poufności.

W ramach ochrony prawnej ważnym zagadnieniem jest ochrona prawno-pa tentowa oprogramowania. W licznych publikacjach zagranicznych wskazuje się na potrzebę stworzenia takich przepisów prawnych. W USA podjęto kroki w sprawie uregulowania tego zagadnienia [11/].

Zjawiskami występującymi przy ochronie tajemnic handlowo-przemysło-

wych są:

10/ Por. Kodeks postępowania cywilnego, Wydawnictwo Prawnicze, Warszawa 1974

11/ Por. Ochrona prawna oprogramowania w krajach zachodnich, Informatyka nr 3,4,5, 1977

- istnienie nieujawnionego obiektu ochrony,
- przedstawienie go odnośnym czynnikom z zastrzeżeniem poufności,
- korzystanie bez upoważnienia z przedmiotu ochrony.

Ochrona tajemnic handlowo-przemysłowych jest stosowana przy programach komputerowych ze względu na nie ujawnianie tajemnic wbrew woli twórcy oraz na niewielkie koszty.

Analizując informacje pochodzące z innych państw należy podkreślić ich znaczenie w Polsce. Wydaje się, że w przypadku programów komputerowych najodpowiedniejszą formą będzie kombinacja ochrony autorstwa przez prawo cywilne z ochroną tajemnicy handlowej i przemysłowej. Trzeba się jednak liczyć z trudnościami administracyjnymi i proceduralno-prawnymi. Nie ulega bowiem wątpliwości, że oprogramowanie komputerów stanowi szczególną formę własności intelektualnej i przemysłowej, a więc musi się znaleźć mechanizm prawny zapewniający mu odpowiednią ochronę.

Program ochrony powinien obejmować także polisę ubezpieczeniową w celu:

- zapewnienia funduszów na naprawę lub odkupienie urządzeń odtworzenia zbiorów oraz pokrycia zwiększonych kosztów związanych z przetwarzaniem awaryjnym,
- zwrotu kosztów osobom trzecim z powodu niemożności wykonania usług przetwarzania /np. kary umowne/,
- pokrycia strat związanych z przerwą w przetwarzaniu.

Ustalenie sum związanych z funduszami na naprawę jest łatwe. Szczególną uwagę należy zwrócić na koszty wymiany urządzeń łącznie z urządzeniami towarzyszącymi, takimi jak instalacja klimatyzacyjna oraz przewidzieć koszty ewentualnych napraw budynków.

Warto zaznaczyć, że PZU w Polsce dotychczas nie zawiera umów na ubezpieczenia ośrodków obliczeniowych, poza normalnym ubezpieczeniem majątkowym od pożaru, powodzi i innych katastrof żywiołowych.

Jako zalety metod prawnych można wymienić:

- fakt istnienia kontroli państwa nad działalnością informatyczną,
- wskazanie dróg egzekwowania odpowiedzialności,
- stworzenia podstaw kompleksowego programu badań problematyki zabezpieczenia eksploatacji systemów informatycznych.

Trudno określić wady takich metod. Należy chyba mówić o trudnościach ich wprowadzenia. Są to:

- trudności administracyjne,
- ochrona prawna jest skierowana nie na zabezpieczenie samego komputera, ale na kształtowanie ludzkiej świadomości i odpowiedzialności.

1.3. Rodzaje infiltracji zbiorów danych

Jak już poprzednio wspomniano, prawie wszystkie elementy systemu informatycznego narażone są na infiltrację. Istnieją trzy rodzaje infiltracji: przypadkowa, pasywna i aktywna.

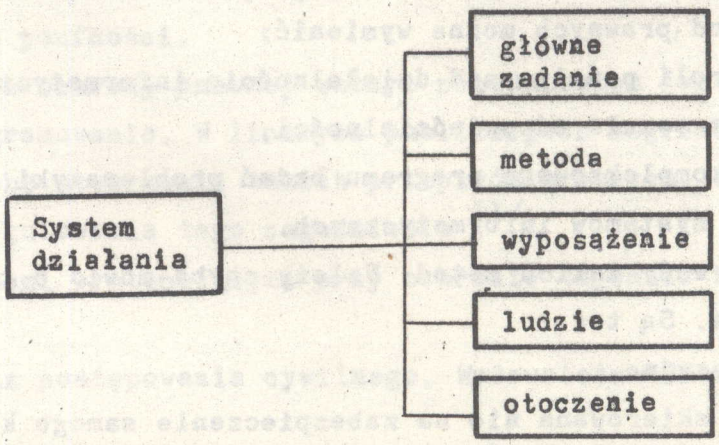
Pierwsza z nich polega na docieraniu informacji do osób nieupoważnionych /awaria terminatu, zły podział pamięci/. Przyczyną takiej przypadkowej infiltracji może być również nieświadome, niewłaściwe postępowanie personelu obsługującego lub użytkownika. Skutki tego mogą być poważne.

Znane są przypadki kiedy właściciel terminalu otrzymywał z pamięci maszyny dane, które absolutnie nie stanowiły przedmiotu jego zainteresowań. Zły podział pamięci, błędne jej stronicowanie sprawiło,że odczytywane i transmitowane dane dotyczyły zupełnie innych zbiorów zajmujących sąsiednie miejsce w pamięci.

Infiltracja pasywna ma miejsce wtedy, gdy ktoś usiłuje przyłączyć się do linii transmisji danych, ograniczając się do odczytywania danych. O tego rodzaju infiltracji mówimy również, wtedy gdy ktoś bada i kopiuje tabulogrgmy lub całe zbiory informacji w czasie transmisji.

I wreszcie infiltracja aktywna, najbardziej niebezpieczna i w największym stopniu dezorganizująca proces przetwarzania danych, polega na uzyskiwaniu świadomego dostępu do systemu celem konwersacji i zadawania pytań. Może ona polegać na wykorzystywaniu znajomości hasła rzeczywistego użytkownika. Fałszywa aktualizacja, wymazywanie poszczególnych danych, celowe przekłamania, nie wyczerpują listy możliwych sposobów tej infiltracji.

Nie ulega wątpliwości, że każda z tych infiltracji w mniejszym lub większym stopniu powoduje zakłócenie prawidłowości przetwarzania, rzetelności wyników, co w efekcie jest podstawą błędnych decyzji i dalszych konsekwencji.



Rys. 2 Układ systemu działania

2. Metodologiczne podstawy projektowania systemu zabezpieczenia danych

2.1. Charakterystyka systemu działania

Do systemów działania należy zaliczyć projektowanie systemu zabezpieczenia przed nieupoważnionym dostępem do danych w ośrodku EPD, według G.Nadlera składa się zawsze z tych samych elementów.

Pierwszym elementem charakteryzującym system działania jest jego główne zadanie, co w wyniku funkcjonowania ma zostać osiągnięte. W naszym przypadku jest to skuteczna ochrona systemu informatycznego.

Drugim elementem jest metoda zabezpieczenia, mająca zagwarantować realizację celu, dla którego system jest projektowany. Metoda ta określa potrzebne środki, czyli wyposażenie systemu - stanowiące trzeci element charakterystyki - obejmujące przemieszczenia, urządzenia, narzędzia i materiały pomocnicze biorące udział w zabezpieczeniu danych. Czwarty element - to ludzie, którzy należą do układu zabezpieczającego i zabezpieczanego, posługujący się jego wyposażeniem i realizacją procesu zabezpieczenia. Wszystko to dzieje się w otoczeniu, które jest ostatnim, piątym elementem charakterystyki.

2.2. Strategia projektowania

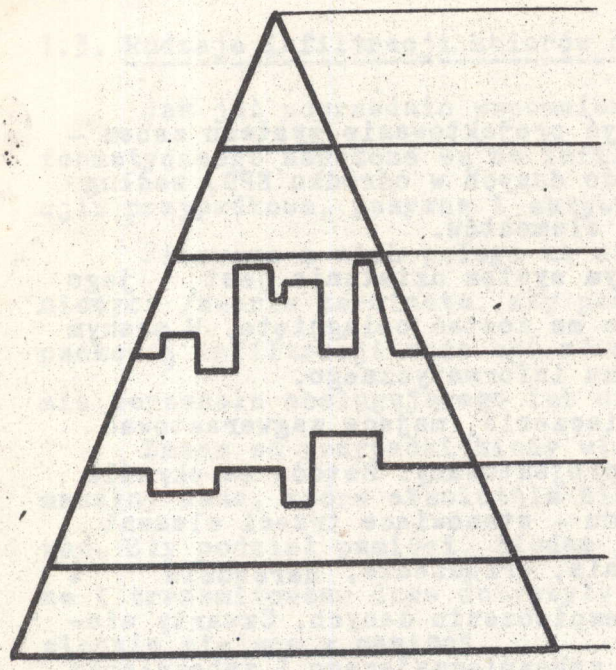
Przedstawiamy tutaj koncepcję rozwiązania idealnego, sformułowaną przez G.Nadlera. Co to jest idealny system zabezpieczenia ? Jest to system zabezpieczenia zbudowany na podstawie rozwiązania idealnego, które ma zapewnić spełnienie głównego zadania w tych warunkach, tj. bez ograniczeń i bez przeszkód.

Rozróżnia się trzy poziomy rozwiązania idealnego systemu zabezpieczenia, przedstawione na rys. 3.

Pierwszy poziom stanowi teoretycznie idealne rozwiązanie, które nie wymaga ponoszenia żadnych kosztów. Jest to oczywiście ideał nieosiągalny. W praktyce tym ideałem może być rozwiązanie jakiegoś problemu w ten sposób, że zadanie rozpatrywanego systemu zabezpieczenia danych staje się w ogóle zbędne i można je pominąć.

Drugi poziom to rozwiązanie idealne perspektywiczne, wykonalne dopiero po przeprowadzeniu pewnych badań naukowych lub prac rozwojowych.

Ostatni poziom to rozwiązanie idealne wykonalne technicznie w najdogodniejszych warunkach, w których nie istniałyby żadne ograniczenia. Na



Rys. 3 Poziomy rozwiązania idealnego systemu zabezpieczenia według G.Nadlera

podstawie koncepcji systemu idealnego, wykonalnego technicznie, opracowuje się projekt techniczny.

2.3. Etapy współdziałania przy projektowaniu

Wyróżniamy trzy zasadnicze etapy:

- wstępny, pozwalający poznać potrzeby i możliwości ich zaspokojenia,
- projektowania technicznego przedsięwzięcia,
- realizacji systemu zabezpieczenia tj. jego budowy, rozruchu i wdrażania.

W każdym z tych etapów można wyodrębnić wiele faz postępowania, spośród których nie wszystkie należą do strefy projektowania. Jednak projektant musi mieć pełną świadomość swojej działalności w ramach całego cyklu zorganizowanego postępowania. Można powiedzieć, że przechodząc przez kolejne stadia, rola i udział projektanta /w stosunku do zleceniodawcy i użytkownika systemu zabezpieczanego/ wzrasta, osiągając swój szczyt podczas projektowania technicznego, a w ostatnim etapie sprowadza się do nadzoru autorskiego.

2.3.1. Etap wstępny, rozpoznawczy

Etap ten obejmuje następujące fazy:

- wstępnego sformułowania określonych potrzeb z zamiarem ich zaspokojenia,
- sformułowania zadania projektowego,
- wstępnego projektowania systemu zabezpieczenia,
- podjęcia decyzji kontynuacji cyklu postępowania.

Za treść, przebieg i wynik etapu rozpoznawczego wyłączną odpowiedzialność ponosi zleceniodawca, który może skorzystać z usług projektanta tylko w zakresie projektowania wstępnego systemu zabezpieczenia. Często zdarza się jednak, że zleceniodawca potrzebuje pomocy z zewnątrz przy formułowaniu samego zadania projektowego, świadczy to, niestety o słabości kadry kierowniczej zabezpieczanego systemu.

2.3.1.1. Sformułowanie potrzeb z zamiarem ich zaspokojenia

Uświadomienie sobie potrzeb stanowi obowiązek liniowego kierownictwa. Nikt nie może ich z tego obowiązku zwolnić.

Systemy zabezpieczenia, obsługujące te potrzeby mogą:
- jeszcze nie funkcjonować, gdyż pojawiły się zupełnie nowe zadania, np. na skutek zakupu nowej maszyny, wdrożenia nowych systemów informatycznych,
- funkcjonować zadawalająco, nie stwarzając żadnych problemów,
- funkcjonować niezadawalająco, wywołując niezadowolenie na terenie instytucji lub u jednostek nadrzędnych.

2.3.1.2. Sformułowanie zadania projektowego

Każde złożone przedsięwzięcie, a takim jest projektowanie systemu zabezpieczenia danych przed nieupoważnionym dostępem, wymaga zaplanowania lub zaprojektowania jego realizacji. Z chwilą, gdy nastąpił podział pracy między liniowym kierownikiem formułującym cele, a specjalistycznym zespołem projektującym ochronę danych, etap ujęcia zadania projektowego staje się niezbędny. Zadanie to obejmuje:
- wybór metody zabezpieczenia,
- określenie głównego zadania systemu zabezpieczenia,
- określenie wymagań, postulatów i ograniczeń nałożonych na rozwiązanie problemu,
- wyodrębnienie sfery działania systemu z otoczenia,
- sformułowanie kryterium oceny realizacji zadania, a zarazem opracowywanego projektu,
- ewentualny podział na systemy funkcjonalne.

Celem wyboru metody zabezpieczenia jest ustalenie w danym momencie najlepszego wariantu odpowiadającego wartości informacji, warunków jej eksploatacji i przechowywania.

Decydujące znaczenie dla formy i treści przyszłych rozwiązań ma wyodrębnienie w sformułowaniu głównego zadania tylko tych elementów, które rozstrzygają o jego istocie, przy założeniu, że wszystkie pozostałe po

stulaty będą przeniesione do listy wymagań i warunków ograniczających rozwiązanie. Poprawne sformułowanie głównego zadania projektowego nie powinno określać sposobu jego realizacji, aby nie zwalniać projektanta od poszukiwania najlepszego rozwiązania.

Fakt, że główne zadanie projektanta systemu zabezpieczenia danych stanowi część zadań całości, nakłada pewne dodatkowe wymagania i ograniczenia na przyszłe rozwiązanie. Ograniczenia te lub wymagania, mogą dotyczyć jednego lub kilku elementów charakterystyki systemu ochrony w różnych aspektach. Postulaty, wymagania i ograniczenia nałożone na projektowany system mogą być sformułowane w postaci określonych relacji, jak i funkcji matematycznych wiążących pewne elementy charakterystyki systemu. W celu pozostawienia projektantowi swobody w działaniu, liczba ograniczeń nałożonych na badany system powinna być jak najmniejsza i wszystko, co nie zasadnicze, odrzucone.

Chcąc, aby określenie obiektu projektowania było precyzyjne, powinno się system zabezpieczenia oraz jego sferę działania wyodrębnić z otoczenia przedmiotowo, czasowo i przestrzennie. Przedmiotowe wyodrębnienie sfery działania systemu jest zwykle zawarte w głównym zadaniu projektowym. Wyodrębnienie okresu eksploatacji pozwala realistycznie spojrzeć na wymagania i warunki ograniczające rozwiązanie systemu. Wyodrębnienie przestrzenne projektowanego systemu w miarę możliwości nie powinno być określane bezwzględnie, lecz jedynie względnie - w odniesieniu do innych obiektów otoczenia.

Następną fazą przy formułowaniu zadania jest opracowanie syntetycznego kryterium oceny jakości rozwiązania. W wypadku systemu zabezpieczenia jest nim skuteczność ochrony dostępu do danych.

Ostatnią fazą jest podział systemu na podsystemy. Podział ten ma miejsce tylko w wypadku złożoności projektowanego systemu zabezpieczenia przy wdrażaniu i eksploatacji oraz przy daleko posuniętej względnej niezależności jego podsystemów. Podsystemy uważa się za niezależne, jeśli można dla nich sformułować mierzalne główne zadanie.

2.3.1.3. Projektowanie wstępne

Projektowanie wstępne, opierające się na koncepcji idealnego rozwiązania, przebiega w następujących fazach:

- poszukiwanie rozwiązania idealnego,
- zebranie informacji o rzeczywistych warunkach działania projektowanego systemu,

- opracowanie wariantów rozwiązań przystosowanych do rzeczywistych warunków,
- wybór rozwiązania projektowanego systemu,
- opracowanie założeń techniczno-ekonomicznych projektowanego systemu.

2.3.1.4. Podjęcie decyzji

Założenia techniczno-ekonomiczne systemu zabezpieczenia są podstawą do podjęcia przez zleceniodawcę decyzji o realizacji, pozwalają bowiem ocenić efektywność przedsięwzięcia. Pełną odpowiedzialność za podjętą decyzję /pozytywną lub negatywną/ ponosi kierownik jednostki zlecającej. Błędnej decyzji nie można tłumaczyć brakiem wiedzy fachowej w konkretnej dziedzinie, niesolidnością zespołu projektantów itd. Renoma firmy projektującej ma także niemałe znaczenie przy udzielaniu zlecenia na opracowanie założeń techniczno-ekonomicznych.

2.3.2. Projektowanie techniczne

Projektowanie techniczne przedsięwzięcia stanowi stadium, w którym rola i odpowiedzialność projektanta jest decydująca. Szczegółowe założenia części systemu zabezpieczenia, będącej przedmiotem opracowania technicznego, powinny zawierać wszystkie parametry systemu, terminy, rozkłady w czasie, ogólny schemat działania oraz warunki techniczne i organizacyjne eksploatacji. Faza ta ma zabezpieczyć zgodność koncepcji autora projektu technicznego wybranej części systemu zabezpieczenia z koncepcją całości i potrzebami użytkowników. Stąd szczegółowe założenia podlegają uzgodnieniu z przyszłym użytkownikiem lub z generalnym projektantem całego systemu /gdy nie ma jeszcze konkretnego użytkownika/.

W fazie projektowania technicznego następuje techniczne określenie wymaganych parametrów, opracowanie schematu operacyjnego działania potrzebnych środków, założeń metodycznych dla środków zabezpieczenia oraz projektów funkcji przygotowawczych, rozruchowych i eksploatacyjnych wraz z dokładną charakterystyką techniczno-ekonomiczną.

Poprzednio opracowane założenia metodyczne zostają w fazie programowania zastąpione dokumentacją archiwalną i eksploatacyjną wchodzącą w skład projektu technicznego.

2.3.3. Realizacja systemu zabezpieczenia danych

Realizacja tj. przygotowanie, rozruch i wdrażanie zaprojektowanego systemu zabezpieczenia danych przed nieupoważnionym dostępem, odbywa się na podstawie dokumentacji przygotowawczej, rozruchowej i eksploatacyjnej

opracowanej w stadium projektowania technicznego i zatwierdzonej do realizacji. Zleceniodawca lub przyszły użytkownik często nie chcą wypowiadać się na temat jakości projektu technicznego wykorzystując fakt, że za projekt techniczny pełną odpowiedzialność ponosi projektant. Z tego względu wykonawca sam obowiązany jest zweryfikować i zatwierdzić projekt techniczny do realizacji.

Przygotowanie, rozruch i wdrażanie każdej wyodrębnionej części systemu zabezpieczenia obejmują przygotowanie warunków technicznych /np. wybudowanie obiektu, zainstalowanie urządzeń/ i organizacyjnych elementów jego funkcjonowania, instruktaż oraz wykonanie czynności przewidzianych instrukcjami przygotowawczymi i rozruchowymi, próbną eksploatację wyników, tzw. rewizję dokumentacji archiwalnej i eksploatacyjnej systemu zabezpieczenia oraz zatwierdzenie systemu do systematycznej eksploatacji. Autorzy projektu są zobowiązani do sprawowania nadzoru w czasie przygotowania, rozruchu i wdrażania systemu, aż do uzyskania wyników przewidzianych projektem. Obowiązuje ich to wówczas, gdy użytkownik spełnił określone wymagania techniczne i eksploatacyjne.

3. Kierunki zastosowań systemów zabezpieczenia danych

Trudno dziś wymienić dziedzinę, która oparłaby się choćby próbom komputeryzacji. Maszyna cyfrowa, jako narzędzie człowieka współczesnego stała się miernikiem postępu i nowoczesności. Perspektywy, jakie otworzyło masowe i umiejętne stosowanie maszyn cyfrowych we wszystkich dziedzinach życia społecznego, są rezultatem nowego sposobu myślenia, w którym twórcze możliwości człowieka są sprzęgnięte z logiczną potęgą maszyny. Daje to w efekcie wyniki, których samodzielnie ani człowiek, ani maszyna, nie są w stanie osiągnąć.

Wzrost liczby informacji na całym świecie spowodował powstanie problemu jej przetwarzania i przechowywania. Tym celom służy przede wszystkim elektroniczna technika obliczeniowa. Informacje można klasyfikować według różnych kryteriów. Jednym z tych kryteriów jest problem tajności przechowywanych danych. Oznacza to, że tylko określona grupa ludzi ma dostęp do pewnych informacji. Praca w takich systemach informatycznych, w których przedmiotem przetwarzania są informacje tajne, narzuca na system i jego organizację pewne nowe jakościowo wymagania i ograniczenia. Wbrew pozorom, dziedzin, w których wymagane jest zabezpieczenie danych, jest

bardzo dużo. Przede wszystkim instytucje wojskowe, urzędy centralne gromadzące dane z zakresu gospodarki, ewidencji ludności, urzędy statystyczne, placówki naukowo-badawcze, instytuty naukowe, przedsiębiorstwa przemysłowe o specyficznym asortymencie produkcji, służba zdrowia magazynująca dane o diagnozach i przebiegach leczenia pacjentów itd. Wykorzystanie tych informacji dla innych niż ich przeznaczenie celów, mogłoby przynieść straty nie tylko jednostce będącej w ich posiadaniu, ale także w skali całego kraju. Zwłaszcza przy stosowaniu systemów wielodostępnych, wyposażonych w teletransmisję danych.

Specjaliści amerykańscy udowodnili, że liczba usiłowań nieupoważnionych dostępów do zbiorów informacji była w funkcyjnej zależności z liczbą funkcjonujących komputerów. Wraz ze wzrostem liczby elektronicznych maszyn cyfrowych wzrastała liczba niedozwolonych seansów dostępu do danych. Ostatnio tezę tę potwierdzili przedstawiciele Anglii, Szwecji, Francji, RFN, a także Jugosławii[12/]. Ze względu na znikomą liczbę systemów wieldostępnych, nie prowadzono podobnych badań w Polsce.

Nie oznacza to jednak, i byłoby błędem tak sądzić, że próby takie nie będą miały miejsca w niedalekiej już przyszłości, kiedy narzędzie, jakim jest komputer stanie się bardziej powszechne.

3.1. Automatyzacja zarządzania

Większość maszyn cyfrowych zainstalowanych obecnie na świecie jest stosowana do automatyzacji zarządzania. Ocenia się, że właśnie tego rodzaju zastosowania są najbardziej opłacalne z ekonomicznego punktu widzenia. Zarządzać można oddziałem fabrycznym, gałęzią przemysłu, armią, badaniami naukowymi w skali całego kraju, czy wreszcie - państwem. Wraz ze wzrostem złożoności zarządzanego organizmu wzrasta liczba informacji.

