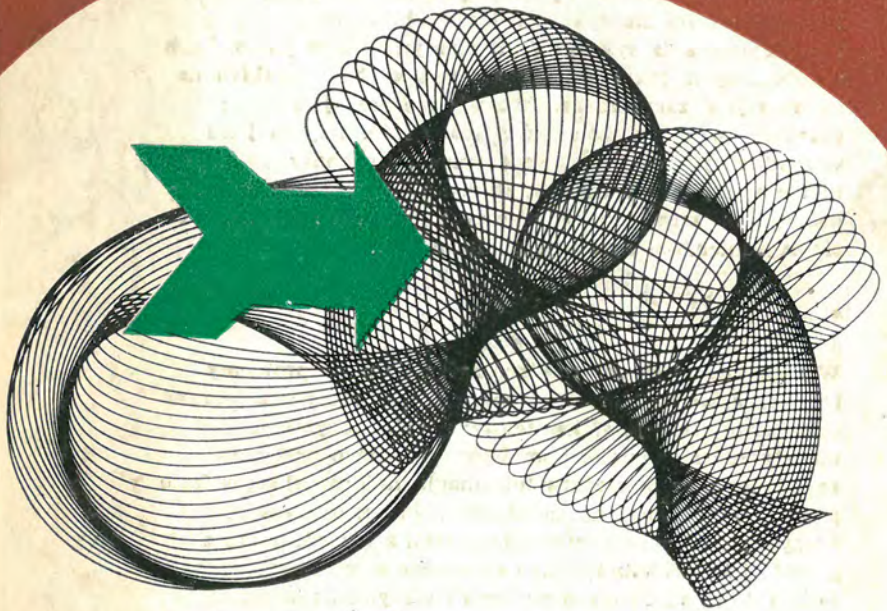
INFORMATYKA W PRAKTYCE



Andrzej Z.Idźkiewicz

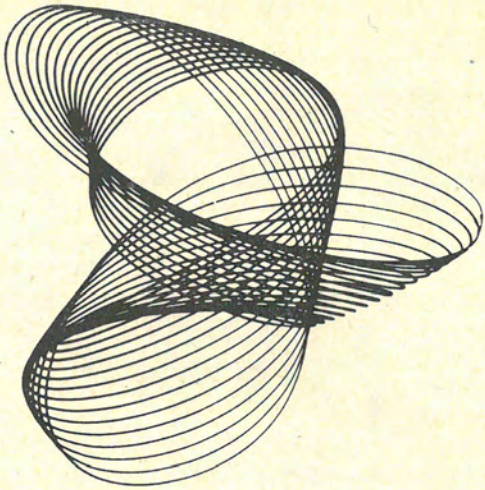
Ochrona informacji w procesie przetwarzania