W krajach kapitalistycznych problem zabezpieczenia danych przed nieupoważnionym dostępem w zarządzaniu jest jednym z pierwszoplanowych problemów. Przedsiębiorstwa strzegą swoich technologii, dystrybucji, list odbiorców, dostawców. W obawie przed konkurencją stosuje się najbardziej wyrafinowane systemy ochrony i zabezpieczenia. Chroni się też dane zmagazynowane w pamięciach maszyn przed przestępczą działalnością personelu i użytkowników. Zabezpiecza się przed włamaniami, kradzieżami, klęskami żywiołowymi.

12/ Por.H.K a l t z, Ohne Sicherung, Informatik nr 7, 1973

Świat finansów także od dawna stosuje komputery w bankach, towarzystwach ubezpieczeniowych i na giełdach. Wiele kas pożyczkowych rejestrujących wpłaty i wypłaty doświadczyło nieuczciwego postępowania swoich klientów, którzy, mając dostęp do systemu, za pomocą programowych zabiegów powodowali znaczne straty finansowe.

W sferach przemysłowych jednym z pionierów rozwoju systemów zabezpieczeń danych jest przedsiębiorstwo Lockheed Missiles And Space. Jego ośrodek obliczeniowy w Sunnyvale w Kalifornii pracuje jako system automatycznego zbierania danych. Ośrodek zbiera informacje o pracy ponad 200 zakładów przemysłowych rozmieszczonych w promieniu ponad 500 km. System rejestruje i kieruje ruchem ponad 200 tysięcy różnych wyrobów produkowanych lub magazynowanych w tych zakładach. Maszyna cyfrowa tego systemu ma także połączenia z 25 placówkami, z których na żądanie można bezzwłocznie otrzymać informacje o zlokalizowaniu magazynu, zlecenia zakupu, stanie zapasów i kosztach robocizny. Od 1969 r. do 1975 r. przedsiębiorstwo z tytułu nieupoważnionych podłączeń do systemu teletransmisji, zniszczenia zbiorów straciło blisko 3 mln. dolarów.

Do najbardziej zaawansowanych obecnie w stosowaniu ochrony danych zaliczyć trzeba także koncern Westinghouse Electric. Jego zdalnie wykorzystywany ośrodek obliczeniowy w Pittsburgu był ośrodkiem nerwowym całego koncernu. W 1972 r. ponad połowa zbiorów danych spłonęła w wyniku pożaru, którego powodem była wadliwie, od kilku lat, działająca aparatura klimatyzacyjna. Zniszczeniu uległy raporty informacyjnego zarządzania kasą, które ewidencjonowały wpływy i wydatki różnych oddziałów Westinghouse. Odszkodowania dla klientów w wysokości 4 mln dolarów stanowiły tylko część strat.

Co oznaczają te zdarzenia dla elektronicznej techniki obliczeniowej i społeczeństw, którym ona służy ? Wydaje się, że organizacje funkcjonować będą sprawniej, lepiej i wydajniej, pod warunkiem zwracania większej uwagi na problem zabezpieczenia eksploatacji systemów informatycznych i strzeżenia ich przed nieupoważnionym dostępem do danych.

3.2. Służba zdrowia

Coraz większa liczba komputerów zostaje instalowana w służbie zdrowia. Maszyny cyfrowe tworzą ogromne banki danych, zawierające informacje o lekach, diagnozach chorób pacjentów, przebiegu leczenia itd. Kwestia pomyłek lub prób świadomych infiltracji zbiorów może pociągnąć w konsekwen-

cji tragiczne skutki w postaci śmierci pacjentów włącznie. Zrozumiałe zatem staje się specjalne zabezpieczenie dostępu do danych tego typu.

W paryskiej klinice chorób zakaźnych w systemie komputerowym rejestrowane były przebiegi leczenia pacjentów chorych na żółtaczkę, odrę i szkarlatynę. Dostęp do maszyny cyfrowej mieli tylko lekarze odpowiednio przeszkoleni w zakresie posługiwania się bazą danych. Nieodpowiedzialna decyzja jednego lekarza, który dopuścił do danych nieupoważnioną pielęgniarkę, której nieumiejętność posługiwania się końcówką spowodowała, że część danych została wymazana, a dane dotyczące dozowania leków dotyczyły innego pacjenta. Efektem tego nieodpowiedzialnego i pełnego ignorancji postępowania były ciężkie powikłania chorobowe pacjentów.

Hamburski Instytut Mikrobiologii prowadził badania nad składnikami krwi osób będących dawcami krwi. Wyniki badań i analiz rejestrowane były w specjalnie zaprojektowanym systemie informatycznym. Dostęp do danych o rodzajach krwi będących w dyspozycji banku miał zespół z oddziału chirurgicznego. Zespół ten korzystał z tych informacji przed zaplanowanymi operacjami, zabezpieczając sobie przygotowanie odpowiedniej grupy krwi do operacji. Pracownik ośrodka obliczeniowego, jako wyraz swojego niezadowolenia z prowadzonej polityki płacowej kierownictwa, spowodował magnesem skasowanie dużej liczby danych zapisanych na taśmach magnetycznych. W rezultacie zespół chirurgów miał poważne kłopoty w czasie operacji, kiedy trzeba było przetoczyć krew i to w większej ilości.

Przedstawione wypadki doskonale ilustrują skutki braku należytej ochrony danych.

Komputery w medycynie to nie tylko bierna rola ewidencjonowania danych. Maszyny cyfrowe są w stanie prowadzić tzw. kontrolę czynną. Automatyczne doglądanie pacjenta polega na pomiarze ważniejszych parametrów świadczących o stanie chorego, takich jak temperatura, ciśnienie krwi, oddech, elektryczna aktywność serca itd. Czujniki pomiarowe, zainstalowane na ciele chorego, są połączone przewodowo z różnego rodzaju aparaturą pomiarową, a ta z kolei jest połączona z maszyną cyfrową. Jedna maszyna może obsługiwać w ten sposób kilkudziesięciu pacjentów. Otrzymuje ona od poszczególnych instrumentów wartości wszystkich istotnych parametrów, dotyczących każdego z chorych objętych opieką, porównuje te wartości z wartościami dopuszczalnymi, a następnie analizuje jak te wartości zmieniają się w czasie. Na podstawie interpretacji pomiarów maszyna wykrywa sytuacje odbiegające od normy lub groźne i natychmiast wysyła sygnał ostrzegawczy do personelu medycznego, podając nazwisko pacjenta, wypisując informacje z przyrządów oraz wskazując na te elementy, które wydały się jej

niepokojące. Szczególnie przydatna bywa maszyna cyfrowa w czasie operacji. Otrzymuje ona z sali operacyjnej wszelkie informacje od czujników zainstalowanych na ciele chorego, a swe własne informacje przesyła lekarzom za pomocą monitora ekranowego ustawionego przy stole operacyjnym. W czasie operacji nowotworu mózgu maszyna analizuje zdjęcia rentgenowskie czaszki pacjenta, ustala na tej podstawie dokładną lokalizację nowotworu i tak steruje ustawienie elektrod, aby było możliwe precyzyjne zniszczenie zdegenerowanej tkanki za pomocą energii fal elektromagnetycznych.

Z przedstawionych opisów wynika, jak skomplikowane i odpowiedzialne procesy powierza się elektronicznej maszynie cyfrowej. Nakłada to na jej dysponentów nowe jakościowo wymagania. Cała sfera działalności maszyny wraz z bliższym i dalszym otoczeniem wymaga ciągłego procesu ochrony danych przed wypadkami losowymi i nieupoważnionym dostępem.

3.3. Badania naukowe

Obliczenia naukowo-techniczne były historycznie pierwszą dziedziną zastosowań maszyn cyfrowych. Badania naukowe, jako pierwsze z dziedzin zastosowań komputerów doświadczyły konsekwencji nieupoważnionego dostępu do danych. W 1962 r. amerykańska firma Flever Company, produkująca samoloty sportowe nie ustrzegła się przed podstępną działalnością konkurencyjnej firmy, której agenci dokonali przekłamań w obliczeniach przez podłączenie się do łączy teletransmisji. Efekt tej działalności doprowadził do kilku katastrof lotniczych, w których zginęło 6 osób.

Postęp nauk fizycznych w dużej mierze wynikał z rozwoju i udoskonalenia metod eksperymentowania. W eksperymencie przeprowadzanym w laboratorium manipuluje się zazwyczaj próbką materii dla zaobserwowania zmian, jakie powstają w niej pod wpływem sztucznych oddziaływań. Cały eksperyment musi się odbywać w starannie kontrolowanych warunkach, aby przede wszystkim nie spowodować reakcji zagrażającej ludzkiemu życiu oraz aby uniezależnić się od wpływu czynników przypadkowych. Tego rodzaju badania są przeprowadzane w celu studiowania budowy materii w laboratoriach wyposażonych w potężne akceleratory. Podobny charakter mają badania przeprowadzane przez biochemików zajmujących się reakcjami chemicznymi zachodzącymi w żywych organizmach.

W Instytucie Fizyki Nuklearnej w Londynie prowadzono w 1974 r. eksperymentalne badania dotyczące stopnia odporności komórek mózgowych człowieka na napromieniowanie. Uzyskane poprzednio dane do badań zostały zagu

bione. Ośrodek nie posiadał dodatkowych kopii. Zdecydowano się kontynuować eksperyment przy zdekompletowanych danych i nie uzyskano zadawalających wyników. Eksperci stwierdzili, że gdyby był pełny zestaw danych, eksperyment miał pełne szanse powodzenia. Nie trzeba uzasadniać, jak droga jest eksploatacja i sprzęt naukowo-badawczy. W związku z tym nie można sobie pozwolić na niedopatrzenie jakim było niezabezpieczenie kopii danych.

Badania przestrzeni kosmicznej i prace z zakresu konstrukcji pojazdów kosmicznych od samego początku wykorzystują elektroniczną technikę obliczeniową. Wynika to przede wszystkim z zapotrzebowania na wyniki o najwyższym stopniu dokładności pozbawione elementu przypadkowości.

Zaprezentowane przykłady dziedzin w których komputery znalazły zastosowanie i powstała konieczność ochrony danych przed zniszczeniem lub nieupoważnionym dostępem, nie wyczerpują problemu.

Właściwie można postawić tezę, że wszystkie systemy informatyczne wymagają odpowiedniej ochrony. Odpowiedniej, to znaczy dostosowanej do wartości przechowywanych informacji, prawdopodobieństwa infiltracji zbiorów i innych czynników, które dokładnie musi przeanalizować użytkownik za nim zdecyduje się wprowadzić system zabezpieczenia.

4. Założenia programowe zabezpieczenia przed nieupoważnionym dostępem do zbiorów

4.1. Zadania i przedmiot zabezpieczenia

Pewien instytut naukowy, prowadzący ważne badania eksperymentalne, postanowił wykorzystać w swojej pracy elektroniczną maszynę cyfrową. Kierownictwo instytutu, zdając sobie sprawę z faktu, że większość badań posiadać będzie klauzulę tajności uznała za konieczne skorzystać z usług wyspecjalizowanego zespołu projektantów systemów zabezpieczenia danych w ośrodkach EPD. Zawarto w tym celu specjalną umowę, która określała warunki współpracy i wymagania użytkownika.

Pierwszą czynnością, jaką uczynił zespół projektantów było dokładne zaznajomienie się z charakterem pracy w instytucie oraz potrzebami tej placówki związanymi ze stosowaniami elektronicznej techniki obliczeniowej.

Znajomość obiektu jest podstawowym i koniecznym warunkiem, aby system zabezpieczenia spełniał należycie swoją rolę. W tym też celu do zespołu projektującego włączono przedstawiciela instytutu. W toku dyskusji

z przedstawicielami instytutu zdefiniowano dokładnie przedmiot zabezpieczenia i zadanie, jakie system zabezpieczenia danych ma spełniać.

Przedmiotem zabezpieczenia miał być komputer wraz ze swoim pomieszczeniem, personelem oraz stacjami zdalnego dostępu. Zadania stawiane przed systemem wymagają:

- uniemożliwienia dostępu osobom nieupoważnionym do danych przetwarzanych w ośrodku oraz do urządzeń końcowych,
- zabezpieczenia urządzeń i pomieszczeń przed pożarem i zalaniem wodą.

4.2. Warunki eksploatacji

Kolejnym etapem pracy zespołu projektującego system zabezpieczenia danych jest dokładne zaznajomienie się z warunkami, w jakich będą eksploatowane systemy informatyczne. Dla tego zespołu duże znaczenie mają informacje o:

- technologii przetwarzania danych,
- zmianowości pracy w ośrodku elektronicznym,
- liczbie personelu i podziale kompetencji,
- zasadach prowadzenia biblioteki zbiorów,
- listach użytkowników maszyny cyfrowej,
- potrzebach użytkowników w zakresie korzystania z elektronicznej maszyny cyfrowej.

Technologia przetwarzania danych stanowi istotny element w zabezpieczeniu dostępu do danych. Trzeba wiedzieć, jak wygląda obieg dokumentów, począwszy od dokumentu źródłowego, przez maszynowy nośnik informacji, do wydruku z drukarki komputera.

Równie istotny jest zestaw urządzeń komputerowych. Dla projektantów nie jest obojętne czy pamięci zewnętrzne maszyny są pamięciami taśmowymi czy też pamięciami dyskowymi, oraz czy ośrodek ma stacje kart magnetycznych.

Projektanci muszą wiedzieć, jaki jest system operacyjny, ponieważ właśnie on dokonuje dystrybucji pamięci operacyjnej, organizuje dostęp urządzeń końcowych, a więc wykonuje czynności, które stanowią newralgiczny punkt każdego systemu. Istotną rzeczą jest także rodzaj łączy między komputerem a urządzeniami końcowymi. W zależności od tego czy łącza są komutowane, czy dzierżawione, zostanie obrana odpowiednia strategia zabezpieczenia łączy transmisji danych.

Jeśli ośrodek pracuje w systemie pracy zmianowej, należy dokładnie znać rodzaje prac, wykonywanych na poszczególnych zmianach, czas trwania zmian i ich personalną obsadę.

Ważnym problemem w działalności każdego ośrodka obliczeniowego jest przechowywanie i zasady użytkowania nośników informacji. W bibliotekach znajdują się najczęściej zbiory na taśmach magnetycznych, dyskach oraz ta bulogramy. Istotną więc rzeczą jest lokalizacja takiej biblioteki. Z jednej strony dobrze byłoby, gdyby była założona blisko ośrodka, chociażby ze względu na dostęp do potrzebnych danych, z drugiej jednak strony fakt istnienia biblioteki materiałów magnetycznych w bezpośrednim sąsiedztwie centrum obliczeniowego naraża ją na niebezpieczeństwo zniszczenia w chwili wybuchu, pożaru czy zalania wodą. Takie dodatkowe problemy jak: zasady ewidencji materiałów magnetycznych, zasady przekazywania tych materiałów do renowacji lub całkowitego zniszczenia, wymagają także jednoznacznego określenia. Zasady konserwacji i przechowywania w połączeniu z listą osób upoważnionych do dysponowania zbiorami, podkreślają wagę tego zagadnienia i wskazują na konieczność uwzględnienia ich przy rozpatrywaniu całości problematyki zabezpieczenia przed nieupoważnionym dostępem do zbiorów w ośrodku elektronicznego przetwarzania danych.

Projektując system zabezpieczenia danych, należy zbadać typowe profile potencjalnych użytkowników i ich zapotrzebowanie na określone zadania obliczeniowe. Wśród użytkowników spotykamy się z różnym stopniem zainteresowania i znajomości techniki obliczeniowej. Może to być np. osoba nie tworząca sytuacji problemowych, lecz pracującą w systemie pytanie - odpowiedź, np. agent linii lotniczych rezerwujący swojemu klientowi miejsce w samolocie. Może to być naukowiec, ale nie informatyk, którego podejście do wykorzystania komputera jest bardziej wymyślne niż użytkownika poprzedniej grupy. Mogą to być także programiści wykorzystujący system wielodostępny do uruchamiania programów wykorzystywanych w przetwarzaniu partiowym.

Biorąc natomiast pod uwagę wyposażenie systemu wielodostępnego, jakim będziemy dysponować, możemy rozróżnić trzy klasy użytkowników. Do klasy A należą użytkownicy eksploatujący jedną maszynę w jednakowy sposób, za pomocą tego samego sprzętu zewnętrznego.

Do klasy B należą użytkownicy wykorzystujący jedną maszynę do rozwiązywania różnych problemów i stosujący różne urządzenia zewnętrzne np. dalekopisy, kodopisy, ekranopisy i inne monitory.

Do klasy C należą użytkownicy wykorzystujący system wielomaszynowy do rozwiązywania różnych problemów i stosujący różne urządzenia zewnętrzne, jako satelitarne mogą być stosowane np. maszyny serii CDC 3000 w połączeniu z maszynami serii CDC 6000.

Oczywiście, w zależności od potrzeb, użytkownik zostanie wyposażony w określony tylko dla niego system rozkazowy. Wymaga tego właśnie zabezpieczenie dostępu do danych, które warunkuje przydzielanie użytkownikom prawa wykonywania określonych czynności na komputerze.

4.3. Założenia programowe

Zespół projektantów systemu zabezpieczenia danych postanowił wraz z przedstawicielem ośrodka elektronicznego przetwarzania danych opracować założenia programowe, na które składać się będą rodzaje potencjalnych zagrożeń oraz zalecenia działania profilaktycznego.

Jako pierwsze, postanowiono rozpatrzyć zagrożenie fizyczne sprzętu i danych.

Zalecenia działania profilaktycznego sformułowano następująco:

1. Ośrodek obliczeniowy instytutu naukowego powinien być zlokalizowany w bezpiecznym miejscu tzn. z dala od centrum miasta, od dużych skupisk przemysłowych. Jeśli budynek jest piętrowy, to pomieszczenia na piętrach nie powinny znajdować się przy zewnętrznych ścianach. Należy też baczną uwagę zwracać na piętra bezpośrednio sąsiadujące z pomieszczeniami ośrodka obliczeniowego.
2. Wstęp do pomieszczenia komputera powinien być dozwolony tylko osobom, które z racji wykonywanych czynności muszą przebywać na sali. W tej grupie znajdą się: operatorzy, konserwatorzy sprzętu oraz wybrani programiści, których obecność jest rejestrowana i obserwowana. Kierownik zespołu operatorów, byłby zobowiązany do kontrolowania osób wchodzących i prowadzenia specjalnej "księgi wejść". Księga ta, jak również inna dokumentacja pracy ośrodka obliczeniowego, powinna być kontrolowana regularnie przez kierownika sekcji zabezpieczenia ośrodka. Zapisane nośniki danych należy przechowywać w specjalnie do tego celu przystosowanym pomieszczeniu. Na sali komputera nie mogą się znajdować żadne inne nośniki informacji, oprócz tych które są aktualnie potrzebne. Podczas pracy wszystkich zmian powinni być obecni bibliotekarze, prowadzący dziennik wypożyczeń i zwrotów wszystkich nośników.
3. Należy przechowywać trzy komplety taśm z tymi samymi danymi. Jeden komplet taśm ma leżeć na półkach w bibliotece materiałów magnetycznych, drugi musi być również na terenie ośrodka, ale w specjalnie do tego przeznaczonym hermetycznym pomieszczeniu w podziemiach budynku. Trzeci komplet taśm powinien znajdować się w podobnym pomieszczeniu tyle tylko, że zlokalizowanym z dala od ośrodka obliczeniowego.

4. Należy w miarę możliwości zapewnić i uzgodnić zasady współpracy z takim samym komputerem, najlepiej będącym w posiadaniu tego samego ośrodka.

Następnym zagrożeniem z jakim należy się liczyć w ośrodku to świadome próby przekłamań. Zalecenia profilaktyczne podzielono w kategoriach operatorów i programistów.

Operatorzy:

1. Nie można zezwalać na pracę jednoosobową w ośrodku obliczeniowym. Obecność drugiej osoby jest psychologiczną barierą dla prób nieupoważnionej ingerencji do systemu.
2. Powinno nastąpić rozdzielenie obowiązków między:
   - kierownika operatorów,
   - operatorów,
   - bibliotekarzy materiałów magnetycznych,
   - kontrolerów dokumentów wejściowych i wyjściowych,
   - specjalistów w zakresie kontroli dokumentów.
3. Dobrze jest zastosować pewną "przypadkowość" w systemie regularnej pracy zmianowej, aby w ten sposób zapobiec możliwościom działań zorganizowanych, konspiracyjnych.
4. Oprócz automatycznego rozliczania prac wykonywanych za pomocą komputera, stosować należy odpowiednią, ręcznie prowadzoną księgę i zlecić kontrolę obu zapisów zespołowi odpowiedzialnemu za bezpieczeństwo.

Programiści:

1. Programiści nie powinni pod żadnym pozorem wykonywać czynności operatorskich i na odwrót.
2. Programy muszą mieć konstrukcję modułową, każdy moduł powinien być napisany przez innego programistę.
3. Programiści mają opracowywać programy w sposób zrozumiały dla ich kierownika. Każdemu programowi musi towarzyszyć przejrzysta dokumentacja.
4. Programy należy opracowywać poza salą, gdzie znajduje się komputer.
5. Zawsze należy wymagać starannego sprawdzenia programów na symulowanych danych.
6. Zmiany do przyjętych programów powinno się wprowadzać jedynie po uzyskaniu zgody i podpisu kierownika działu.

Następnym zagrożeniem dla ośrodka i danych jest przedostanie się niepożądanych osób na teren ośrodka. W tym względzie zalecane jest:

- w sysmetach z końcówkami należy stosować identyfikację za pomocą hasła i odzewu,

- w systemach ze stałymi połączeniami wprowadzić jednorazowe hasła,
- należy prowadzić dokumentację wszystkich transakcji napływających z poszczególnych, odległych urządzeń końcowych i badać wszystkie odchylenia od przyjętej procedury.

Czwarty rodzaj zagrożenia to instalowanie podsłuchu na liniach transmisyjnych. Zalecenia w tym względzie są następujące:

- wszystkie dane transmitowane z /lub do/ odległych końcówek należy przekazywać w postaci zaszyfrowanej,
- należy tak programować jednostkę centralną, aby działała z dużą prędkością w oddalonych zaś końcówkach stosować minikomputery z podobnych możliwościach.

Po zaznajomieniu się z zadaniami stawianymi przed systemem i warunkami eksploatacji oraz po ustaleniu założeń programowych, następuje faza realizacji wprowadzenia systemu zabezpieczenia danych przed nieupoważnionym dostępem. W fazie realizacji uczestniczy cały zespół projektantów systemu zabezpieczenia, a całość pracy jest nadzorowana przez kierownika tej grupy.

5. Kryteria oceny systemów ochrony zbiorów danych i korzyści płynących z ich wprowadzenia

5.1. Klasyfikacja kryteriów

Przy rozważaniu zabezpieczenia dostępu do danych ważnym problemem jest wysokość kosztów, jakie należy ponieść. Trzeba zdać sobie sprawę z tego co chce się chronić i jaka jest wartość chronionego obiektu dla użytkownika i dysponenta.

Elektroniczna technika obliczeniowa pracuje na usługach różnych instytucji, jednostek gospodarczych, administracyjnych, politycznych. Potrzeby tych instytucji w zakresie liczby i ważności informacji są różne. Przechowywane zbiory wymagają często większego stopnia kontroli lub nawet zabezpieczenia systemowego, gdy infiltracja ich może mieć nieobliczalne następstwa. Stąd wynika, że skuteczność i ekonomiczność systemów ochrony danych wymaga dokładnego sprecyzowania stopnia zabezpieczenia informacji, który jest stosunkiem przypadkowej lub umyślnej infiltracji do podatności informacji na niekontrolowane i niepożądane wykorzystanie. Kryteriami oceny systemów zabezpieczenia danych są:

- skuteczność,
- koszty opracowania,
- stopień komplikacji działania metody [13/].

Każde z tych trzech kryteriów ma swoje znaczenie. Rozpatrywane na przykładzie konkretnego systemu informatycznego może okazać się mniej lub bardziej ważne. Dla przykładu wyobraźmy sobie, że jesteśmy w fazie dyskusji dotyczącej zabezpieczenia trzech różnych systemów informatycznych. Pierwszy z nich będzie wojskowym systemem informatycznym, przechowującym informacje z zakresu obronności kraju, ewidencji uzbrojenia, liczebności armii itd. Drugi system dotyczy ewidencji przestępczości kryminalnej w Polsce. Zawiera dane o osobach będących w kolizji z prawem, odbywających karę w zakładach penitencjarnych, o liczbie przestępstw, częstotliwość ich popełniania, wykrywalność itd. Trzeci system informatyczny działania na usługach wielkiego przedsiębiorstwa przemysłowego, które dla usprawnienia procesu zarządzania i planowania w zakładzie postanowiło wykorzystać własny ośrodek ETO, który prowadzi ewidencję materiałów, ewidencję stanu załogi, listę płac itd.

Przykład tych trzech systemów ma za zadanie pomóc nam w jak najbardziej obiektywnym spojrzeniu na problematykę zabezpieczenia dostępu do danych.

5.2. Skuteczność

Najistotniejszą cechą każdej metody ochrony zbiorów jest jej skuteczność. Bez względu na to czy będziemy rozpatrywać system wojskowy, czy system w przedsiębiorstwie przemysłowym. Powstaje pytanie, czy istnieje system zabezpieczenia, którego skuteczność działania wynosiłaby 100 %. Eksperyment dający częściowo odpowiedź na to pytanie, przeprowadził profesor E.L.Glaser z Cleveland, który poddał kilka systemów informatycznych testom na skuteczność. W opinii właścicieli były one uważane za skutecznie chronione. Okazało się jednak, że prawie każdy z systemów po wnikliwym przeanalizowaniu mógł być eksploatowany nieprawidłowo, mimo procedur zabezpieczających. Warto przy tym zauważyć, że nie można tłumaczyć się, że sprawę badał wybitny fachowiec i specjalista. Wiadomo bowiem, że ten komu zależyć będzie na defraudacji zbiorów lub infiltracji systemu zrobi wszystko aby zamierzenia swoje zrealizować.

Współczesne systemy zabezpieczeń nie są doskonałe. Śledząc jednak uważnie ich ewolucję, choć niezwykle krótką, można dojść do przekonania,

13/ Por.A.S o k o ł o w s k i, wyd.cyt.

że niedaleka przyszłość będzie w stanie zaoferować system superbezpieczny. Największe nadzieje wiąże się ze specjalnie opracowanymi pamięciami asocjacyjnymi oraz z urządzeniem identyfikującym linie papilarne użytkownika. Oczywiście należy przy tym pamiętać, że system zabezpieczenia to tylko pewien mechanizm posłuszny woli człowieka i od niego zależny. Człowiek natomiast, jeśli się zdecyduje na świadome dokonanie czynności odczulają - cych system, może zniweczyć i zupełnie zredukować jego wartości.

Przed ostatecznym wdrożeniem każdej metody zabezpieczenia należy przeprowadzić specjalne badania jej skuteczności. Uzyskuje się to przez stworzenie odpowiednio zaplanowanych warunków zagrożenia. Na przykład parametrem obrazującym skuteczność zabezpieczenia może być oszacowana wielkość prawdopodobieństwa ochrony zbiorów.

Z omawianych w pracy metod zabezpieczenia, największym stopniem skuteczności odznaczają się układy techniczne identyfikujące użytkownika /sprawdzające jego linie papilarne lub nawet charakter pisma, czy cechy wizualnie dostrzegalne/. Stosowanie szyfrów i kodów jest dostatecznym zabezpieczeniem do momentu kiedy więcej osób nieupoważnionych nie pozna charakteru tego zabezpieczenia. W takim wypadku metoda formalnie przestaje istnieć i należy dokonać przeszyfrowania.

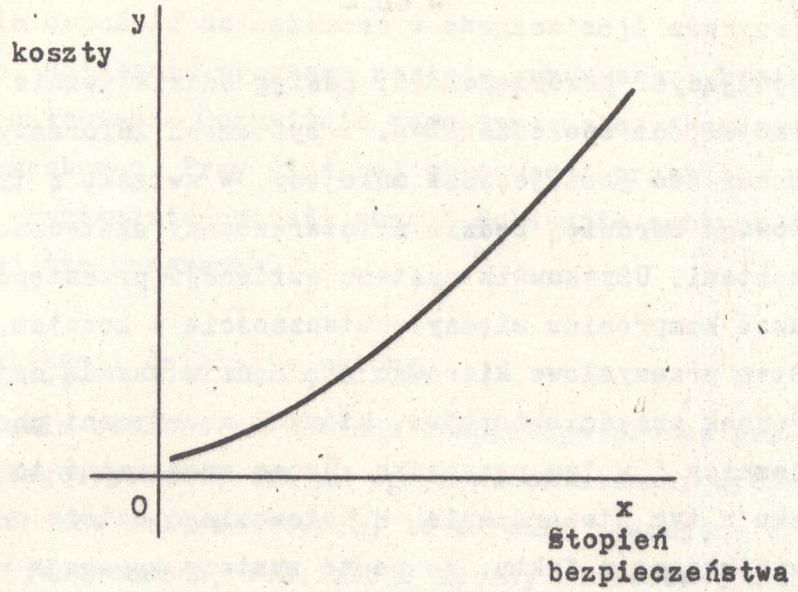
Podobnie jest z zabezpieczeniem programowym. Jest skuteczne do momentu nie szyfrowania schematu procedur. W związku z tym należy odpowiednio często dokonywać zmian parametrów identyfikowanych przez program, aby w ten sposób uniemożliwić i przeciwdziałać ewentualnym próbom infiltracji zbiorów.

O metodzie organizacyjnej trudno mówić jako o metodzie reprezentującej określony stopień bezpieczeństwa, jako, że sama na ogół nie występuje. Uzupełnia ona pozostałe metody, przyczyniając się do wzrostu stanu bezpieczeństwa.

5.3. Koszty opracowania

Skuteczność metody zabezpieczenia pozostaje w ścisłym związku z kosztami jej opracowania. Na podstawie badań okazało się, że koszty ponie - sione na zabezpieczenie systemu informatycznego wzrastają gwałtownie w miarę jak rośnie stopień bezpieczeństwa. Zjawisko to ilustruje wykres nr 4 /3/.

Jak wynika z wykresu wzrostu kosztów i pełnego bezpieczeństwa, przybiera postać funkcji wykładniczej. Oznacza to, że koszty rosną wykładni -



Rys. 4 Koszty opracowania zabezpieczenia

czo, gdy rozpatrywany stopień bezpieczeństwa systemu będzie się zbliżać do poziomu pełnego bezpieczeństwa tzn. 100 %.

Mając na uwadze taką zależność, zanim ostatecznie użytkownik zdecyduje się na odpowiedni poziom zabezpieczenia, musi wstępnie dokonać oszacowania danych, które mają być chronione przed ujawnieniem, nieupoważnionym dostępem czy niewłaściwym użytkownikiem. Użytkownik musi także ocenić i przewidzieć wpływ jaki może wywołać utrata lub zniszczenie informacji na funkcjonowanie instytucji czy przedsiębiorstwa. Dla lepszej analizy wskazane byłoby, aby użytkownik dysponował także danymi prawdopodobnymi związanymi z próbami nieupoważnionych infiltracji zbiorów. Mając zestaw wskaźników liczbowych można o wiele dokładniej ustalić wysokości kosztów, jakie należy ponieść na zabezpieczenie.

"Według ogólnych oszacowań opłacalny jest system ochrony, którego koszt nie przekracza 10 % całego komputera, przy czym 5 % tej ceny wystarcza do wprowadzenia 70 % wymaganego zabezpieczenia" [14/] - stwierdza M.Kotowski w swoim artykule. Tylko częściowo można się zgodzić z tym stwierdzeniem. W systemach wojskowych, gdzie zabezpieczenie jest szczególnie istotne, ponosi się nakłady rzędu nawet 50 % ceny całego komputera, przy czym okazuje się niejednokrotnie, że i takie zabezpieczenie nie jest stuprocentowe. W systemach tych przechowuje się informacje szczególnej wagi i potencjalna infiltracja może znaleźć swe odbicie w całym społeczeństwie, niejednokrotnie wykraczając poza obszar jednego państwa. W syste -

14/ M.K o t o w s k i, Komputer i bezpieczeństwo, Polityka nr 6, 1974

mach ewidencjonujących przestępczość, zasięg oddziaływania zmniejsza się do pewnej tylko części społeczeństwa. W systemach informatycznych przedsiębiorstw obszar ten jest jeszcze mniejszy. W związku z tym użytkownik systemu wojskowego bardziej będzie zainteresowany skutecznością zabezpieczenia niż kosztami. Użytkownik systemu ewidencji przestępczości będzie z pewnością szukał kompromisu między skutecznością a kosztem, natomiast przedsiębiorstwo przemysłowe kierować się będzie zasadą najmniejszych kosztów. Są jednak przedsiębiorstwa, których asortyment produkcji, podlega pełnej tajemnicy i w tym przypadku system musi wziąć to pod uwagę.

W związku z tym stwierdzenie M.Kotowskiego należy przyjmować z pewną rezerwą, wynikającą z faktu, że pewne systemy wymagają zabezpieczeń, może nie za wszelką cenę, ale na pewno daleko kosztowniejszych, niż 10 % ceny całego komputera. Ponadto brak zabezpieczenia informacji w pewnych systemach może postawić pod znakiem zapytania możliwości jego eksploatacji. Z tego też względu, koszty, choć niejednokrotnie bardzo wysokie, trzeba będzie ponieść. Tego typu urządzenia jak urządzenia umożliwiające porównanie odcisku zgłaszającego się użytkownika z wzorcem linii papilarnych przekazywanych do pamięci, kosztują około 30 % drożej niż sama jednostka pamięci centralnej komputera. Uruchomienie seryjnej produkcji tego typu urządzeń jest w tej chwili po prostu niemożliwe, wobec zupełnego braku nabywców. Należy się jednak spodziewać, że urządzenia te, jako jedyne gwarantujące pełne bezpieczeństwo eksploatacji systemu, zostaną produkowane masowo.

Stosowanie pozostałych trzech metod zabezpieczeń: tzw. stosowanie szyfrów, metody organizacyjnej i zabezpieczenia programowego, wymagają skromniejszych nakładów. Stosowanie szyfrów, wymaga w chwili obecnej, przy dobrze już opanowanej produkcji wszelkiego typu koderów i dekoderów, nakładów rzędu 80-krotnie mniejszych niż przy stosowaniu układów technicznych. Jeszcze mniejszych kosztów wymaga zabezpieczenie organizacyjne, które w gruncie rzeczy zależy od ludzkiej zaradności, operatywności i sprawności działania. Wszelkie dodatkowe przedmioty materialne stanowić mogą tylko uzupełnienie zasadniczej koncepcji postępowania.

Programowe zabezpieczenie charakteryzuje się niskimi kosztami i temu należy przypisać wyjątkową, jak na razie popularność. Wykorzystanie przez programistę procedur dozwolonych w określonym języku algorytmicznym wyższego rzędu, np. instrukcja ACCEPT w COBOL-u, pozwala uczynić z programu sprawny mechanizm samokontrolujący i samoregulujący całą działalność

mającą na celu nie dopuścić do zakłóceń w eksploatacji systemu. Wobec bra ku pewnych danych, działanie programu zostaje przerwane i konieczna jest wtedy ingerencja człowieka. Oczywiście tego typu zabezpieczenie jest stosunkowo łatwo zdemaskować. Przy dłuższej obserwacji przebiegu programu, każdy w zasadzie programista potrafi poznać dokładnie schemat działania maszyny sterowanej tym programem.

5.4. Stopień komplikacji działania metody

Stopień w jakim zastosowana metoda komplikuje proces przetwarzania danych i pracę całego systemu, też ma wpływ na ostateczny wybór rozwiązania. Większość ośrodków obliczeniowych, to ośrodki pracujące z dużą czę - stotliwością przy jednoczesnej realizacji zasady wielodostępności. Praca w takich ośrodkach podporządkowana jest zasadzie maksymalnego wykorzystania sprzętu liczącego i minimalizacji wszelkich przestojów lub nieekono - micznych i nieoptymalnych przebiegów przetwarzania. Wszystkie rozwiązania jakie znajdą zastosowanie w tak działającym systemie informatycznym, mogą wydłużać czas przetwarzania. Dominującymi zatem będą metody programowe, organizacyjne i ewentualnie stosowanie szyfrów, rzadziej natomiast spotkać można w tego typu systemach zabezpieczenie za pomocą układów technicznych. Oczywiście, mogą zdarzyć się przypadki kiedy wartości informacji i konieczność pełnej gwarancji ochrony zbiorów wymagać będą instalowania kosztownych urządzeń technicznych. Wówczas, zasada szybkości przetwarzania musi zostać podporządkowana zasadzie skuteczności.

Faktem jest, że systemy informatyczne wykorzystujące zabezpieczenia techniczne są wolniejsze i nie są w pełni wykorzystane ich możliwości eksploatacji. Jest to jednak podyktowane koniecznością bezwzględnej ochrony danych w systemie.

Dobra organizacja pracy i organizacyjne działania zabezpieczające mogą przyczynić się do poprawy ochrony danych. Zła organizacja wywołuje zazwyczaj skutki wprost odwrotne. Częste przestoje, awarie, brak operatywności, dezorganizuje pracę. Stosowanie programów zabezpieczających i szyfrów, wymaga dodatkowego czasu.

Na podstawie specjalnie przeprowadzonych pomiarów okazało się, że system informatyczny funkcjonujący z urządzeniami technicznymi zabezpieczającymi jego prawidłową eksploatację, wydłuża swój podstawowy cykl przetwarzania o blisko 40 % w stosunku do przewidzianego efektywnego czasu pracy. Przy użyciu koderów i dekoderów procent ten wynosi odpowiednio oko

ło 20 %, a stosując programowe zabezpieczenie czas przetwarzania wydłuża się tylko o blisko 7 %. Wielkości te, gdyby je ze sobą porównywać są oczywiście względne. Wiadomo bowiem, że różne komputery odznaczają się różnymi parametrami eksploatacyjnymi i dlatego np. czas potrzebny na obliczenie i wydrukowanie jednakowej listy płac w maszynie IBM 360 przy zastosowaniu urządzenia identyfikującego linie papilarne użytkownika jest i tak krótszy o blisko 20 % w porównaniu z maszyną ZAM-21, która do tego celu wykorzystuje tylko programową ochronę informacji.

5.5. Przyczyny niskiej skuteczności stosowanych obecnie metod zabezpieczenia

W dotychczasowej praktyce obserwuje się zróżnicowany poziom rozwoju sprzętu komputerowego i dążenia do rozwoju przetwarzania danych, Do przyczyn niedoskonałości współczesnych systemów ochrony można zaliczyć:

1/ Brak ogólnej koncepcji ochrony. Rozważania na temat sposobu wprowadzania zabezpieczenia systemowego koncentrują się wokół zagadnienia: czy stosować jeden ogólny system ochrony dla wszystkich użytkowników i programistów, czy raczej zdecydować się na wprowadzenie kilku różnych wyspecjalizowanych systemów.

2/ Błędne pojmowanie istoty zabezpieczenia. Do wczesnych lat sześćdziesiątych utożsamiano zazwyczaj ochronę komputerów z zabezpieczeniem systemów przed przekłamaniem, źle wydziurkowanymi kartami itp.

3/ Koncentrowanie uwagi na zagadnieniach związanych z efektywną eksploatacją systemów. Zwiększanie pojemności pamięci maszyn cyfrowych, doskonalenie techniki dostępu itd.

4/ Przyjmowanie tezy, że wprowadzanie systemów zabezpieczeń jest nieekonomiczne i niemożliwe do realizacji w praktyce.

5/ Niemożliwość udzielania odpowiedzi na pytanie, jak zabezpieczyć i jak chronić sam mechanizm ochrony danego systemu.

Od momentu kiedy wypadki nieupoważnionych infiltracji zbiorów, przekłamań, pożarów i innego rodzaju zniszczeń, zaczęły stawać się coraz częstszymi, kiedy obalono mit o technicznej barierze niedostępności maszyn cyfrowych dla laików, kiedy wielkie firmy na własnych zyskach odczuły powstałą groźbę, rozpoczęto wyścig z czasem. Tezy o nieekonomiczności stosowania środków zabezpieczających, a co więcej o ich bezcelowości, należą już do przeszłości. Producenci maszyn cyfrowych coraz częściej wyposażają swoje zestawy komputerowe w minimalne nawet środki ochrony. I choć obec -

nie sytuacja nie jest zadowalająca należy oczekiwać, że już niebawem, w standardowym wyposażeniu będzie również działał skuteczny aparat ochrony.

Wnioski jakie się nasuwają w toku rozważań nad zabezpieczeniem można sprecyzować następująco:

1. Należy zdawać sobie sprawę /dotyczy to zarówno użytkowników, projektantów systemów, jak i pozostałej kadry/ z obiektywnej konieczności ochrony informacji zawartej w systemach informatycznych.
2. Mając na uwadze konieczność ochrony, należy dokonać takiego jej wyboru, aby uwzględniała potrzeby różnego typu systemów informatycznych a nie tylko tych, gdzie zabezpieczenie jest bezwzględnym warunkiem eksploatacji.
3. Budowanie odpowiedniej metody zabezpieczenia powinno się odbywać równolegle z pracami projektowymi nad przyszłym systemem, tylko bowiem w ten sposób można dokładnie poznać wymagania systemu w tym zakresie, a ponadto wcześniej przewidzieć późniejsze zakłócenia.
4. Konieczną staje się umiejętność przeprowadzenia odpowiedniej analizy sytuacyjnej w jakiej działa system i zaproponowania metody zabezpieczenia, adekwatnej do potrzeb systemu. Chodzi o to, aby systemy, które nie wymagają nadzwyczajnych środków ochrony, nie były wyposażone w kosztowne i zbyteczne urządzenia. Trzeba zdawać sobie sprawę z proporcji między wartością informacji z jednej strony, a skutecznością, kosztownością i stopniem skomplikowania metody, z drugiej strony.
5. W miarę jak wzrasta zastosowanie komputerów i społeczne zainteresowanie informatyką powstaje obiektywna potrzeba wyznaczenia przedstawiciela kierownictwa, który byłby osobą czuwającą nad procesem wdrażania procedur zabezpieczających. Powinien to być inspektor systemów EPD.
6. W ramach Ośrodka Badawczo-Rozwojowego Informatyki stworzyć komórkę do spraw zabezpieczenia systemów. Zadaniem takiej komórki byłoby podejmowanie badań i proponowanie nowych rozwiązań ochrony systemów z jednoczesnym uwzględnieniem najnowszych zdobyczy w tej dziedzinie. Byłaby to teoretyczna baza dla potrzeb użytkowników.
7. Jeśli OBRI zajmowałby się stroną teoretyczną projektów, to należałoby zainteresować praktyczną stroną zagadnienia bezpośredniego producenta sprzętu komputerowego, Zjednoczenia MERA.
8. Okazją do integracji badań w tym zakresie mógłby się stać program komputeryzacji w państwach RWPG, na EMC JS-RIAD.

5.6. Korzyści zabezpieczenia przed nieupoważnionym dostępem do danych

Wprowadzenie systemów zabezpieczenia danych przed nieupoważnionym dostępem prowadzi nie tylko do ponoszenia dużych nakładów i wykonywania określonych prac organizatorskich, ale przede wszystkim warunkuje otrzymanie wymiernych korzyści. Należy już do przeszłości mniemanie, że z systemami zabezpieczenia wiąże się więcej kłopotów niż korzyści. Zresztą w sytuacji kiedy stosowanie zabezpieczenia stało się niejednokrotnie podstawowym warunkiem ich eksploatacji, trudno dłużej rozwodzić się nad samą potrzebą takich systemów. Zabezpieczenie informacji nabrało po prostu w chwili obecnej waloru oczywistości. Pojawia się nawet literatura z zakresu efektywności stosowania systemów zabezpieczenia danych.

Do najważniejszych korzyści związanych z wprowadzeniem zabezpieczenia danych przed niepożądanym dostępem zaliczyć należy:

- swobodę działania systemów informatycznych,
- zwiększenie stopnia prawidłowości działania systemów,
- wzrost jakości działania ośrodka EPD,
- poprawienie istniejących rozwiązań zabezpieczenia zbiorów z danymi przetwarzanymi w Ośrodkach EPD.

W sytuacji kiedy użytkownik nie ma pewności, że dane mogą być uchronione przed infiltracją, stara się, działając półśrodkami, wyeliminować choć w części to zagrożenie. Podejmowanie działań na zasadzie półśrodków w większym stopniu komplikuje zasadniczy proces przetwarzania danych.

Następna korzyść, jaka płynie z zastosowania systemu zabezpieczenia danych wynika bezpośrednio z pierwszej. Zrezygnowanie z działania półśrodkami upraszcza działanie systemów informatycznych, a zastosowanie sprawnego systemu ochrony danych zwiększa stopień prawidłowości działania systemu. Należy bowiem pamiętać, że zabezpieczenie danych uwzględnia także kontrolę prawidłowości przetwarzania w sposób niezależny od czynności systemu operacyjnego i programów sterujących.

Dobrze zabezpieczony dostęp do danych to punkt wyjścia dla stworzenia w pełni efektywnego modelu wykorzystania możliwości ośrodka obliczeniowego. Większość ośrodków obliczeniowych w Polsce pracuje jako ośrodki usługowe. Rodzaj prowadzonych prac w zakresie przetwarzania danych, stopień ich tajności, często ogranicza zakres prac z tego względu, że wymaga to dostępu do systemu nowej grupy osób. W takich wypadkach efektywność działania ośrodka EPD jest podporządkowana wymaganiom bezpieczeństwa danych. Taka hierarchia zależności jest oczywiście konieczna w sytuacji kie

dy jest potrzeba zabezpieczenia danych, a ważność informacji jest na tyle duża, aby miała priorytet nad efektywnością wykorzystania sprzętu.

W najbliższym czasie nie będzie możliwości osiągnięcia pełnego zabezpieczenia danych. W związku z tym każdy zastosowany system ochrony danych stanowi pewne nagromadzenie doświadczeń w tej dziedzinie. Ani pierwszy, ani drugi system nie będzie z pewnością doskonały. Będzie posiadał swoje słabe punkty. Ale świadomość tych słabych punktów pozwoli w przyszłości na ich wyeliminowanie. Wymiana doświadczeń z przedstawicielami innych ośrodków obliczeniowych, z producentami sprzętu i projektantami systemów informatycznych przyczynia się do poszerzenia spojrzenia na całość zagadnienia. Wskazana jest również współpraca i zainteresowanie problemem ośrodków badawczo-rozwojowych informatyki i instytutów naukowych.

Bibliografia

1/ Europejski Program Badawczy Diebolda, Przeglądy kontrolne systemów, OBRI nr 40/1973.

2/ GACKOWSKI Z., Informatyka w zarządzaniu przedsiębiorstwem przemysłowym, PWE, Warszawa 1973

3/ IDŹKIEWICZ A., Zabezpieczenie informacji oraz sprzętu jej przetwarzania przed zniszczeniem, uszkodzeniem i nieupoważnionym dostępem, Problemy Informatyki, Warszawa 1974

4/ KALTZ H., Ohne Sicherung, Informatik nr 7/1973

5/ Kodeks postępowania cywilnego. Wydawnictwo Prawnicze, Warszawa 1974

6/ KOTOWSKI M., Komputer i bezpieczeństwo, Polityka nr 6/1974

7/ Ochrona prawna oprogramowania w krajach zachodnich, Informatyka nr 3, 4, 5/1977

8/ Praca zbiorowa pod red. E.A.FEIGENBAUMA i I.FELDMANA, Maszyny matematyczne i myślenie, PWN, Warszawa 1972

9/ SAWICKI E., Automatyczne rozpoznawanie mowy, Elektroniczna Technika Obliczeniowa nr 4/1974

10/ SOKOŁOWSKI A., Ochrona zbiorów informacji w systemach informatycznych, Informatyka nr 12/1973

11/ TARGOWSKI A., Polscy prawnicy o informatyce, Informatyka nr 9/1976

12/ WEIAMANN O., Sicherung in der Zukunft, Datenverarbeitung nr 5/1976

13/ Zbiór artykułów "Scientific American", Dziś i jutro maszyn cyfrowych, PWN, Warszawa 1960.

Zbigniew KOŚCIOŁEK

OCHRONA ŚRODOWISKA INFORMACJI - ROLA CZŁOWIEKA

WSTĘP

W każdej działalności, a szczególnie gospodarczej, zahamowanie dopływu informacji lub przepływ jej do osób nieupoważnionych może spowodować duże trudności lub nieobliczalne następstwa i zakłócenia. W każdym ośrodku obliczeniowym stosowane są pewne środki i narzędzia zabezpieczające dostęp do zbiorów systemów informatycznych. Nie mniej, w większości przypadków zwłaszcza w tzw. ośrodkach otwartych, są one niewystarczające. Zwykle, zagadnienie ochrony informacji zaczyna być dostrzegane, nie w okresie projektowania ośrodka, lecz dopiero po rozpoczęciu działania, gdy zinstytucjonalizuje się określony tryb obiegu dokumentów, technologii, gospodarki zbiorami itp.

Powstaje wówczas konieczność odzwyczajania od przyjętych form "życia" ośrodka, od form, które okazały się z punktu widzenia zabezpieczenia środowiska informacji przed niepożądanym dostępem chybione lub wprost niewystarczające. Zmiana funkcjonowania ośrodka ze względu na konieczność ochrony informacji wywołuje zwykle reakcje nieprzychylne zamierzonemu działaniu. Jest to reakcja normalna potwierdzająca tezę, że łatwiej jest nauczać niż oduczać. W związku z tym w dalszym ciągu główny akcent położony będzie na uświadomienie pracownikom ośrodków przetwarzania danych potrzeby, a nawet konieczności stosowania i podporządkowania się ustalonym przepisom o ochronie informacji.

1. Dlaczego chronimy środowisko informacji ?

Na Konferencji Europejskiego Programu Badawczego Diebolda w 1972 r. W.H.Murray stwierdził, że: "Bezpieczeństwo jest to grupa zadań kierownictwa, obejmująca dbanie o dokładność i nienaruszalność informacji potrzebnej do prowadzenia przedsiębiorstwa, o poufność i niedostępność wrażliwych danych, o ochronę instalacji obliczeniowej przed katastrofami naturalnymi niewłaściwym użyciem itp."o ustrzeżenie pracowników przed pokusą, a kierownictwa przed nieprzezornością. Bezpieczeństwo musi zapewnić, że przedsiębiorstwo przetrwa katastrofę i będzie kontynuować realizację swoich zadań. Bezpieczeństwo musi współzawodniczyć z innymi zadaniami kie

rownictwa. Należy więc na nie patrzeć jako na funkcję operacyjną, liniową a nie szbatową".

Jeśli uznać, że zacytowane stwierdzenie daje tylko zasadniczą i bardzo syntetyczną wytyczną dla kierownictwa czym jest bezpieczeństwo w ośrodku obliczeniowym, to praca ob.K.Marciniaka systematyzuje i podaje metodologię stosowania zabezpieczeń właśnie traktując je jako funkcję operacyjną, liniową realizowaną przez wszystkie ogniwa, zespoły i grupy pracownicze w ośrodku obliczeniowym.

Czytając kolejne rozdziały opracowania nieodparcie nasuwa się wniosek, że mimo, iż przedmiotem zabezpieczenia są zbiory danych w ośrodku obliczeniowym, to jednak podstawową jednostką, z którą związana jest ochrona informacji jest człowiek.

Opracowując odpowiednie systemy zabezpieczenia w ośrodku obliczeniowym, w rezultacie końcowym efektem jest ochrona człowieka bez względu na to z jakiego punktu widzenia będziemy na rzecz patrzyli.

Zabezpieczenia przed działaniem siły wyższej /pożar, zalanie wodą, itp./ ma na celu uchronienie się przed katastrofą - utratą zbiorów, danych, które są podstawą działalności np. gospodarczej, gdzie podejmowanie decyzji ma wpływ w mniejszym lub większym stopniu na losy, kariery, możliwości prawidłowego działania ludzi.

Zabezpieczenie przed dostępem do zbiorów przez osoby nieupoważnione, a działające aktywnie z zewnątrz to nie tylko fakt utraty informacji, lecz konsekwencje związane z odpowiednią grupą ludzi. Brak prawidłowych zabezpieczeń stwarza również pokusę dla pracowników ośrodka,

Ogólnie rzecz biorąc, organizacja systemu zabezpieczeń powinna być tego rodzaju, aby wśród osób stykających się bezpośrednio a nawet pośrednio z elektronicznym przetwarzaniem danych istniało przeświadczenie, że dostęp do informacji dla osób niepowołanych jest trudny, że wszelkie próby dokonania penetracji będą bezzwłocznie wykryte, a wobec winnych zaniedbań lub działających w złej wierze wyciągnięte zostaną dyscyplinarne lub karne konsekwencje, aby cel ten mógł być osiągnięty, musi powstać wśród załogi przeświadczenie, że kierownictwo przywiązuje dużą wagę do ochrony zbiorów maszyn i urządzeń służących do przetwarzania, przechowywania lub przekazywania danych.

Funkcjonowanie systemu zabezpieczenia musi być podtrzymywane na codzień, bowiem każdy tego rodzaju system bardziej lub mniej rozwinięty jest pewnym utrudnieniem w działalności pojedynczego pracownika lub zespo

łu. Naturalnym odruchem pracownika jest odrzucanie wszelkiego rodzaju nakazów lub zakazów, które z punktu widzenia są zbędnym balastem. W wypadku systemu zabezpieczeń jest to tym bardziej istotne, że podział kompetencji lub ich zawężenie do określonego odcinka, wywołuje krytykę. W związku z tym, należy dążyć do takich rozwiązań systemu zabezpieczeń, aby nie stanowiły uciążliwego narzędzia, przesłaniającego podstawowy cel działalności osrodka obliczeniowego tj. świadczenie usług dla użytkowników systemów EPD.

2. Rola człowieka

Jak już powiedziano, ochrona środowiska informacji wynika z konieczności ustrzeżenia się przed zniszczeniem, zdeformowaniem lub wykorzystaniem zbiorów przez niepowołane osoby. Ochronę tę tworzymy dla człowieka i w przeważającej mierze przez człowieka. Człowiek jest tu jedynym ogniwem mającym pełną świadomość swojego działania i poczynań.

System ochrony środowiska informacji może funkcjonować prawidłowo /zakładając, że jest właściwie opracowany/ tylko wówczas, gdy istnieje pełna świadomość celu działania oraz przestrzegania ustaleń zawartych w tym systemie. Oczywiście system ten musi być sterowany i kontrolowany. Kontrola musi odbywać się w sposób ciągły i nieformalny. Przypadkowa, nie planowana, coraz rzadziej przeprowadzana kontrola, utwierdza pracowników osrodka w odczuciu, że system ochrony można odłożyć ad acta.

Brak planowej, dynamicznej kontroli osłabia w większości przypadków świadomość celu jaki ma spełniać ochrona środowiska informacji. Dotyczy to również tych pracowników, którzy z racji swoich stanowisk są odpowiedzialni, na powierzonych im odcinkach pracy, za część systemu ochrony. Jak wiadomo, system ochrony nakłada wiele ograniczeń, stwarza pewne nakazy i zakazy, które "nie podobają" się pracownikom. Najbardziej popularnymi argumentami jakie słyszy się od pracowników to, to że: nie stosując systemu, można bardziej efektywnie wykorzystywać komputery i szybciej zaprogramować system użytkowy oraz dokonywać tzw. poprawek "w locie".

Argumenty te są o tyle chwytliwe, że z reguły system ochrony środowiska informacji jest wprowadzony po pewnym czasie od dnia uruchomienia ośrodka. A jest rzeczą oczywistą, że niektóre operacje lub czynności przy stosowaniu systemu ochrony są bardziej czasochłonne. Jeśli, jeszcze będziemy rozpatrywali przykłady ośrodka, w którym częstotliwość dzienna

zmiany systemów użytkowych jest duża, to wówczas zwiększenie czasu na nowe wynikające z zastosowania systemu ochrony czynności mogą nasuwać takie wnioski.

Na przykład zasada podziału kompetencji przy projektowaniu systemu użytkowego, w niektórych ośrodkach może napotykać na trudności braku odpowiednich specjalistów i fachowców, co w rezultacie prowadzi do rezygnacji z przyjętej zasady.

Innym nie sprzyjającym zjawiskiem są przetwarzane w jednym ośrodku systemy użytkowe tajne, poufne i jawne. Stwarza to konieczność ustalenia bardziej zróżnicowanego systemu ochrony informacji, bowiem próby równania "w górę" z reguły trudne są i nieuzasadnione. Dodatkowo mogą komplikować sprawę fakty zamiany po przetwarzaniu zbioru jawnego na tajny i odwrotnie.

Wracając do rolą człowieka, należy jasno określić cel systemu ochrony środowiska informacji oraz przekonać pracowników o konieczności jego stosowania. Przekonywanie to, zwłaszcza gdy wprowadzenie systemu odbywa się w ośrodku o dość długim stażu, staje się problemem bardzo trudnym i uciążliwym, wymagającym od osób bezpośrednio czuwających nad bezpieczeństwem ośrodka nie tylko szczegółowej znajomości systemu ochrony, ale przede wszystkim, poczucia taktu, zdolności przekonywania i konsekwentnej realizacji poczynań.

Wdrażając w funkcjonującym już ośrodku system ochrony środowiska informacji inaczej należy uzasadniać konieczność jego wprowadzania pracownikom pionu projektowo-programistycznego, inaczej operatorom, a jeszcze w inny sposób należy to wytłumaczyć serwisowi technicznemu.

Najtrudniejszy jest zwykle okres około 3 miesięcy od momentu wprowadzenia systemu ochrony. W tym czasie należy z jednej strony konsekwentnie przestrzegać ustaleń zawartych w systemie ochrony środowiska informacji, a z drugiej strony starannie i z rozwagą wyważać kary dla pracowników popełniających uchybienia.

System ochrony środowiska informacji, który w rezultacie ma służyć człowiekowi i realizowany jest w zasadzie wyłącznie przez człowieka musi uświadomić wszystkim pracownikom ośrodka obliczeniowego korzyści, jakie z niego płyną, nie koniecznie bezpośrednio dla jednostki i nie zauważalnie w krótkim czasie jego działania. Pomocniczą rolę, jaką spełnia system ochrony, jest przyswojenie przez pracowników zasad porządku, systematyczności, poczucia odpowiedzialności, które to cechy mogą i powinny być wykorzystywane w codziennej pracy zawodowej.

Mieczysław KUBASIEWICZ

KONTROLA DANYCH JAKO ELEMENT ZABEZPIECZENIA INFORMACJI W SYSTEMACH INFORMATYCZNYCH

1. Ogólna charakterystyka błędów i przyczyny ich powstawania w systemach informatycznych

Jednym z zadań systemu informatycznego powinno być uzyskanie odpowiedniego poziomu wiarygodności informacji. Chcąc skutecznie przeciwdziałać powstawaniu oraz wykrywać przekłamania w procesie przetwarzania danych należy:

- ustalić prawdopodobne przyczyny powstawania,
- zlokalizować miejsce powstawania,
- opracować skuteczne metody wykrywania,
- zapewnić możliwość korekty wykrytych nieprawidłowości oraz włączenia poprawionych danych w najbardziej odpowiednim miejscu.

Przeciwdziałanie zniekształceniom danych informacji oraz ich przekłamaniom itp. powinno odbywać się w czasie całego procesu przetwarzania danych - od pomiaru i pierwotnej rejestracji danych o zdarzeniu, do analizy i informacji wynikowej.

Błędy i przekłamania w danych mogą powstawać w samym systemie informatycznym, jak również w jego otoczeniu, zwłaszcza w systemach zarządzania, które korzystają ze źródeł pomiaru i rejestracji danych o zjawiskach i zdarzeniach powstających w procesach produkcji i zarządzania. Charakterystycznymi błędami dla tych źródeł są:

- przekłamania w kwantyfikatorach, wynikające z błędnego: odczytu z przyrządów, wpisu do formularza, przeniesienia danych na maszynowy nośnik /MND/;
- przekłamania w identyfikatorach, polegające na: wpisaniu do formularza lub przeniesieniu na MND niewłasciwego symbolu, błędnym przyporządkowaniu w symbolu, nieodpowiednim zaklasyfikowaniu;
- pominięciu danych lub ich części w wyniku nie wykonania pomiaru lub rejestracji przez zapomnienie lub z innych przyczyn;
- wielokrotne pomiary lub rejestracja danych dotyczących tego samego zjawiska lub zdarzenia;
- pomiary lub rejestracje danych po upływie wyznaczonego terminu, po którym dane te przestały być aktualne i w związku z tym są bezużyteczne.

W czasie wykonywania różnych funkcji procesu przetwarzania danych takich jak: przekazywanie /przesyłanie/, przenoszenie na MND, wprowadzanie /pamiętanie/ do pamięci komputera, przetwarzanie i udostępnianie informacji mogą powstawać przekłamania w danych /kwantyfikatorach i identyfikatorach/ lub opóźnienia w ich przekazywaniu spowodowane innymi przyczynami.

W operacjach komputerowych istnieje możliwość generacji zbędnych danych, zniekształcenia struktury oraz zmiany ich sensu czy właściwości. W zależności od funkcji procesu przetwarzania, fakty wywołujące tego rodzaju skutki są zróżnicowane. Źródeł powstawania wszelkiego rodzaju błędów należy szukać w samym systemie informatycznym, należącym do systemów człowiek-maszyna. W systemie tym występują dwa elementy - człowiek oraz środki techniczne /takie jak: urządzenia rejestracji i pomiaru, urządzenia do przenoszenia danych na maszynowe nośniki, komputery/.

Na podstawie przeprowadzonych w kombinacie Robotron [1/] badań ustalono, że prawdopodobieństwo wystąpienia błędu określonego jako stosunek liczby błędnych znaków do ogólnej liczby znaków przetworzonych /przesłanych/ kształtuje się następująco:

a/ człowiek - od $1 \cdot 10^{-2}$ do $1 \cdot 10^{-3}$
b/ połączenia telefoniczne - $3 \cdot 10^{-4}$
c/ połączenia teleksowe - $1 \cdot 10^{-4}$
d/ dalekopisy, dziurkarki, czytniki kart /taśm/ dziurkowanych, drukarki - $1 \cdot 10^{-6}$
e/ transmisja danych - od $1 \cdot 10^{-6}$ do $1 \cdot 10^{-8}$
f/ jednostka centralna komputera - od $1 \cdot 10^{-8}$ do $1 \cdot 10^{-10}$.

Analiza systemu informacji dokonywana w aspekcie podziału procesu przetwarzania na operacje /pomiar, rejestracja danych, przenoszenie danych na MND itd./ bądź na elementy /algorytmy, metody, programy, instrukcje, sprzęt i ludzie/, pozwala na lepsze poznanie przyczyn powodujących powstawanie błędów. Charakterystykę danych pod względem ich wiarygodności można przeprowadzić biorąc pod uwagę błędy:

- w danych źródłowych,
- popełnione przez operatorów urządzeń,
- w oprogramowaniu SI,
- w algorytmach i metodach,
- wynikające z faktu użycia sprzętu technicznego - uszkodzenia lub oddzia

1/ Por.D.H o r n, N.B u s c h, Datensicherung im System der EDV. VEB Kombinat Robotron, Dresden 1970, s. 21

ływania wszelkiego rodzaju zakłóceń /np. elektrycznych, mechanicznych/.

Wymieniono pięć grup przyczyn, z czego w czterech przypadkach błędy powstają przy współudziale człowieka i w związku z tym to ogniwo SI należy rozpatrzyć ze szczególną uwagą. Wpływ sprzętu na wiarygodność danych jest niewielki/gdyż odpowiedni poziom niezawodności zabezpieczony jest w sposób układowy.

Błędy popełniane przez człowieka można zaliczyć do klasy błędów systematycznych. Błędy z tego tytułu mogą być związane z niedokładną znajomością zjawisk powstających w komputeryzowanym obiekcie, przyjęciem niewłaściwej dla danego obiektu metody obliczeń, niezauważeniem w czasie projektowania pomyłek w algorytmach przetwarzania, niewłaściwym opracowaniem instrukcji eksploatacyjnej, niepoprawnymi założeniami programu, niewykrytymi usterkami w programach itp. Z chwilą ustalenia charakteru i przyczyn błędów można je całkowicie wyeliminować.

Błędy mogą powodować przekłamania w danych, przekształcać je, nadawać im inne jakościowo znaczenie, mogą się stać również przyczyną zagubienia danych, rekordów, czy też wygenerowania nowych danych. Skutki błędów mogą być nie tylko zróżnicowane, ale i bardzo groźne dla działania systemu informatycznego. Są one trudne do przewidzenia i w związku z tym nie można opracować skutecznych metod ich wykrywania; Skorygowanie zniekształconych danych oraz usunięcie przyczyn błędów wymaga najczęściej powtórzenia części prac projektowych.

Podstawową trudnością jest tu stochastyczna natura danych, powodująca, że przy obecnych metodach opracowywania programów nie można uzyskać wszystkich możliwych układów danych do testowania, gdyż liczba ich może sięgać tysięcy kombinacji.

Na zwiększenie się liczby błędów popełnianych przez personel obsługujący system informatyczny oraz zarządzania mają wpływ następujące elementy:

- niewłaściwa interpretacja rejestrowanych, przetwarzanych i wykorzystywanych danych,
- niedokładne, o niskiej jakości instrukcje postępowania lub ich brak,
- obojętność, niedbalstwo operatorów urządzeń,
- brak indywidualnej odpowiedzialności za jakość wykonywanych prac, brak kontroli, celowe zniekształcanie danych, nieraz nawet z egoistycznych powodów /pomyłki na własną korzyść/,
- niedostateczne zrozumienie znaczenia wykonywanych prac.

Przeprowadzenie wyczerpującej i jednoznacznej klasyfikacji błędów, ich przyczyn i skutków jest zadaniem skomplikowanym. Związane jest to zarówno z określonym SI, jak również z tym, że ten sam błąd /np. przekłamanie znaku/ może powstawać w różnych miejscach procesu przetwarzania danych i wynikać z różnych przyczyn /błędy w rejestracji i programach, przekłamanie w transmisji itp./. Może zaistnieć również taka sytuacja, że jeden błąd będzie pociągał za sobą wiele innych.

2. Sposoby kontroli danych w procesie przetwarzania

Przedmiotem kontroli jest proces uzyskiwania danych źródłowych oraz przekształcania ich w informacje wynikowe, a w szczególności elementy danych, występujące w procesie przetwarzania w określonym czasie i kolejności w postaci samodzielnej lub w postaci określonych sekwencji informacyjnych, zawierających dowolną liczbę danych elementarnych.

Celem kontroli jest sprawdzenie wiarygodności, kompletności i terminowości przetwarzanych danych.

Ze względu na technikę realizacji można wyróżnić w procesie przetwarzania danych czynności kontrolne, wykonywane wizualnie /optycznie/, układowo i programowo.

Kontrola w i z u a l n a polega na manualnej weryfikacji prawidłowości określonej formy prezentowania danych /np. na ekranie, liczniku, formularzu/, uzyskanych wyników /np. tabulogramów kontrolnych/ albo też na obserwacji przebiegu realizacji procesu przetwarzania.

Kontrola u k ł a d o w a związana jest z możliwościami techniczno-eksploatacyjnymi zastosowanych urządzeń technicznych. Polega ona na automatycznym sprawdzeniu prawidłowości wykonania określonej czynności przez urządzenie /np. zakończenie przesyłania danych między urządzeniami, przesuwu taśmy lub karty w urządzeniu czytającym, zastosowanie właściwego kodu/.

Kontrola p r o g r a m o w a przeprowadzana jest w celu weryfikowania tych elementów systemu informatycznego, które nie mogą być sprawdzone w inny sposób lub wówczas, gdy ten rodzaj kontroli jest najbardziej efektywny bądź ekonomicznie uzasadniony. Tym rodzajem kontroli mogą być objęte tylko te elementy SI, które można sklasyfikować i zalgorytmizować.

Wśród metod, którymi przeprowadzana jest kontrola w procesie przetwarzania danych, można wyróżnić metodę porównawczą, rachunkową oraz weryfikacyjną.

Metoda p o r ó w n a w c z a polega na porównaniu rezultatów uzyskanych w różny sposób lub w sposób identyczny ale przez innych wykonawców, bądź w porównaniu z obowiązującymi standardami. Przykładem takiej kontroli jest sprawdzenie dziurkowania kart w urządzeniu kontrolno-odczytującym.

Przy kontroli r a c h u n k o w e j porównuje się wielkości pozostające względem siebie w określonej zależności arytmetycznej; stosuje się sumy i liczby kontrolne, uwzględniania zasady bilansowania, weryfikuje się format danych, liczb zapisów itp.

Przeprowadzając kontrolę procesu przetwarzania metodą w e r y f i k a c y j n ą porównuje się uzyskany wynik /np. MND/ z materiałem będącym podstawą jego uzyskania, istniejącymi standardami lub określonymi zależnościami.

Przedstawione rodzaje i metody kontroli mogą być stosowane w różnych momentach procesu przetwarzania danych samodzielnie lub też we wzajemnym powiązaniu. Wynika to głównie z powodu:

- stosowania urządzeń technicznych o różnorodnych możliwościach i przeznaczeniu,
- wymagań i możliwości związanych z wiarygodnością danych,
- określonej organizacji przechowywania danych,
- charakteru i struktury przetwarzania danych w pewnej fazie.

Decydując się na zastosowanie określonego rodzaju kontroli, należy pamiętać o tym, że jej skuteczność ocenia się nie liczbą wykrytych błędów, ale przede wszystkim liczbą przepuszczonych błędów.

Ponieważ poszczególne rodzaje kontroli nie gwarantują wykrycia wszystkich błędów w związku z tym stosuje się łączenie kilku metod kontroli w wielofazowy cykl kontrolny. Przykładem może być weryfikacja sporządzenia MND, która przeprowadzana jest na sprawdzarkach, a kontynuowana podczas kontroli poprawności wczytanych danych przez komputer.

Trzeba jednak pamiętać o tym, że skorygowanie wszystkich błędów jest przy obecnej technice nie możliwe. Do błędów, które trudno znaleźć lub w ogóle jest to nie do zrealizowania należą przede wszystkim błędy popełniane w czasie rejestracji, przenoszenia na MND, lub wczytywania danych kwantyfikujących, dotyczących wielkości ilościowych /np. ilości materiałów, czas pracy sprzętu, liczba powstałych uszkodzeń/. Część tych błędów można łatwo zauważyć jak np. liczba przejechanych przez pojazd w ciągu doby kilometrów, przekraczająca możliwości techniczne pojazdu lub staż pracy za-

wodowej pracownika nie odpowiadający jego wiekowi, uzyskanie tytułów wojskowych lub naukowych w zbyt krótkich terminach, wydanie z magazynu ilości materiałów przekraczających aktualny stan posiadania. Błędów tych nie można zauważyć w czasie wprowadzania danych, można to zrobić dopiero przy realizacji kolejnej fazy procesu przetwarzania danych /np. aktualizacji zbiorów danych ewidencyjnymi/ lub w końcowej fazie przy opracowywaniu informacji wynikowej przed wprowadzeniem jej z systemu informatycznego.

3. Zasady organizacji systemu kontroli danych w systemach informatycznych

W pełnym cyklu procesu przetwarzania danych, od pomiaru /rejestracji/ danych aż do informacji wynikowej, występuje wiele operacji wykonywanych ręcznie lub automatycznie z wykorzystaniem różnych środków techniki obliczeniowej. Przedmiotem tych operacji są zawsze dane wejściowe, wynikiem - odpowiednio przetworzone dane. W tej sytuacji, gdy mamy zawsze do czynienia z danymi i z przeprowadzaniem na nich różnych operacji /obliczeniowych, organizacyjnych/ należy się liczyć z możliwością wystąpienia błędów.

Dążąc do zmniejszenia liczby błędów lub do całkowitego ich wyeliminowania z procesu przetwarzania, stosuje się wybrane metody szukania ich analizowania, określenia ich typu oraz formy ich skorygowania lub zasygnalizowania błędnej sytuacji w sposób zrozumiały dla człowieka.

Prawidłowo funkcjonująca kontrola zapewnia uzyskanie wyników odpowiadających rzeczywistości przy minimum nakładów, co jest jej głównym celem.

Projektując system kontroli należy przestrzegać pewnych zasad:

- kontrola i weryfikacja danych powinny zapewnić osiągnięcie pożądanego poziomu wiarygodności danych na wyjściu systemu informatycznego /SI/,
- kontrola nie może wpływać na parametry systemu informatycznego /na terminowość, pracochłonność, koszt/,
- kontrola i weryfikacja danych nie może być podstawowym celem systemu informatycznego lecz tylko jedną z jego funkcji,
- błędów należy szukać w miejscu ich powstawania bądź w najbliższej im fazie procesu przetwarzania danych,
- sposób znalezienia i sygnalizacji błędów musi zapewnić jednoznaczną identyfikację złej sekwencji danych,
- informacje o błędach powinny być przekazywane tym komórkom organizacyjnym, które są źródłem danych lub odpowiadają za poprawność danych, bądź są uprawnione /mają możliwości/ do ich korekty,

- warunki techniczne powinny zapewnić możliwość włączenia poprawionych danych do procesu przetwarzania,
- system kontroli musi obejmować cały proces przetwarzania danych tj. od momentu rejestracji danych aż do zweryfikowania przydatności i poprawności uzyskanej informacji wynikowej.

Zasięg i złożoność systemu kontroli danych uwarunkowane jest wymaganiami dotyczącymi kompletności i wiarygodności informacji wynikowej oraz terminem dostarczenia jej użytkownikom.

Należy tu podkreślić sprzeczność tych dwóch wymagań, gdyż zwiększenie stopnia kompletności i wiarygodności pociąga za sobą wydłużenie czasu przetwarzania wpływa na to: analiza, korekta, powtarzanie niektórych przebiegów procesu przetwarzania danych.

W zależności od wymagań, system kontroli wiarygodności danych może być mniej lub bardziej złożony. Duże różnice w systemach informatycznych i w wymaganiach dotyczących wyników przetwarzania uniemożliwiają omówienie wszystkich wariantów organizacji systemu kontroli danych. W związku z tym organizacja ta powinna być oparta na następujących założeniach:

- elementy procesu przetwarzania danych powinny być zaprojektowane z uwzględnieniem wymagań systemu kontrolnego,
- system informatyczny należy do systemów, w których dane są przetwarzane w skali masowej o dużym stopniu kompletności i wiarygodności informacji wynikowej,
- w ośrodku przetwarzania danych muszą istnieć wydzielone komórki zajmujące się wstępnym przygotowaniem dokumentów źródłowych /przyjmowanie, kontrola, paczkowanie/, sporządzaniem i kontrolą maszynowych nośników informacji, ponadto musi być wyznaczony operator systemu, odpowiedzialny za eksploatację systemu informatycznego,
- rejestracja danych o zjawiskach i zdarzeniach powinna być zrobiona na formularzach /bezpośrednia rejestracja danych na maszynowych nośnikach w niczym nie narusza koncepcji systemu kontroli, gdyż powoduje jedynie wyeliminowanie jednego lub kilku ogniw procesu przetwarzania danych/.

4. Programowa metoda weryfikacji danych

W czasie przetwarzania danych można wyróżnić następujące fazy procesu produkcyjnego:

- wstępne przygotowanie danych,
- przygotowanie maszynowych nośników informacji,
- elektroniczne przetwarzanie danych,
- końcowe przygotowanie informacji dla użytkowników.

Faza 1 - wstępne przygotowanie danych

W wypadku, gdy dane do przetwarzania są dostarczone przez użytkownika na dokumentach źródłowych /pierwotnych/, przyjęciu ich powinna towarzyszyć operacja obróbki i kontroli wstępnej danych. Obróbka wstępna polega na rejestracji liczby spływających dokumentów, obliczaniu liczby kartpozycji, sporządzeniu arkusza sum kontrolnych. Do kontroli wstępnej zaliczamy: sprawdzenie pod względem formalnym dokumentów /czy są wypełnione zgodnie z wymogami systemu określonymi w instrukcji/ paczkowanie i przygotowanie dokumentów do perforacji.

Faza II - przygotowanie maszynowych nośników informacji

Paczki sprawdzonych dokumentów mają tzw. karty obiegowe i są przekazywane na stanowiska przygotowania maszynowych nośników danych. Przygotowanie kompletnego zbioru wymaga kontaktów z dostawcami dokumentów. Ponieważ nie zawsze jest to możliwe, pojawiają się dodatkowe błędy wynikające z mało czytelnego wypełnienia dokumentów i ewentualnych pomyłek perforatorek MNI. Część z tych błędów zostaje zauważona i usunięta przy sprawdzaniu poprawności przygotowanych danych, pozostałe zaś, jak logiczne powinny zostać ujawnione w fazie elektronicznego przetwarzania danych.

Faza III - elektroniczne przetwarzanie danych

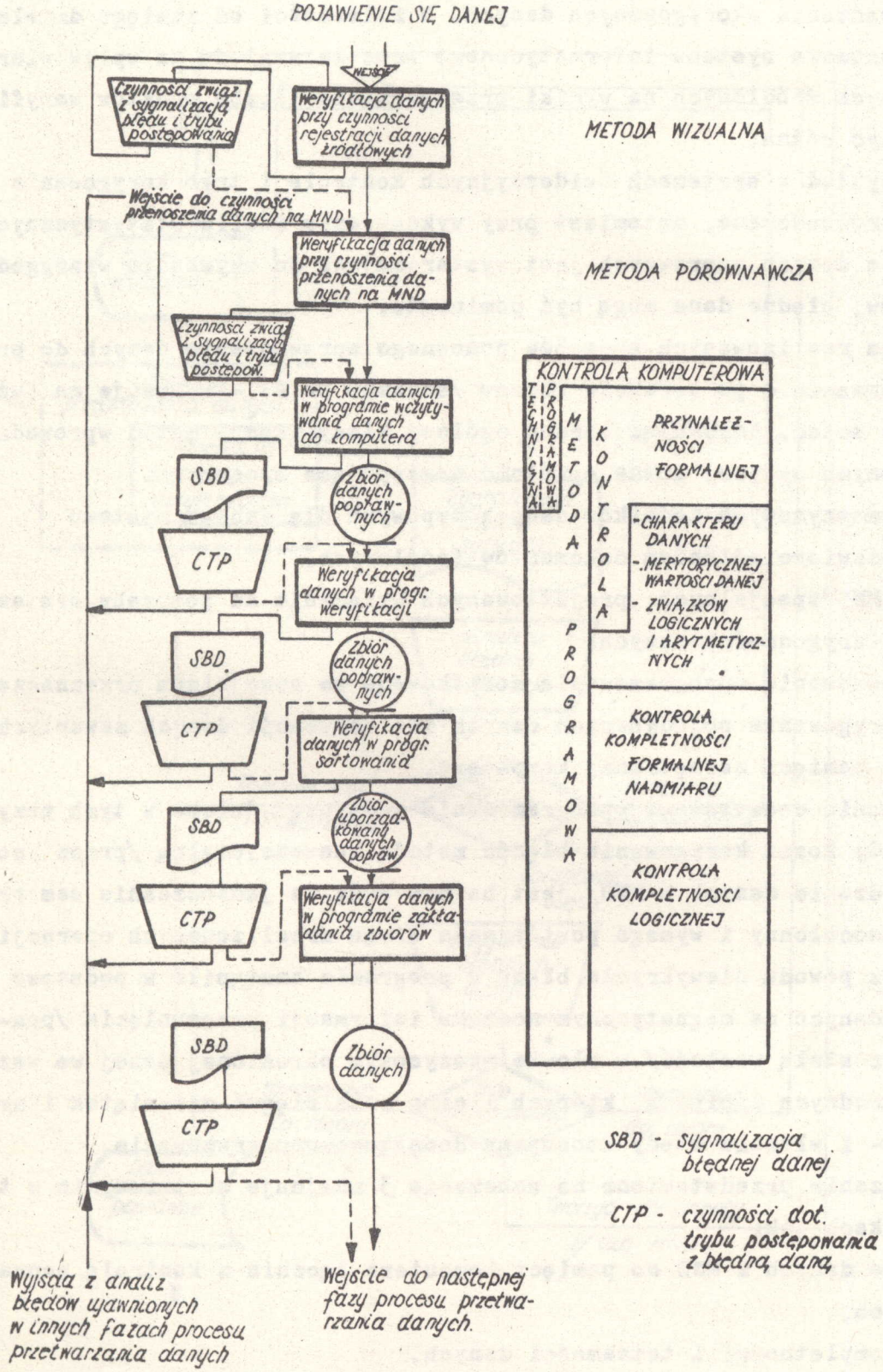
Przygotowane przez dział MNI partie nośników danych muszą być wprowadzone do zbiorów systemu informatycznego. Do najbardziej optymalnych metod weryfikacji wprowadzonych danych należy metoda programowa. Polega ona na zastosowaniu kilku odrębnych programów lub podprogramów, które różnią się możliwościami znalezienia błędów i miejsca ich powstawania. W metodzie tej ujawnienie błędu jest wynikiem wykrycia przez komputer sprzeczności jednego z podstawowych warunków logicznych, jakie powinny spełniać dane przed wykonaniem określonej fazy przetwarzania /np. awansowanie pułkownika do stopnia kapitana/ lub gdy nie ma odpowiednika przynależnościowego w ewidencji komputerowej /np. ujęto dane aktualizujące, a w ewidencji takiej pozycji nie ma/. Są też znajdowane inne błędy występujące we wprowadzanych zbiorach danych np. wynikające z niewłaściwej perforacji, nieodpowiedniego wypełnienia dokumentów źródłowych, które nie zostały wcześniej zauważone.

Proces weryfikacji wprowadzanych do systemu informatycznego danych można przedstawić w postaci schematu nr 1.

Na schemacie pokazane są typowe operacje procesu przetwarzania danych, zawierające procedury kontrolno-weryfikacyjne, sposób sygnalizowania znalezionych błędów /SBD/ oraz czynności analizy i korekty.

Schemat 1

Elementy weryfikacji danych w procesie wprowadzania danych do bazy systemu informatycznego.



Podstawowe powiązanie funkcjonalne między elementami systemu kontroli a elementami systemu informatycznego, wskazujące kolejność operacji i czynności w danym przebiegu przetwarzania pokazane zostały za pomocą linii ciągłej. Linia przerywana wskazuje zaprojektowanie alternatywnych rozwiązań wprowadzania skorygowanych danych. W zależności od zasięgu działania, przeznaczenia systemu informatycznego oraz ze względu na wpływ wiarygodności danych źródłowych na wyniki przetwarzania, liczba punktów weryfikacji może być różna.

Na przykład w systemach ewidencyjnych kontrola i tryb korygowania będą bardzo rozbudowane, natomiast przy wykonywaniu analiz statystycznych, jeżeli liczba danych poprawnych jest wystarczająca do uzyskania wiarygodności wyników, błędne dane mogą być pominięte.

Analiza realizowanych sposobów ponownego wprowadzania danych do procesu przetwarzania - po korekcie błędów /schemat nr 2/ - wskazuje na dużą różnorodność metod. Dokonując bardzo ogólnej klasyfikacji metod wprowadzania poprawionych danych, można wyróżnić następujące sposoby:

- za pomocą maszynowych nośników danych typowych dla danego systemu, i będących odzwierciedleniem dokumentów źródłowych,
- za pomocą MND specjalnych, projektowanych wyłącznie na potrzeby systemu kontroli wiarygodności danych,
- przez zastosowanie oprogramowania dodatkowego ze specjalnym przeznaczeniem do korygowania pojedyńczych danych lub sekwencji danych zawartych w zbiorach pamięci zewnętrznej komputera.

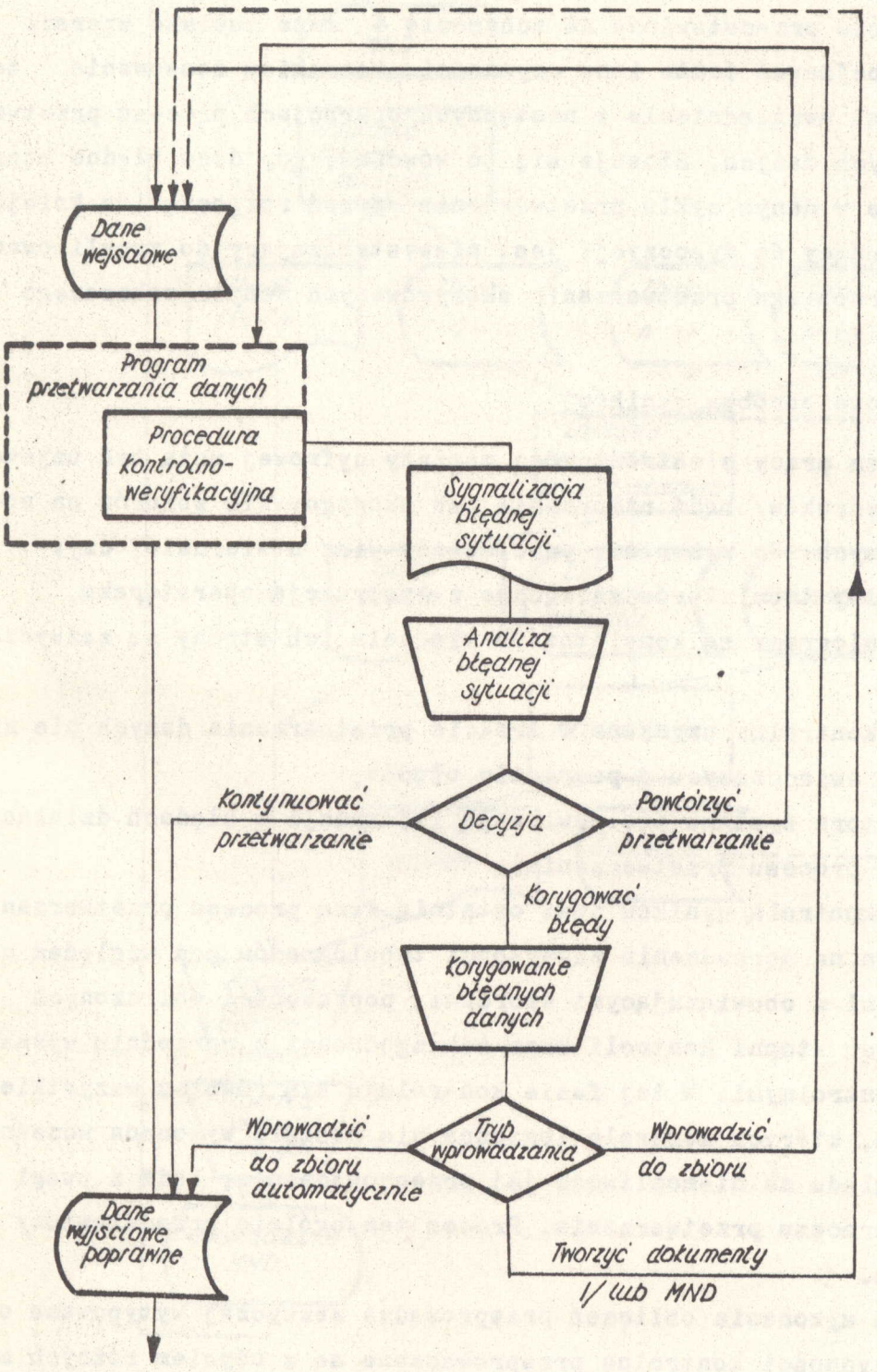
Stosowanie dodatkowego oprogramowania jest uzasadnione w tych przypadkach, kiedy koszt korygowania błędów metodą konwencjonalną /przez ponowne wprowadzenie danych z MND/ jest bardzo duży, a jednocześnie sam proces jest czasochłonny i wymaga powtórzenia wielu zrealizowanych operacji. Na przykład z powodu niewykrycia błędu w programie nastąpiło w podstawowym zbiorze danych na magnetycznym nośniku informacji przesunięcie /pomnożenie przez stałą wartość/ w słowie maszynowym określonej danej we wszystkich jednorodnych zapisach, których liczba może sięgać dziesiątek i setek tysięcy - i właśnie wtedy stosujemy dodatkowe oprogramowanie.

Rozwiązanie przedstawione na schemacie 3 znajduje zastosowanie w takich przypadkach jak:

- wczytywanie danych z MND do pamięci komputera łącznie z kontrolą poprawności danych,
- kontrola kompletności i tożsamości danych,
- okresowa aktualizacja zbioru podstawowego.

Schemat 2

Analiza i korekta błędów oraz ponowne wprowadzanie danych do systemu informatycznego.



Warunkiem stosowania tego rozwiązania powinno być dysponowanie odpowiednim okresem umożliwiającym włączenie skorygowanych danych /bez wpływu na wiarygodność informacji wynikowej/ do przetwarzania w następnym cyklu lub następnej operacji - przez zorganizowanie dodatkowego przebiegu tylko dla poprawionych danych.

Rozwiązanie przedstawiono na schemacie 4 może znaleźć szersze zastosowanie i obejmować także inne czynności. Warunkiem stosowania tego rozwiązania jest uwzględnienie w następnych operacjach procesu przetwarzania skorygowanych danych. Stosuję się to wówczas, gdy dane błędne muszą być skorygowane w danym cyklu przetwarzania /przed rozpoczęciem kolejnej operacji/, a będący do dyspozycji jest niewystarczający do zrealizowania podstawowego przebiegu przetwarzania skorygowanych danych pokazanego na schemacie 3.

Faza IV - końcowa obróbka wyników

Rezultatem pracy elektronicznej maszyny cyfrowej może być uzyskanie tabulatorów /wydruków/ bądź utworzenie lub skorygowanie zbiorów na nośnikach magnetycznych. Po wykonaniu prac należy więc stwierdzić, czy:

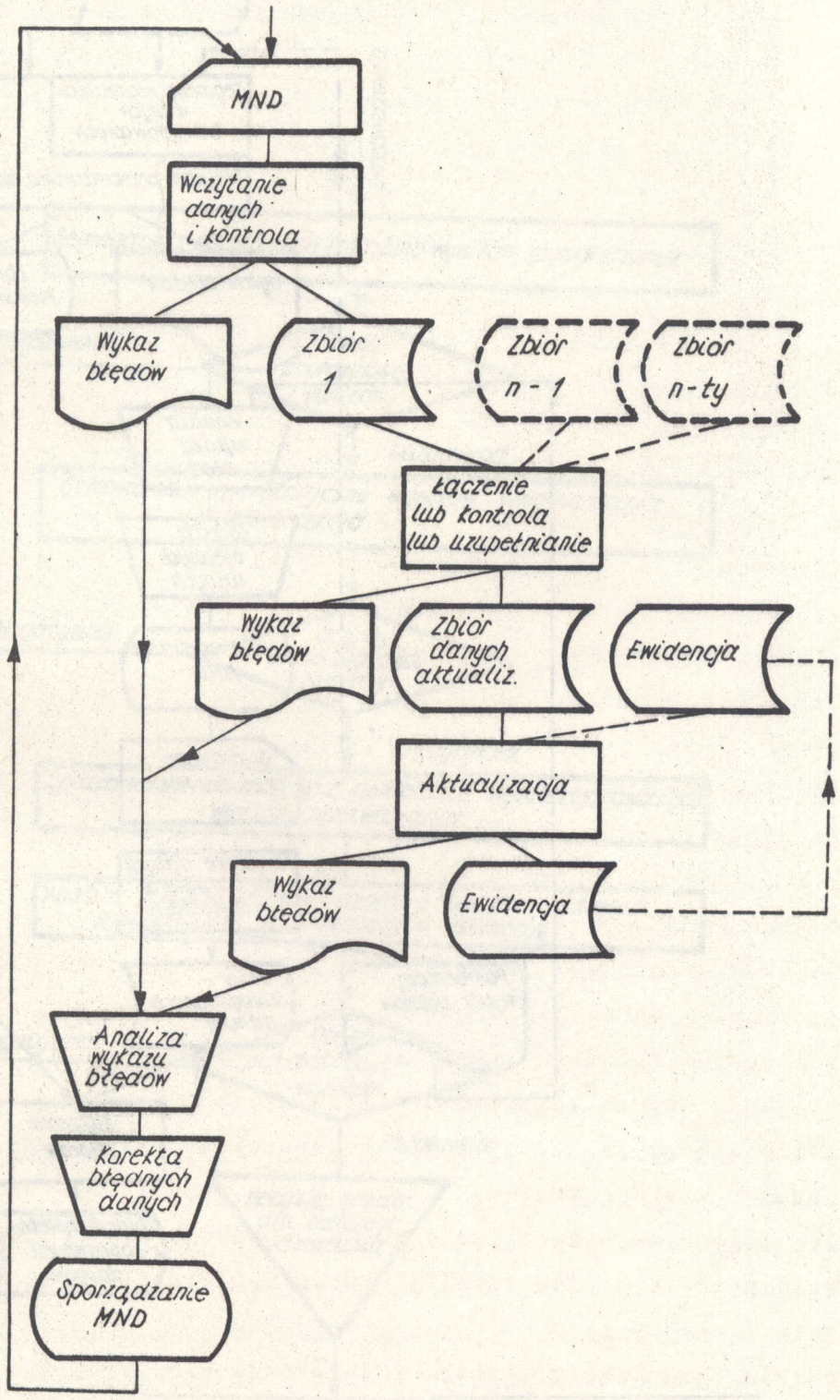
- liczba i rodzaj tabulatorów są zgodne z instrukcją operatorską,
- uzyskane tabulogramy są kompletne /w tym celu ich strony są zazwyczaj numerowane/,
- tabulogramy kontrolne uzyskane w trakcie przetwarzania danych nie zawierają pozycji świadczących o powstaniu błędów,
- wydruki monitora systemu nie zawierają informacji o błędach działania urządzeń lub procesu przetwarzania.

Końcowa kontrola wyników jest ostatnią fazą procesu przetwarzania danych i polega na sprawdzeniu zawartości tabulogramów pod względem czytelności, zgodności z obowiązującymi wzorcami, poprawności obliczonych sum według kolejnych stopni kontroli oraz ich zgodności z uprzednio wyznaczonymi sumami kontrolnymi. W tej fazie kontroluje się również wszystkie elementy rachunku, których kontrola logiczna nie została wykonana wcześniej bądź to ze względu na niemożliwość jej przeprowadzenia, bądź z uwagi na uproszczenie procesu przetwarzania. Proces ten ogólnie przedstawiony jest na schemacie 5.

Kontrolę wykonania obliczeń przeprowadza zazwyczaj wytypowana osoba lub zespół. Czynności kontrolne przeprowadzane są z użyciem różnych metod i środków technicznych. W większości wypadków polegają one na wzrokowym sprawdzeniu cech zewnętrznych tabulogramów i oszacowaniu wiarygodności

Schemat 3

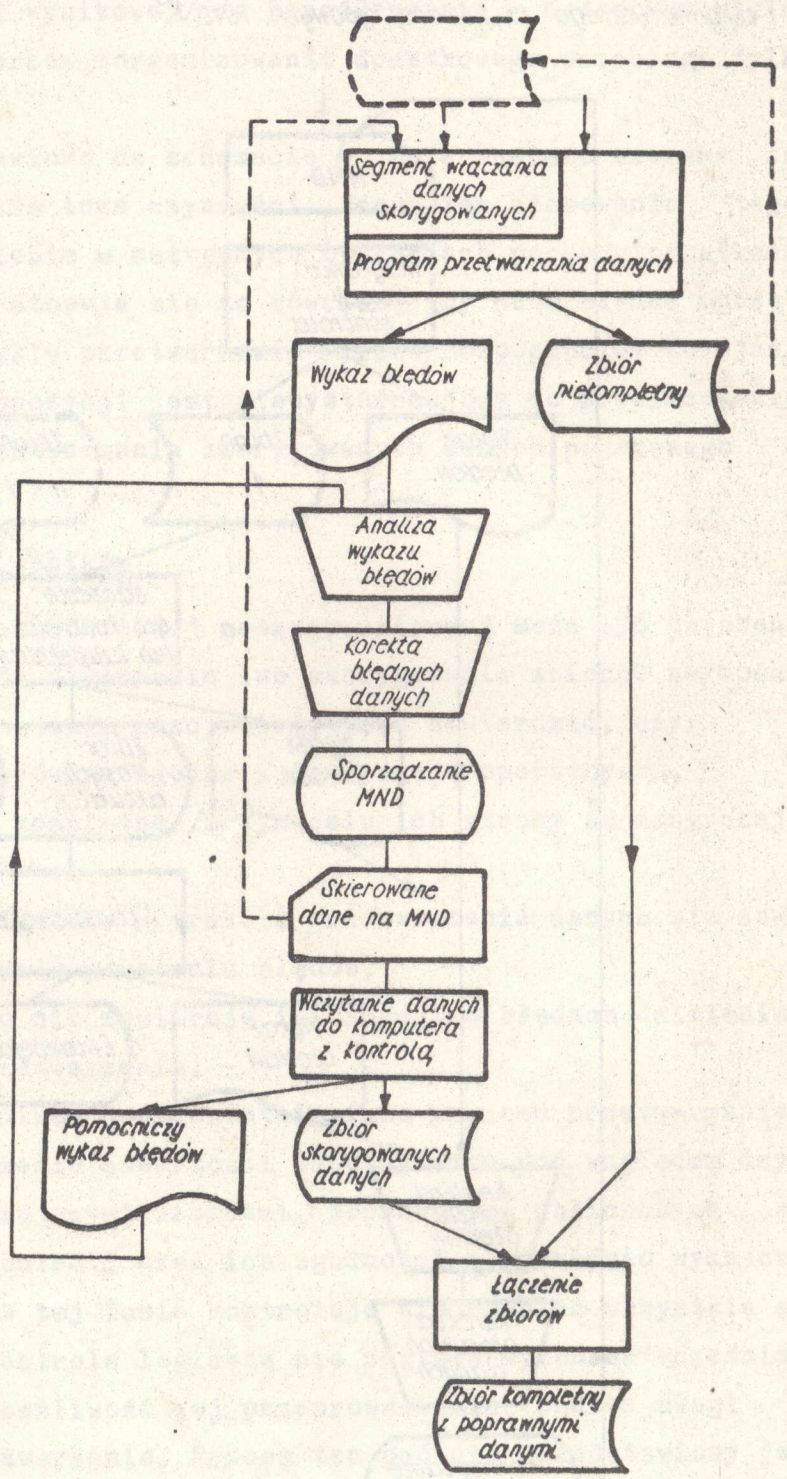
Organizacja wprowadzania skorygowanych danych do zbiorów systemu informatycznego za pomocą typowych MND. [1]



[1] B. Busko, J. Śliwieński, Eksploatacyjno - organizacyjne problemy zabezpieczania wiarygodności danych w SI, Informatyka 1976, nr 10, s. 10.

Schemat 4

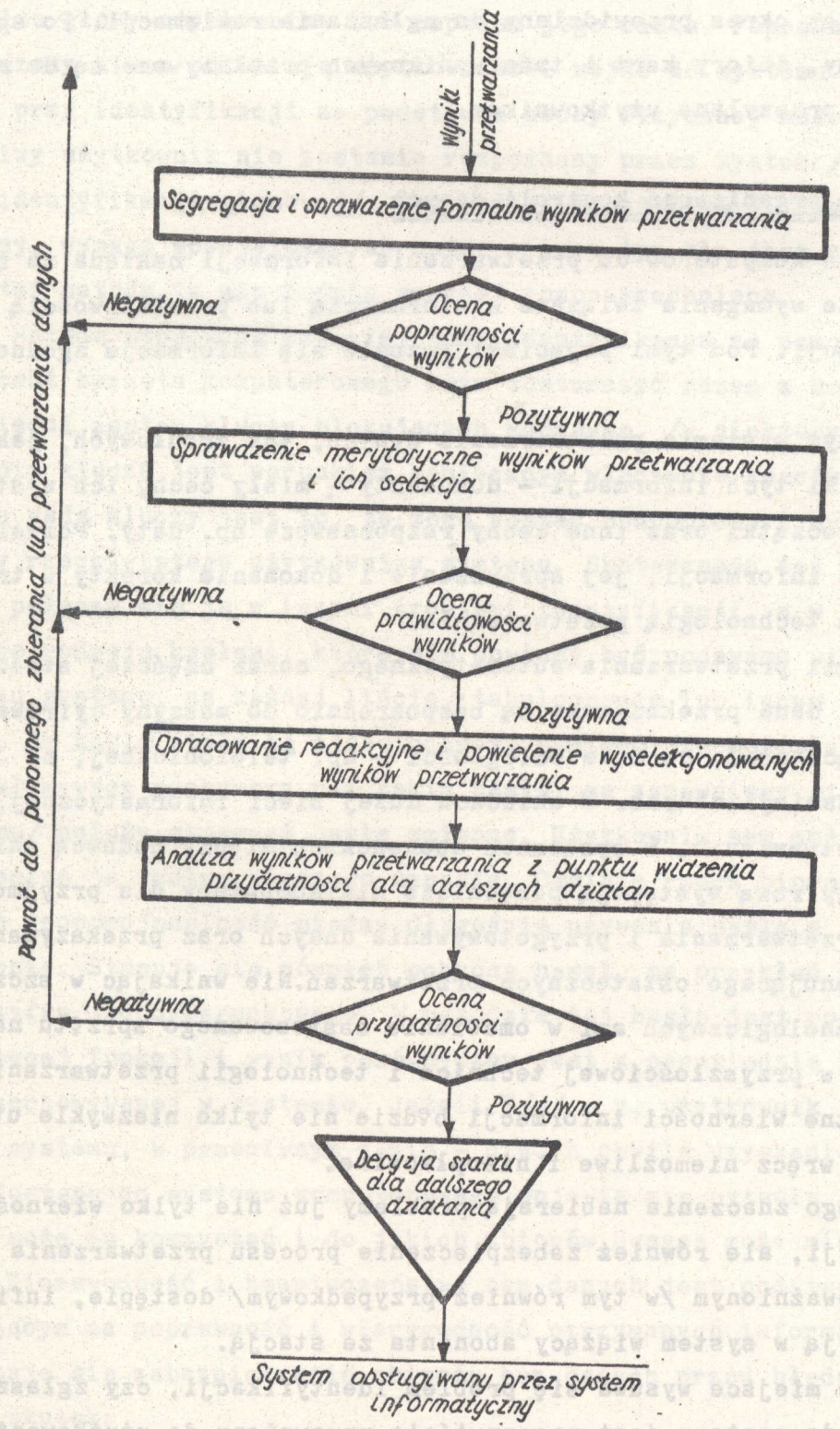
Organizacja wprowadzania skorygowanych danych do zbiorów systemu za pomocą specjalnych MND.[1]



[1] B. Busko, J. Śliwiński, Eksploatacyjno-organizacyjne, op. cit., s. 11.

Schemat 5.

Ogólny proces końcowej obróbki wyników. 1/



1/ M. Ciesielski, Systemy informatyczne w drogownictwie, WKiŁ, Warszawa 1977, s. 35.

otrzymanych wyników. W sytuacji zauważenia błędu kontrolowany jest szczegółowo cały tabulogram, w celu wykrycia mechanizmu powstania błędu.

Tabulogramy błędne, których odręczne skorygowanie jest niemożliwe, zwracane są do powtórnego opracowania. Wszystkie dokumenty związane z kontrolą obliczeń i rozliczeniem czasu pracy przechowywane są w ośrodku obliczeniowym przez okres przewidziany do zgłaszania reklamacji. Po sprawdzeniu tabulogramy, zbiory kart i taśm wynikowych przekazywane są do zarejestrowania oraz przesyłane użytkownikom.

5. Przyszłościowa organizacja kontroli danych

Zastosowanie komputerów do przetwarzania informacji nakłada na źródła informacji duże wymagania związane z wiernością lub prawidłowością generowanej informacji. Pod tymi pojęciami rozumie się informacje zgodne z rzeczywistością.

W tradycyjnym systemie przetwarzania danych, tak źródłowych, jak i wynikowych, nośniki tych informacji - dokumenty - miały cechy ich wystawców: podpisy i pieczątki oraz inne cechy rozpoznawcze np. daty. Pozwalało to na odtworzenie informacji, jej sprawdzenie i dokonanie korekty w trybie przewidzianym technologią przetwarzania.

W technologii przetwarzania automatycznego, coraz częściej stosowanej, informacje i dane przekazywane są bezpośrednio do maszyny cyfrowej drogą szybkiej łączności, na duże odległości - np. telefonicznej, za pomocą środków transmisji danych. W układach dużej sieci informatycznej, przy zdalnym przetwarzaniu, w systemach abonenckich między nadawcą informacji a maszyną cyfrową występują pomocnicze minikomputery dla przyjmowania, wstępnego przetwarzania i przygotowywania danych oraz przekazywania do komputera dokonującego ostatecznych przetwarzań.Nie wnikając w szczegóły rozwiązań technologicznych ani w omawianie zastosowanego sprzętu należy stwierdzić,że w przyszłościowej technice i technologii przetwarzania sprawdzanie zwrotne wierności informacji będzie nie tylko niezwykle utrudnione, ale nawet wręcz niemożliwe i nieopłacalne.

Tym większego znaczenia nabierają problemy już nie tylko wierności danych i informacji, ale również zabezpieczenie procesu przetwarzania danych przed nieupoważnionym /w tym również przypadkowym/ dostępie, infiltracją i ingerencją w system wiążący abonenta ze stacją.

Na pierwsze miejsce wysuwa się problem identyfikacji, czy zgłaszający się ze stacji do systemu jest rzeczywiście uprawniony do użytkowania jej. Można wyróżnić trzy podstawowe metody identyfikacji przez:

- cechę fizyczną użytkownika,
- przedmiot należący do użytkownika,
- informację znaną użytkownikowi.

Badając metodę pierwszą próbowano wykorzystać wiele ludzkich cech fizycznych, począwszy od analizy głosu a skończywszy na wykorzystaniu kształtu głowy użytkownika lub zapachu jego ciała. Poprawne hasło czy nie uszkodzony klucz pozwalają użytkownikowi wejść do systemu zawsze, natomiast przy identyfikacji na podstawie cechy fizycznej może się zdarzyć,że właściwy użytkownik nie zostanie rozpoznany przez system /np. zakatarzenie przy identyfikacji głosowej/. Ten rodzaj identyfikacji jest wyjątkowo kosztowny, wymaga specjalnego sprzętu, a przy tym nie jest niezawodny. Dlatego też metoda ta nie będzie szerzej rozpowszechniana.

Metodą stosowaną częściej jest identyfikacja za pomocą przedmiotu. Producent sprzętu komputerowego może dostarczyć razem z końcówką abonencką odpowiedni zestaw kluczy blokujących końcówkę, /w niektórych wypadkach włożenie klucza jest warunkiem koniecznym włączenia końcówki do sieci/. Główną wadą kluczy jest to, że mogą zostać podrobione i wykorzystane bez wiedzy rzeczywistego użytkownika systemu. Skuteczność tej metody wzrasta jeśli połączy się ją z innymi środkami identyfikacji, a w szczególności z różnego rodzaju hasłami, które nie powinny być podawane wizualnie w żadnym miejscu systemu, na każdej liście, tabulogramie lub innym nośniku. Z uwagi na to, że hasła stałe są słabą ochroną systemu /są dość łatwo przełamywalne, włamywacz zdobywszy raz takie hasło, ma zapewniony stały dostęp do systemu/ należy stosować hasła zmienne. Użytkownik sam może tworzyć hasła i zmieniać je według własnego uznania. Ogólnie rzecz biorąc, istnieje odwrotna proporcjonalność między długością używania hasła a stopniem zabezpieczenia. Stosuje się również ochronę haseł, na przykład przez wprowadzenie szyfru jednokierunkowego. W metodzie tej hasło jest poddawane działaniu pewnej funkcji i wynik porównywany jest z odpowiednią pozycją w tablicy przechowywanej w systemie. Jeżeli $F/x/ = y$, użytkownik jest dopuszczany do systemu, w przeciwnym razie - nie. Z chwilą uzyskania przez użytkownika dostępu do systemu komputerowego pojawia się pytanie, z jakich programów może on korzystać i do jakich zbiorów danych może mieć dostęp.

Niezawodność i bezpieczeństwo baz danych jest podstawowym problemem rzutującym na poprawność i wiarygodność otrzymanych informacji. Koniecznym staje się zabezpieczenie zbiorów baz danych przed błędami powstającymi na skutek:

- niewłaściwego użycia,
- zniszczenia,

- niepowołanego dostępu do zbiorów,
- interferencji,
- konteminacji,
- konfliktu jednoczesnego dostępu.

Trzy ostatnie czynniki są źródłem wielu błędów w bazie danych pracującej w trybie konwersacyjnym.

Najnowsze systemy operacyjne zapewniają zabezpieczenie baz danych przez system kontroli dostępu użytkowników oraz okresowe składowanie zbiorów, umożliwiające ich odtworzenie.

Przedstawione metody kontroli dostępu do danych nie gwarantują pełnego zabezpieczenia przed błędami systemowymi zarówno oprogramowania, jak i sprzętu technicznego. W celu zmniejszenia wrażliwości systemu na błędy tego typu w najnowszych rozwiązaniach maszyn cyfrowych programy kontroli i ochrony tworzą pakiet, w którym poszczególne metody protekcji realizowane są obok siebie. Tylko bowiem kompleksowe ujęcie problemu pozwoli w maksymalnym stopniu uzyskać wiarygodność i informacje. Pełna odpowiedzialność za prawidłowość przewidzianych etapów kontrolnych systemu informatycznego leży w gestii projektantów i programistów. Zadaniem ich jest takie skonstruowanie programów, aby zostały wychwycone wszystkie nieprawidłowości logiczne przekazywanej informacji.

6. Wnioski

Jednym z istotnych elementów, który powinien występować zawsze przy projektowaniu systemów informatycznych, jest zapewnienie odpowiedniego poziomu jakości otrzymywanej informacji. Wartość wytwarzanej przez system informatyczny informacji - jako parametr określający jego efektywność - jest niezmiernie trudna do ustalenia. Wynika to przede wszystkim z wieloaspektowości systemów, a tym samym i odmiennego oceniania tych samych informacji w ramach różnych zastosowań. Oceny funkcjonowania systemu można natomiast dokonywać, analizując i oceniając kształtowania się wiarygodności, kompletności i terminowości wytwarzanej informacji.

Czynniki te w sposób bezpośredni wpływają na wartość wytwarzanej informacji, są łatwe do określenia i przeprowadzenia oceny zarówno dla poszczególnych zastosowań, jak i w ujęciu kompleksowym. Ich rola wzrasta szczególnie w warunkach stosowania wspólnej bazy danych, gdyż w tym przypadku funkcje zbierania i wykorzystania informacji są rozłączne. Ponieważ w procesie pomiaru i rejestracji oraz wprowadzania informacji do wspólnej bazy danych uczestniczą ludzie oraz są stosowane środki techniczne o określonej

niezawodności, należy liczyć się z tym, że przekłamania mogą wystąpić we wszystkich fazach procesu przetwarzania, zarówno w sferze działania systemu /np. ,nieprawidłowo sporządzanie maszynowego nośnika danych, wadliwie działające urządzenie, błędy w programach/ jak też i poza sferą tzn. w obrębie współpracujących ogniw organizacyjnych lub otoczenia /np. w zakresie pomiaru zdarzenia, przekazywania danych/. Każde przekłamanie, które nie zostanie wykryte - w zależności od stopnia wykorzystania danej sekwencji informacji - może zniekształcać wyniki wszystkich lub części zastosowań, korzystających z informacji znajdujących się w bazie danych, a ich zasięg jest zależny od rodzaju danych. W przypadku danych zmiennych zasięg od - działywania jest ograniczony, natomiast przy danych stałych może stać się powodem całego łańcucha przekłamań.

Ujmując problematykę kontroli danych całościowo nie można ograniczyć się wyłącznie do tej części procesu przetwarzania danych, które jest realizowana przez wyspecjalizowane, wydzielone organizacyjnie komórki ośrodka obliczeniowego. Skuteczne przeciwdziałanie przekłamaniom w systemach informatycznych będzie efektywne dopiero wtedy, gdy będzie obejmować cały proces przetwarzania danych począwszy od pomiaru i pierwotnej rejestracji danych o zdarzeniu, kończąc zaś na analizie i wykorzystaniu informacji wynikowej.

Należy pamiętać, że podstawowym "źródłem" błędów i przekłamań jest człowiek. Należy go jednak również widzieć jako: istotny element procesu wykrywania nieprawidłowości w realizacji oraz podstawowy element procesu podejmowania decyzji /korygowanie lub pomijanie wykrytych błędów/. Dopiero takie ujęcie umożliwia ustalenie wszystkich prawdopodobnych miejsc i przyczyn powstawania zakłóceń lub błędów oraz pozwala na opracowanie systemu kontroli, który zapewniałby osiągnięcie wymaganego stopnia wiarygodności przetwarzania danych.

System kontroli powinien być projektowany równolegle i w sposób podobny ,jak system informatyczny. Nie może on być tworzony, jak najczęściej do tej pory ma miejsce, na zasadzie dowolności bądź intuicji projektanta oraz realizowany w sposób fragmentaryczny i niezależny od całego systemu. Określenie wymaganego poziomu wiarygodności w systemie powinno być oparte na wnikliwej analizie i ocenie znaczenia informacji wyjściowej dla potrzeb efektywnego zarządzania oraz na analizie skutków odchyleń rzeczywistej wiarygodności od zakładanej. Poziomu tego nie można zawyżać, ponieważ wzrost wiarygodności informacji jest związany ze wzrostem kosztów projektowania i eksploatacji systemu. Obok wymagań dotyczących wiarygodności informacji wynikowej muszą być uwzględnione wyniki wszechstronnej analizy

teoretycznych możliwości wystąpienia przekłamań oraz faktycznego stanu jakości pracy poszczególnych ich elementów /urządzeń, ludzi/. Pozwoli to nie tylko na właściwy dobór środków technicznych i organizacji procesu przetwarzania danych, ale ponadto umożliwi ustalenie najodpowiedniejszych metod i środków weryfikacji prawidłowości jak i sposobu umiejscowienia danych w procesie przetwarzania.

Należy jednak podkreślić, że w obecnych warunkach brak jest wielu przesłanek do zrealizowania w pełni wymienionych postulatów. Wynika to z powierzchownego lub fragmentarycznego naświetlenia tego problemu w literaturze fachowej, dotyczącej metodyki projektowania systemu informatycznego oraz z braku publikacji w zakresie uzyskanych doświadczeń lub wyników badań.

Bibliografia

1. Automatyczne przetwarzanie informacji pod red. Z.Hellwiga, PWE, Warszawa 1977 r.
2. BAZEWICZ M. Wielodostępne systemy informatyczne, PWN, Warszawa 1976 r
3. BUŚKO B., ŚLIWIEŃSKI J. Eksploatacyjno-organizacyjne problemy zabezpieczenia wiarygodności danych w SI, Informatyka nr 10, 1976 r.
4. BUŚKO B., ŚLIWIEŃSKI J. Jakość informacji w systemach informatycznych, Informatyka 1976, nr 4
5. CIESIELSKI M. Systemy informatyczne w drogownictwie, WKiŁ, Warszawa 1977
6. FISCHER E. Systemy abonenckie, WNT, Warszawa 1977
7. HORN D., BUSCH N. Datensicherung in System der EDV. VEB Kombinat Robotron, Dresden 1970
8. KOTOWSKI M. Identyfikacja użytkownika w systemach wielodostępnych, Informatyka 1977, nr 6
9. MISZCZAK M. Ochrona danych w systemach informatycznych, Wojskowy Przegląd Organizacji i Informatyki 1977, nr 1
10. ŚLIWIEŃSKI J. Sposoby kontroli wiarygodności w procesie przetwarzania, Informatyka 1976, nr 5
11. Rozproszone przetwarzanie danych, Europejski Program Badawczy Dieblda, OBRI 1977, z. 91

Tadeusz JAEGERMANN
Stefan SEMCZUK

OCHRONA DANYCH W GŁÓWNYM URZĘDZIE STATYSTYCZNYM

Szczególne akcentowanie w Głównym Urzędzie Statystycznym problematyki ochrony danych wynika z faktu, że w resorcie tym przechowuje się zbiory danych o wielkiej wadze dla funkcjonowania aparatu państwowego, przy konieczności zachowania tzw. prywatności w stosunku do zapisów indywidualnych respondentów.

Proces przetwarzania danych, obejmuje w warunkach GUS obszerne cykle rozpoczynające się od zbierania "surowych" danych, a kończące się na przekazywaniu wynikowych tablic zleceniodawcom. Są nimi przede wszystkim departamenty branżowe GUS, instytucje państwowe i społeczne, czynniki polityczne, instytucje naukowe, międzynarodowe instytucje statystyczne.

W Głównym Urzędzie Statystycznym, ochronie podlegają wszystkie dane statystyczne, niezależnie od ich formalnej kwalifikacji. W praktyce jednak zakres i metody ochrony są zróżnicowane zarówno ze względu na koszty, jak i na koncentrację uwagi na miejscach szczególnie wrażliwych.

W wyniku wieloletniego doświadczenia GUS ma osiągnięcia w zakresie kontroli danych we wszystkich fazach przetwarzania. Szczególny akcent jest położony na fazę:

- wielostopniowego "czyszczenia" danych "surowych" /przy współpracy ze zleceniodawcami i respondentami/,
- programowej kontroli zbiorów o znacznym stopniu skomplikowania /w trybie przetwarzania wsadowego/,
- automatycznej kontroli zgodności z komputerowo aktualizowanym katalogiem [1/] jednostek sprawozdawczych /REGON/

Te osiągnięcia warsztatowe statystyki państwowej będą nadal rozwijane i wykorzystywane w całokształcie ochrony danych. Nie mniej jednak aktualny poziom technologii przetwarzania danych, a w pierwszym rzędzie zarysowujące się zmiany w tej technologii wymagają wprowadzenia bardziej nowoczesnego, kompleksowego systemu ochrony danych. W związku z tym w marcu 1978 r. ukazało się Zarządzenie Dyrektora Naczelnego Zarządu Mechanizacji i Automatyzacji Opracowań Statystycznych Głównego Urzędu Statystycznego, wprowadzające ramowe wytyczne ochrony danych w 10 ośrodkach komputerowych statystyki państwowej [2/]. Wydanie tego zarządzenia, poprzedzone naradami

1/ Nie wszystkie, nawet dobrze wyposażone urzędy statystyczne na świecie dysponują tym udogodnieniem.

2/ Przez ochronę danych rozumie się w GUS stwarzanie warunków zabezpieczających przed przypadkowym lub rozmyślnym /a nie autoryzowanym/ ujawnieniem, zniekształceniem lub zniszczeniem danych, oprogramowania, dokumentacji, haseł, zapisów historii systemu itp.

z dyrektorami tych ośrodków było wyrazem potrzeby sformułowania zasad ochrony danych.

Poza ujednoliceniem i zebraniem rozproszonych dotąd instrukcji i przepisów wewnętrznych, funkcjonujących już od wielu lat w ośrodkach GUS, zarządzenie to było pierwszym krokiem o charakterze jakościowym, zmierzającym do utworzenia w przyszłości wyodrębnionej /podległej bezpośrednio dyrektorom ośrodków/, wyspecjalizowanej technologicznie służby ochrony danych. Zarządzenie zobowiązywało dyrektorów ośrodków do powierzenia funkcji koordynacyjno-doradczych w dziedzinie ochrony danych specjalistom o dużym doświadczeniu technologicznym.

Wkroczenie aparatu obliczeniowego GUS na teren nowych technologii, które skrótowo określa się mianem banków danych, nie jest bynajmniej odległą perspektywą. Rozwinięty Wojewódzki Bank Danych działa już w OE GUS-Katowice, promieniując na wiele innych ośrodków. System zdalnego przetwarzania funkcjonuje już w Ośrodku WUS w Olsztynie i OE-GUS Wrocław. Przed Ośrodkiem Elektronicznym GUS Warszawa została postawiona realizacja banku danych "Rozwój". Stały wzrost wieloprogramowości w eksploatacji komputerów, pobudzany rozbudową pamięci dyskowych, uzupełnia obraz dążenia pionu obliczeniowego GUS do stosowania coraz nowocześniejszych technologii przetwarzania danych.

Zasadniczym powodem, zwrócenia uwagi informatyków na konieczność zajęcia się problematyką ochrony danych, było uświadomienie sobie wpływu, jaki na metody ochrony, ich stopień dojrzałości i zakres, mają realizowane kierunki zmian w technologii przetwarzania. Konieczność rozbudowy i modernizacji systemu ochrony danych w miarę rozwoju nowych technologii, a więc banków danych ze zdalnym dostępem lub przetwarzania rozproszonych w warunkach sieci komputerów - obserwujemy w krajach o znacznie wyższym niż u nas nasyceniu nowoczesnymi środkami przetwarzania. Można powiedzieć, że istnieje próg rozwoju nowych metod, którego przekroczenie możliwe jest wyłącznie w warunkach wdrożenia i stałego rozwijania precyzyjnie przemyślanego, kompleksowego systemu ochrony danych.

Jeśli nawet stosowane metody ochrony nie grożą dziś poważniejszymi konsekwencjami i są ostatecznie "do przyjęcia", to już jutro staną się one hamulcem wprowadzania nowocześniejszych technologii. Oto teza, którą nowe zarządzenie postawiło przed wszystkimi informatykami pracującymi w pionie obliczeniowym statystyki państwowej.

Ramowe wytyczne podkreślają i rozwijają problematykę fizycznej ochrony środowiska i organizacji przetwarzania. Jest to zrozumiałe, gdyż wprowadzenie na tym odcinku porządku /często małymi kosztami/ warunkuje kolej-

ne wprowadzenie bardziej subtelnych metod ochrony systemowo-logicznej. W literaturze przedmiotu zwraca się uwagę na fakt żenującej niekiedy niefrasobliwości we wprowadzaniu elementarnego porządku, który wbrew przypuszczeniom ma zasadnicze znaczenie dla ochrony systemów komputerowych i zbiorów. Kto będzie chciał ryzykować zakładanie aparatu podsłuchowego na wewnętrzną linię łączącą komputer z końcówką, jeśli potrafi wynieść pod pachą taśmę magnetyczną.

W celu administracyjnego wprowadzenia porządku omawiane zarządzenie zobowiązało dyrektorów ośrodków elektronicznych GUS do sprecyzowania obrębu powierzchni chronionych, w ramach których obowiązują obostrzone metody ochrony. Są to ogólnie stosowane zasady ograniczenia ruchu osób w salach komputerowych, ze szczególnym uwzględnieniem bibliotek /archiwów/ taśm i dysków magnetycznych, sal przygotowania nośników informacji /GUS stosuje elektroniczne rejestratory danych na taśmach magnetycznych/, magazynów międzyoperacyjnych, sal kompletacji wsadu i wyników, sal z końcówkami ekranowymi, magazynów makulatury, archiwów dokumentów źródłowych oraz recepcji /od lady recepcyjnej/.

Do pomieszczeń chronionych zarządzenie zalicza miejsca instalacji niezwykle dla systemów komputerowych wrażliwych urządzeń klimatyzacyjnych, urządzeń zasilających /rozdzielnie niskiego napięcia, przetwornice/ oraz wewnętrzne rozdzielnie kabli telefonicznych, w tym dla teleprzetwarzania.

Wytyczne wprowadzają zasadę kontroli osób wchodzących do pomieszczeń chronionych, choć nie jest to proste do realizacji w warunkach istniejących budynków, z których korzysta większość ośrodków GUS. Na podstawie pierwszych sygnałów osób odpowiedzialnych za wdrożenie można stwierdzić, że wytyczne te wymuszają wyeliminowanie programistów aplikacyjnych i w pewnym zakresie operatorów systemu z sal komputerowych. Jest to istotne usprawnienie, które stwarza niezbędne warunki dla określenia zakresu odpowiedzialności operatorów komputera. Wstęp do biblioteki nośników magnetycznych ma wyłącznie jej obsługa /przy pracy wielozmianowej należy dążyć do obecności bibliotekarza na każdej zmianie/. Praktycy wiedzą jak kłopotliwe jest to zadanie, szczególnie na trzeciej zmianie.

Omawiane zarządzenie określa również zasady bezpieczeństwa chronionych pomieszczeń po zakończeniu pracy, gdy w gmachu pozostaje jedynie wartownik lub portier. Komputer jest wtedy narażony na wiele niebezpieczeństw, a w szczególności - na pożar. Poza zasadą zamykania pomieszczeń na klucz i dokładnymi instrukcjami dla portiera /lub wartowników/ przepisy mówią o niezbyt często stosowanych urządzeniach alarmowych przeciwwłamaniowych, ograniczeniu wglądu do pomieszczeń chronionych przez oszklone drzwi lub okna itd.

Warto tutaj podkreślić, że w zarządzeniu z marca 1978 r. podane są wskazówki dla służby inwestycyjnej, organizującej projektowanie budów nowych ośrodków, przystosowania już istniejących budynków itd. Trudno bowiem idealnie zabezpieczyć budynki już stojące, natomiast nie można dopuścić do realizacji nowych projektów, które nie uwzględniałyby elementarnych zasad ochrony. Temat ten jest przedmiotem dalszych studiów w GUS.

W każdym podręczniku ochrony danych istnieje zawsze osobny rozdział o ochronie przeciwpożarowej i ochronie przed zalaniem urządzeń wodą. Sprawy te nie mogły zostać pominięte w zarządzeniu. Zwraca się szczególną uwagę na pomieszczenia przyległe do sali komputerowej ze specjalnym uwzględnieniem pomieszczeń znajdujących się nad salą. Zaleca się organizowanie okresowej specjalistycznej kontroli urządzeń wodociągowych i c.o. nad salą oraz otoczenie niezwykłą opieką pomieszczeń przyległych z punktu widzenia ochrony przeciwpożarowej. Praktyka wykazała bowiem, że niezwykle rzadko pożar rozpoczyna się na sali ze sprzętem, natomiast wiele ośrodków zostało zniszczonych w wyniku pożaru lub zadymienia, powstałych w innych pomieszczeniach budynku. W ogóle temat ochrony fizycznej środowiska wymaga specjalistycznej wiedzy i doświadczenia, dlatego też ośrodki powinny korzystać z pomocy ekspertów w tych dziedzinach.

Zwięszeniu ochrony danych sprzyja, w każdym ośrodku, stałe aktualizowanie zakresów czynności pracowników oraz wzrost odpowiedzialności za kolejne fazy przetwarzania danych. Połączenie problematyki ochrony danych z organizacją jest w pełni zrozumiałe.

Niedopuszczalne są praktyki przyjmowania przez operatorów ustnych wskazówek /nie zamieszczonych w dokumentacji eksploatacyjnej/ od operatorów systemu lub programistów. Za pulpitem komputera ma prawo zasiadać wyłącznie operator, prócz niektórych ściśle określonych wypadków - konserwacja EMC, ładowanie systemu operacyjnego itp.

Wydruki z konsoli komputera oraz zbiory dziennika /log/ są ważnym elementem kontroli, który w miarę przechodzenia na bardziej nowoczesne metody przetwarzania stanowić będzie jeden z zasadniczych materiałów wchodzących w zakres ochrony danych.

W Głównym Urzędzie Statystycznym istotne znaczenie ma właściwie zorganizowane przekazywanie zbiorów na taśmach magnetycznych, głównie między ośrodkami elektronicznymi Urzędu /plombowane pojemniki metalowe itp./.

W celu dokładnego określenia odpowiedzialności pracowników za dane ustala się zasady rejestracji i kontroli międzyoperacyjnej we wszystkich fazach przetwarzania danych w ramach ośrodka, ze szczególnym uwzględnieniem rejestracji ruchu taśm magnetycznych.

Wszelka makulatura, stwarza poważne zagrożenie niepożądanego ujawnienia danych. Brak technicznych urządzeń do cięcia i belowania papieru nie może usprawiedliwić braku niezbędnej ochrony tej niebezpiecznej i łatwopalnej substancji. Praktyka uczy, że rozdzielanie makulatury /szczególnie wydruków komputerowych/ na możliwą do rozszyfrowania i na całkowicie nieczytelną jest trudne i nie daje gwarancji. W zależności od lokalnych warunków makulaturę należy zabezpieczać w pomieszczeniach chronionych, a następnie komisyjnie ją transportować i zniszczyć - najlepiej chemicznie w papierni.

Obok wdrażania zasad fizycznej i organizacyjnej ochrony danych, w nowoczesnych konfiguracjach komputerowych stale rosnącą rolę spełniać będą zabezpieczenia logiczne i systemowe, ujmowane w systemach użytkowych oraz wykorzystujące ochronne cechy systemów operacyjnych.

Z uwagi na podjęte inicjatywy wojewódzkich banków danych oraz stałą rozbudowę systemów teleprzetwarzania należy zwrócić szczególną uwagę na zabezpieczenie systemów wielodostępnych, umożliwiających dostęp do zbiorów z końcówek zainstalowanych poza salami komputerowymi.

W przepisach podano minimum zabezpieczeń logiczno-systemowych, podkreślając, że w zależności od potrzeb oraz wiedzy i doświadczenia kadry każdy ośrodek powinien doskonalić metody ochrony danych, ich planowego wdrażania i kontroli.

Odcinek ten znajduje się pod merytoryczną kontrolą Zakładu Projektowania i Oprogramowania Ośrodka Elektronicznego GUS w Warszawie, który to Zakład /zgodnie z obowiązującymi kompetencjami/ koordynuje i konsultuje całokształt działalności projektowej i programistycznej ośrodków elektronicznych GUS.

Wyjątkową rolę w systemie ochrony danych odgrywa system operacyjny komputera, jego właściwy wybór i sposób wygenerowania. Specjaliści doskonale zdają sobie sprawę jak delikatną materią jest każdy system operacyjny i jakie potencjalnie ryzyko zawiera.

Z punktu widzenia omawianego tematu powinno się wyciągnąć wniosek, że inżynier-konserwator i programista systemowy muszą być sojusznikami ludzi odpowiedzialnych za ochronę i jej stałe doskonalenie, szczególnie w warunkach zdalnego przetwarzania w trybie interaktywnym. Kompetencja i wysoki poziom moralny tych specjalistów ma decydujący wpływ na "panowanie" nad systemem komputerowym z punktu widzenia ochrony danych.

Celem wydanych przepisów jest nie tylko ochrona mienia państwowego, do którego należy zawarta w danych statystycznych informacja, ale również

ochrona uczciwych i rzetelnych pracowników przed zarzutami niedopełnienia w pewnych sytuacjach obowiązków służbowych.

Kluczem do stworzenia właściwej ochrony jest stosunek ludzi do tej sprawy. W związku z tym w realizacji wytycznych - co podkreślono na specjalnym sypozjum szkoleniowym GUS w kwietniu 1978 r. poświęconym problematyce ochrony danych - konieczny jest akcent na motywacje personelu, dobre stosunki międzyludzkie w ośrodkach. Tu właśnie kryją się możliwości nieobliczalnych strat i ryzyka, a z drugiej strony pozytywnych inicjatyw.

Cierpliwym i konsekwentnym działaniem trzeba w załogach wyrobić stanowczość w ścisłym przestrzeganiu zasad dostępu do pomieszczeń chronionych i wykonywania procedur ochronnych zgodnie z obowiązującą technologią. A nie jest łatwe wyplenienie takich aktów niefrasobliwości jak "wypożyczanie" haseł, podpieranie przysłowiowym papierkiem samozatrzaskujących się drzwi do sali komputerowej, zabieranie do domu wydruków dla sprawdzenia "w wolnej chwili","obrażanie się" za brak dostępu do konsoli operatora itp.

We wdrażaniu systemu ochrony danych zasadnicze znaczenie ma przemyślane "forsowanie barier" subiektywnych. Dlatego niezwykle ważne jest,aby pracownicy nigdy nie zauważyli cienia wątpliwości na twarzy swego przełożonego co do celowości określonego reżimu ochrony, a już na pewno nigdy nie spotkali się z "ruchami pozornymi" /często w opakowaniu działań biurokratycznych/. Posunięcia w dziedzinie ochrony trzeba dokładnie przemyśleć i sformułować, następnie konsekwentnie wdrażać i wymagać.

Metod ochrony systemów komputerowych i danych nie można nigdy sprowadzić wyłącznie do przepisów i instrukcji, chociaż wiele odcinków musi być nimi uregulowane. Starania o najlepszą w danych warunkach ochronę muszą stanowić troskę całego personelu, który powinien dostosowywać swe czynności do zmiennych zadań i potrzeb, do stale rozwijającego się postępu technicznego.

Na wspomnianym sypozjum przedstawiono również ogólny program akcji szkoleniowych, jakie będą przeprowadzone w GUS-sie w latach 1978 i 1979. Przewiduje się zorganizowanie cyklu szkolenia różnych grup specjalistów, rozpoczynając od kadry kierowniczej i wytypowanych przez ośrodki elektroniczne GUS specjalistów pełniących przy dyrektorach ośrodków funkcje koordynacyjno-doradcze w dziedzinie ochrony danych. Przygotowano między innymi opracowane tłumaczenia niektórych materiałów oraz wprowadzający podręcznik o charakterze pomocniczego materiału szkoleniowego.

W latach 1978 i 1979 przewiduje się skierowanie wybranych pracowników na specjalistyczne kursy zagraniczne z dziedziny ochrony danych.

Jako zadanie o charakterze bardziej długofalowym przyjmuje się zasadę nie dublowania istniejącego systemu doskonalenia kadr, a nasycenia istniejących programów szkolenia problematyką nowoczesnych metod ochrony danych.

Bardzo istotnym dla aparatu statystycznego zjawiskiem jest ochrona danych osobistych zebranych w trakcie badań statystycznych. Ustawa 1/ z dnia 15 lutego 1962 r. o organizacji statystyki państwowej nakłada na GUS jednoznaczne obowiązki postanawiając, że informacje i zeznania indywidualne, uzyskane w wyniku spisów powszechnych i badań statystycznych mogą być wykorzystywane tylko do zestawień statystycznych w przeciwnym wypadku będą stosowane kary. Sformułowane i przedstawione zasady określa się w gronie statystyków krótkim terminem "tajemnica statystyczna". Dla osób nie wprowadzonych w sprawy GUS wydawać się może, że tajemnica statystyczna jest sprawą raczej abstrakcyjną. Pracownicy aparatu statystycznego spotykają się jednak z tym zagadnieniem na codzień.

W grudniu br. w całym kraju będzie przeprowadzony Narodowy Spis Powszechny. Do każdego mieszkania przyjdzie rachmistrz spisowy i zarejestruje wiele danych, które nie zawsze udzielane są chętnie sąsiadom, znajomym, a nawet władzom administracyjnym. Przekazanie informacji żonie o roku urodzenia sąsiadki, szefowi przedsiębiorstwa o wykonywaniu dodatkowej pracy przez jego pracownika, wydziałowi finansowemu o prowadzeniu warsztatu bez posiadania pozwolenia jest naruszeniem tajemnicy statystycznej i rachmistrz spisowy lub stały pracownik resortu GUS może i powinien być za to karany. Innym bardziej obrazowym przykładem może być konieczność zachowania tajemnicy statystycznej w badaniach budżetów rodzinnych. Wylosowana do tych badań rodzina prowadzi bardzo szczegółową rejestrację wydatków i dochodów. Instruktor może niekiedy zaobserwować systematyczną nadwyżkę wydatków nad oficjalnymi dochodami, lecz spostrzeżenie to będzie zawsze chronione tajemnicą statystyczną.

Przykładów konieczności chronienia danych osobistych można przytoczyć bardzo dużo, gdyż na ogół pracownicy nowi mają wyrobione poczucie odpowiedzialności za chronienie tajemnicy służbowej lub państwowej, natomiast zachowanie tajemnicy statystycznej musi im dopiero wejść w nawyk.

W warunkach przetwarzania masowej informacji statystycznej problem ochrony tajemnicy statystycznej jest rozwiązany głównie środkami organizacyjnymi.

1/ Dziennik Ustaw 1962, nr 10, poz.47.

Ankiety z umieszczonymi personaliami przechodzą przez następujące etapy opracowania:

- kompletowanie,
- nanoszenie symboli,
- przenoszenie danych na maszynowy nośnik.

Poza tym część ankiet wykorzystywana jest do weryfikacji danych, określonych przez programy informatycznej kontroli jako błędne.

Wszystkie te operacje wykonywane są w skali masowej i istnieje małe prawdopodobieństwo, że pracownik natrafi na ankietę osoby znajomej, tym bardziej, że wykonuje on czynności zrutynizowane, wśród których nie ma potrzeby /i czasu/ na czytanie nazwisk i adresów.

Informacja przeniesiona na maszynowy nośnik jest już wyłącznie zbiorem cech i ulega całkowitej depersonifikacji. Powstaje więc pytanie, jaki jest cel umieszczenia na ankietach nazwisk i adresów badanych osób, gdy te cechy nie są wykorzystywane w trakcie opracowania. Długoletnia praktyka dowiodła, że należy, szczególnie w początkowych etapach opracownia, umożliwić powrót do badanej osoby dla weryfikacji danych błędnie zarejestrowanych. W niektórych badaniach stosuje się losową weryfikację, jak ma to miejsce np. w spisach rolnych.

Są również przypadki, że zbiory ankiet służą jako aparat losowania prób dla innych badań statystycznych i wtedy istnieje możliwość ponownego trafienia do badanej osoby, nawet po upływie kilku lat.

W ośrodkach obliczeniowych ochrona tajemnicy statystycznej sprowadza się więc do ograniczenia dostępu do zbiorów ankiet oraz do uświadomienia pracowników mających styczność z ankietami o obowiązku zachowania dla siebie informacji o osobach znajomych, jeśli nastąpi taki rzadki przypadek, że nazwiska zostaną zauważone w plikach pośpiesznie opracowywanych dokumentów.

Andrzej DERLATKA

PRAWNE ASPEKTY FUNKCJONOWANIA SYSTEMÓW INFORMATYCZNYCH

W publikacjach coraz częściej prowadzone są rozważania dotyczące statusu organizacyjno-prawnego systemów informatycznych. /5,s.32 i 6,s.14/. Zaznacza się przy tym wpływ informatyki na obowiązujący zespół norm prawnych w naszym ustawodawstwie. Warunkiem prawidłowej oceny tych problemów jest rzeczowa i w miarę pełna identyfikacja nowych zjawisk społecznych będących rezultatem stosowania informatyki oraz właściwa ocena skutków, zwłaszcza tych negatywnych. Jesteśmy zatem świadkami powstawania "prawa informatycznego", wzorem "prawa handlowego", "prawa morskiego" itd. Omawiana problematyka jest bardzo rozległa. Przede wszystkim konieczne jest ustalenie precyzyjnego i spójnego zbioru pojęć. Innym zagadnieniem bardzo ważnym jest zastosowanie konkretnej doktryny prawnej. Może się okazać, że wiele obecnie obowiązujących norm prawnych znajdzie swoje zastosowanie przy rozstrzyganiu nowych kwestii, chociaż na pewno potrzebna będzie pewna nowelizacja.

Wśród tematów wspólnych dla informatyki i prawa szczególną uwagę należy zwrócić na:

1/ ustrojowo-prawne uwarunkowania systemów informatycznych,
2/ administracyjno-prawne problemy systemów informatycznych,
3/ status prawny informacji,
4/ ochronę systemów informatycznych za pomocą norm prawnych,
5/ ochronę własności intelektualnych w systemach informatycznych /1,s.17/.

1. Ustrojowo-prawne problemy systemów informatycznych

Jeśli przyjąć, że system informatyczny jest to zbiór elementów w postaci oprogramowania, środków przetwarzania, procedur organizacyjnych oraz ludzi, a elementy te pozostają ze sobą w dynamicznie zmieniających się zależnościach, to można uznać, że każdy system informatyczny, stworzony przez podmiot administracji państwowej i od niego zależny, przybiera formę zakładu państwowego. Zgodnie z najnowszą teorią polskiego prawa administracyjnego należy go uważać za "podmiot administracji państwowej" /1,s.18/.

Zgodnie z nauką prawa administracyjnego można wskazać podstawowe tematy ustrojowo-prawne systemów informatycznych:

- charakterystyka prawna systemu informatycznego,
- zasady i podstawy prawne tworzenia systemów informatycznych,
- określenie relacji systemu informatycznego z otoczeniem zewnętrznym,
- prawne regulacje organizacji procesów informatycznych,
- odpowiedzialność dyscyplinarna,
- prawne zasady dokumentowania działalności systemów informatycznych,
- prawne określenie odnowy systemów informatycznych,
- określenie zasad kontroli systemu informatycznego,
- prawne regulacje stosunków między systemami informatycznymi a innymi jednostkami państwowymi,
- przydział kompetencji w stanowieniu aktów normatywnych dla systemów informatycznych /7/.

2. Administracyjno-prawne problemy systemów informatycznych

Stosunki administracyjno-prawne systemów informatycznych, mają miejsce między organami administracji państwowej a innymi podmiotami lub osobami fizycznymi. Jest to zagadnienie bardzo ważne ponieważ w warunkach funkcjonowania systemów informatycznych dochodzi często do konfrontacji interesów prawnych władz administracji z osobami prawnymi lub fizycznymi. W związku z tym istnieje potrzeba sprecyzowania aktów zarówno ogólnych, jak i szczegółowych, które będą regulowały te stosunki.

Nie jest także rzeczą obojętną czy zasady te będą odpowiadać istniejącemu prawu kodeksu postępowania administracyjnego, czy też będą ich uzupełnieniem. Podstawowe problemy występujące na tym etapie rozwoju informatyki to:

- kompetencje organów państwowych w kwestii zbierania, przetwarzania i wykorzystania danych osobowych w systemach informatycznych,
- ustalenie i regulacja interesów prawnych obywateli pozostających w związku z działaniem systemów informatycznych /ochrona sfery życia osobistego obywateli/ /1,s.20/.

Wymienione zagadnienia dotyczą jednak tylko ochrony danych. Całokształt problematyki administracyjno-prawnej obejmuje również takie sprawy, jak nadzór i kontrolę nad respektowaniem przepisów prawnych lub zasady prowadzenia działalności finansowo-rachunkowej.

3. Status prawny informacji

Studia nad polskim systemem prawnym dowodzą, że brak jest w nim określenia pojęcia dokumentu lub innego środka, nośnika informacji.

Producenci urządzeń informatycznych i projektanci systemów dążą do maksymalnego skracania obiegu technologicznego nośników informacji, a co za tym idzie samej informacji. Nie trzeba specjalnie dowodzić, jak usprawnia i przyspiesza to pracę systemu informatycznego. Jest to o tyle zrozumiałe i uzasadnione, że przygotowanie maszynowego nośnika danych /np. karty dziurkowanej/, a następnie dostarczenie go do maszyny cyfrowej, zajmuje blisko 80 % czasu potrzebnego na wykonanie konkretnego zadania. Pomimo, że w polskim systemie prawa brak jest określenia dokumentu, to w praktyce uznawane są i mają moc urzędową tabulogramy komputerowe. Istotą dokumentu jest jego zawartość informacyjna, która może być narażona na nieodpowiednie gromadzenie przetwarzanie lub wykorzystanie. Powstaje więc konieczność szybkiego ustalenia, czy należy uznać informację za kategorię prawną i czy powinna być ona chroniona w polskim systemie prawa ? Jeśli założymy, że odpowiedź na te pytania będzie twierdząca, to należy określić jednoznacznie wzajemne relacje między takimi pojęciami jak: informacja, dane, maszynowy nośnik danych, tabulogram.

W przypadku gdy ustawodawcy uda się sprostać tym wszystkim wymaganiom, to nadal pojawiać się będą pewne wątpliwości. Jak można orzec , czy dokument komputerowy jest zgodny z prawem, lub nie ? Bardziej realnym jest określenie technicznej poprawności lub błędności takiego dokumentu /1,s. 23 i dalej/.

W procesie przetwarzania danych istnieje pewien okres, w którym informacje znajdują się w pamięci maszyny w wersji kodu maszynowego. Status prawny informacji powinien także uwzględnić i to zjawisko, jako zagwarantowanie wiary publicznej. Może to mieć znaczenie dla prowadzenia ksiąg notarialnych, wieczystych itp.

4. Ochrona systemów informatycznych przy pomocy norm prawnych

Wśród metod zabezpieczenia systemów informatycznych wymienia się także ochronę za pomocą norm prawnych. Oczywiście stosowanie tylko takiego zabezpieczenia, nawet przy najbardziej precyzyjnie skonstruowanych normach prawnych, nie zapewni wymaganego poziomu bezpieczeństwa. Norma prawna ma spełnić rolę dodatkową, ponad materialną. Jej zadaniem jest stworze

nie takiego środowiska dla działania systemu informatycznego, w którym każde działanie niezgodne z normą pociąga za sobą konsekwencje karno-administracyjne.

Prace legislacyjne dotyczące ustawowego uregulowania działania systemów informatycznych należy skierować na:

- określenie uprawnień dla systemu informatycznego do gromadzenia, przetwarzania, przechowywania i wykorzystywania danych,
- zagwarantowanie obywatelom i instytucjom materialnych oraz prawnych interesów łącznie z ewentualnoscią prawa wglądu do danych znajdujących się w działającym systemie,
- zobowiązanie określonych organów i instytucji do wprowadzania i aktualizowania danych,
- ustalenie zasad korzystania z informacji przechowywanych w systemie,
- ustalenie zasad związanych ze statusem prawnym informacji /2,s.122/.

Tak przedstawione zadania pozwalają określić w przybliżeniu, jak powinny być sformułowane przepisy egzekwujące karno-administracyjną odpowiedzialność podmiotów za niedopełnienie obowiązków wynikających z ustawy /2,s.122/.

W dyskusjach nad pracami legislacyjnymi wiele uwagi poświęca się również problematyce rozgraniczania odpowiedzialności dyscyplinarnej, karno-administracyjnej i karnej. W praktyce formułowania doktryn polityczno-prawnych spotkać można różne kryteria. Do najczęściej wymienianych i najbardziej popularnych zaliczyć można:

- kryterium stopnia społecznego niebezpieczeństwa czynu,
- kryterium organów realizujących odpowiedzialność karną i dyscyplinarną,
- kryterium wielkości szkodliwych następstw naruszenia.

Obecnie przedmiotem rozważań prawników i informatyków stały się możliwości przystosowania zasad odpowiedzialności karno-administracyjnej do grupy elementów będących zabezpieczeniem sprawnego funkcjonowania systemów informatycznych. Mamy na myśli dwie grupy podmiotów, które mogą stanąć wobec odpowiedzialności karno-administracyjnej. Pierwsza grupa to osoby będące reprezentantami organów państwowych lub osób prywatnych. Odpowiedzialność ich dotyczyć może nieprawidłowego dostarczania danych do komputera lub jakiegokolwiek utrudniania i uniemożliwiania ich wprowadzania.

Każdy system informatyczny, realizując określone funkcje, powinien dostarczać jego decydentowi informacje dokładne, systematyczne i czytelne.

Dbałość o te cechy informacji należy do wielu podmiotów państwowych, zależnie od wielkości i zasięgu działania systemu. Poczyniono już pierwsze kroki w naszym ustawodawstwie, na których można się wzorować. Związane jest to szczególnie z ustawą o organizacji statystyki państwowej z dnia 15 lutego 1962 r. art. 19, 20, 21, 22 oraz Kodeks Wykroczeń z 1971 r. art. 65, 66, 146, 147.

Przepisy te dokładnie określają rodzaj czynu i sankcję wynikającą z jego niedopełnienia. Ustawy te nie rozwiązują jednak wszystkich problemów. Jako postulaty de lege ferenda proponuje się konieczność zagrożenia karami następujące rodzaje działań:

- niedopełnienie przekazywania danych,
- świadome składanie danych niezgodnych z prawdą,
- niedopełnienie terminowego obowiązku aktualizacji zbiorów danych,
- utrudnianie lub uniemożliwianie osobom upoważnionym wprowadzanie i aktualizowanie danych w systemie informatycznym,
- udzielanie osobom nieupoważnionym informacji zawartych w systemie,
- odmowę pracownika systemu informatycznego spełnienia słusznych żądań zainteresowanego obywatela jednostki gospodarki uspołecznionej lub urzędu /2,s.128/.

Druga grupa osób mogących ponosić odpowiedzialność karno-administracyjną to pracownicy systemu informatycznego, którzy nie zachowali tajemnicy danych lub nie przestrzegali uprawnień użytkowników. W odniesieniu do wszystkich pracowników systemu mogą mieć zastosowanie przepisy kodeksu karnego dotyczące ochrony tajemnicy państwowej lub służbowej. Zastosowanie przepisów prawno-karnych chroniących tajemnicę państwową lub służbową może mieć miejsce tylko wtedy, gdy dane i ich zbiory objęte zostaną tajemnicą. Fakt ten wymaga jednak odpowiednich aktów prawnych.

Kodeks karny z roku 1969 stwierdza wyraźnie, że przestępstwo w postaci naruszenia tajemnicy państwowej można popełnić z winy umyślnej i nieumyślnej /art. 260 § 1 i § 2 § 3 kk/. Natomiast czyn, który jest naruszeniem zarządzeń o ochronie tajemnicy państwowej /tj. gdy nastąpi naruszenie zarządzenia powodując w efekcie niebezpieczeństwo ujawnienia tajemnicy państwowej/ może być popełniony tylko z winy umyślnej. Stąd wniosek, że nieumyślne naruszenie tajemnicy służbowej oraz zarządzeń wydanych w celu jej ochrony pozostaje poza zasięgiem prawa karnego.

Ze względu na przedmiot ochrony, jakim są uprawnienia osób mających dostęp do danych osobopoznawczych, rozważenia wymaga następujący problem:

Czy nie byłoby słuszne wyłączenie z przewinień służbowych czynów nieumyślnie naruszających zarządzenia dotyczące ochrony tajemnicy związanej z systemem informatycznym, a odpowiedzialność za ich popełnienie określić w kodeksie wykroczeń ? W tym przypadku, należy doprowadzić do wydania aktu prawnego, który jednoznacznie określałby zakres uprawnień użytkownika systemu.

Osobna grupa to problematyka tzw. przestępczości komputerowej. Abstrahując od poprawności sformułowania /przestępstwa nie dokonuje przecież komputer/ koniecznym jest rozpoczęcie szczegółowych badań prawnych i empirycznych nad występowaniem i charakterem tych przestępstw. Badania te musi cechować wszechstronność, w związku z tym powinni w nich brać udział specjaliści nie tylko z dziedziny prawa i informatyki, ale także przedstawiciele socjologii, psychologii, teorii organizacji i zarządzania /3/.

5. Ochrona własności intelektualnych w systemach informatycznych

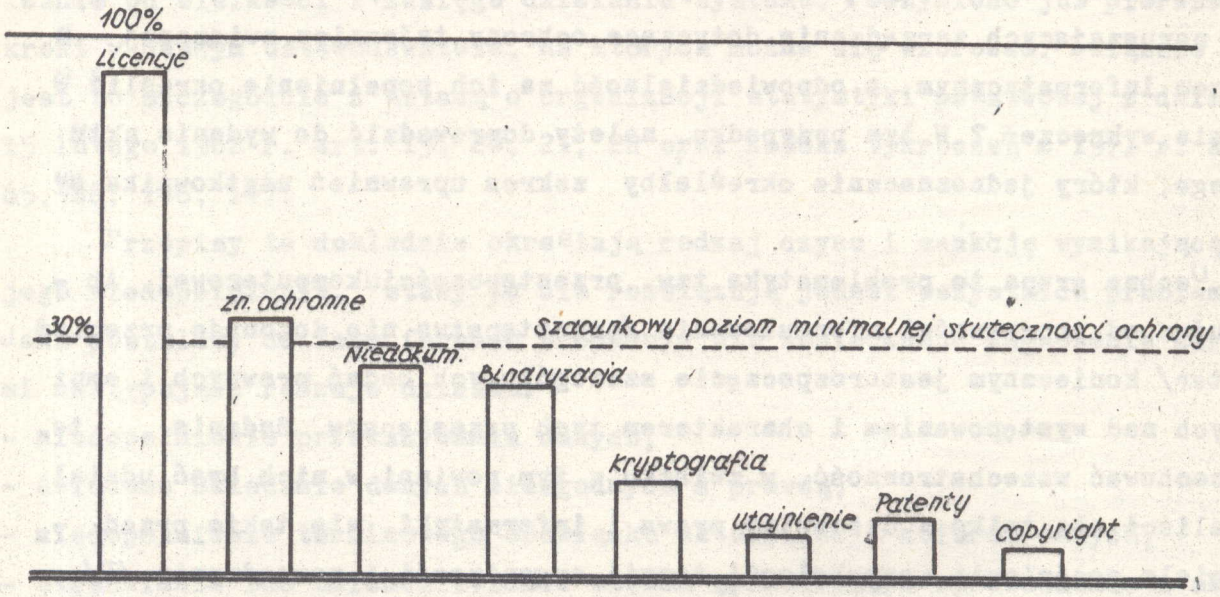
Zapewnienie ochrony praw autorskich i wynalazczych ma niewątpliwie duże znaczenie społeczne. Od ich sprawności i elastyczności zależą interesy twórców oraz odbiorców tej twórczości. Systemy gromadzenia i wyszukiwania publikacji zmuszają do wkroczenia nauki prawa w dziedzinę informatyki, choćby w celu ochrony prawa wydawniczego i autorskiego. Podobny problem, któremu obecnie poświęca się dużo uwagi, to ochrona interesów twórców oprogramowania.

Wyniki ankiet 46 brytyjskich ośrodków obliczeniowych, dotyczących ochrony prawnej oprogramowania, zaskoczyły swoimi wynikami wszystkich zainteresowanych /10,s.34/. Najwyższy wskaźnik skuteczności ochrony do kosztu zapewnia dostarczanie odbiorcy niedokumentowanego oprogramowania. Natomiast utajnienie programów znajduje się w grupie środków o najniższej skuteczności ochrony.

Respondenci w swoich wypowiedziach sugerowali stworzenie takiego aparatu, który zapewni ochronę:

- tanią,
- o małym stopniu zbiurokratyzowania,
- szybką w skutkach,
- uwzględniającą pośredników,
- mającą zasięg międzynarodowy,
- potencjalnie efektywną,
- możliwą praktycznie do wyegzekwowania.

Rys. 1 Skuteczność różnych form ochrony prawnej do kosztu



W historii rozwoju informatyki w USA można zaobserwować starania o ochronę dokonywanych inowacji w ramach istniejącego statusu prawnego /4, s.19/. Zostało to potwierdzone przez orzecznictwo sądowe. W warunkach amerykańskich, w przypadku programów komputerowych, najodpowiedniejszą formą ochrony autorstwa okazała się kombinacja prawa publicznego /Common law copyright/ i ochrona tajemnicy handlowej i przemysłowej /Trade secrets/.

Ochrona programów komputerowych nie jest możliwa na tle przepisów polskiego prawa autorskiego. Są one dostosowane do ochrony wartości intelektualnych ze względu na ich walory estetyczne lub poznawcze i ukierunkowane głównie na ochronę oryginalnego sposobu demonstrowania dzieła /8,s.5/ Podstawową funkcją programów do maszyn cyfrowych jest ich użyteczność. Tym co powinno być zasadniczym elementem ich ochrony jest niekonwencjonalność i oryginalność rozwiązania.

Proponuje się objęcie programów ochroną prawno-autorską de lege ferenda /8,s.6/. Wspomniano poprzednio o międzynarodowym charakterze takiej ochrony. Słuszność tego potwierdza fakt, że organizacje międzynarodowe działające w dziedzinie praw na dobrach intelektualnych, w kręgu swoich zainteresowań umieściły ochronę prawną oprogramowania. Organizacją taką jest dla przykładu AIPPI /Stowarzyszenie Ochrony Własności Przemysłowej/. Dorobek AIPPI wykorzystała inna organizacja pod nazwą WIPO /Światowa Organizacja Własności Intelektualnej/. Grupa ekspertów tej organizacji zaleciła opracowanie wersji ustawy wzorcowej. Projekt wzorcowych przepisów dla krajowych ustaw o ochronie oprogramowania dla maszyn cyfrowych, składa

się z ośmiu artykułów opatrzonych uzasadnieniami i komentarzami wyjaśniającymi treść zawartych w nich postanowień.

Przedmiotem dyskusji w wielu krajach jest przede wszystkim ochrona patentowa i ochrona praw autorskich, a spośród innych środków ochrony prawnej - przepisy o nieuczciwej konkurencji. Jednakże w poszczególnych grupach krajów różnie akcentuje się te instytucje prawa. W krajach anglosaskich, a szczególnie w Stanach Zjednoczonych, niemal cała dyskusja o ochronie prawnej oprogramowania sprowadza się do problemu opatentowania /9,s.32/.

W krajach niemieckiego obszaru językowego przedyskutowano wiele problemów ochrony z tytułu prawa autorskiego i coraz więcej uwagi poświęca się przepisom o nieuczciwej konkurencji. We Francji w roku 1968 wydana została ustawa, która zapewnia ochronę oprogramowania w drodze umowy.

Analiza porównawcza problematyki ochrony prawnej oprogramowania w różnych krajach pozwala na określenie zasadniczych i niezbędnych elementów, które powinny uwzględnić przepisy prawne:

- czas obowiązywania ochrony prawnej,
- rejestracja programów powiązana z obowiązkiem publikacji,
- uwzględnienie różnych interesów stron zainteresowanych ochroną,
- prosta i szybka procedura administracyjna,

Ponadto ochrona prawna oprogramowania powinna uwzględnić potrzeby swobodnego rozwoju nauki, jak również ustanowić nie podlegający ochronie zakres bardzo prostych programów, nie mających większej wartości intelektualnej.

Zakończenie

Każda nowa sytuacja społeczna wymaga prawnego uregulowania. W pełni dotyczy to także zastosowań informatyki w administracji i gospodarce narodowej. Brak przepisów prawnych lub ich niekompletność w tym względzie, daje podstawę do wydania nowych aktów prawnych lub nowelizacji istniejących.

Przepisy dotyczące informatyki są w Polsce bardzo rozproszone. Można je znaleźć w prawie administracyjnym, finansowym, cywilnym i innych. Nie sprzyja to ich uporządkowaniu i systematyczności.

Z zaprezentowanej treści wynika potrzeba stworzenia nowej, odrębnej "informatycznej gałęzi prawa". Koncepcje wyodrębnienia takiej gałęzi prawa mają zresztą w kraju wielu zwolenników /9/.

Doceniając pozytywy takiego projektu trzeba jednak zdawać sobie sprawę z ewentualnych trudności, które mogą wystąpić w trakcie jego realizacji. Przykładem tego może być choćby stworzenie aparatu pojęciowego, w pełni spójnego wewnętrznie. Jednak cele nadrzędne, tzn. coraz lepsze możliwości techniczne informatyki, które pozwolą wydatniej zaspakajać społeczne potrzeby, są dostateczną argumentacją na rzecz konieczności uregulowania jej prawnego statusu.

Bibliografia

1. ACHTELIK E., WOŁOCH J., Prawne problemy systemów informatycznych, a prawo informatyczne. Materiały z konferencji informatyki prawniczej, Wrocław 1976, t.1
2. BOGUNIA E., Ochrona karno-administracyjna systemów informatycznych administracji państwowej. Materiały z konferencji informatyki prawniczej, Wrocław 1976 t.1
3. BOSSOWSKI A., Nadużycia komputerowe i szpiegostwo technologiczne. Studia Kryminologiczne 1975, t.3
4. DEMBIŃSKI A., Ochrona prawna oprogwamowania w USA, "Informatyka" 1972 nr 12
5. BRONIATOWSKI, Prawne problemy zautomatyzowania systemu zarządzania. "Organizacja, Metody, Technika" 1972 nr 12
6. KOTOWSKI M., Komputer i prawa jednostki, "Polityka" 1974 nr 12
7. OCHENDOWSKI, Zakład administracyjny jako podmiot administracji państwowej, Poznań 1969
8. WALUSZEWSKI J., Zagadnienia ochrony prawnej programów dla maszyn cyfrowych na forum międzynarodowym, "Informatyka" 1977 nr 11
9. Obecna sytuacja w zakresie ochrony prawnej oprogramowania w różnych krajach, "Informatyka" 1977 nr 5
10. Ochrona prawna oprogramowania, "Informatyka" 1976 nr 10

TNOiK 170/78
n. 180+90 A-4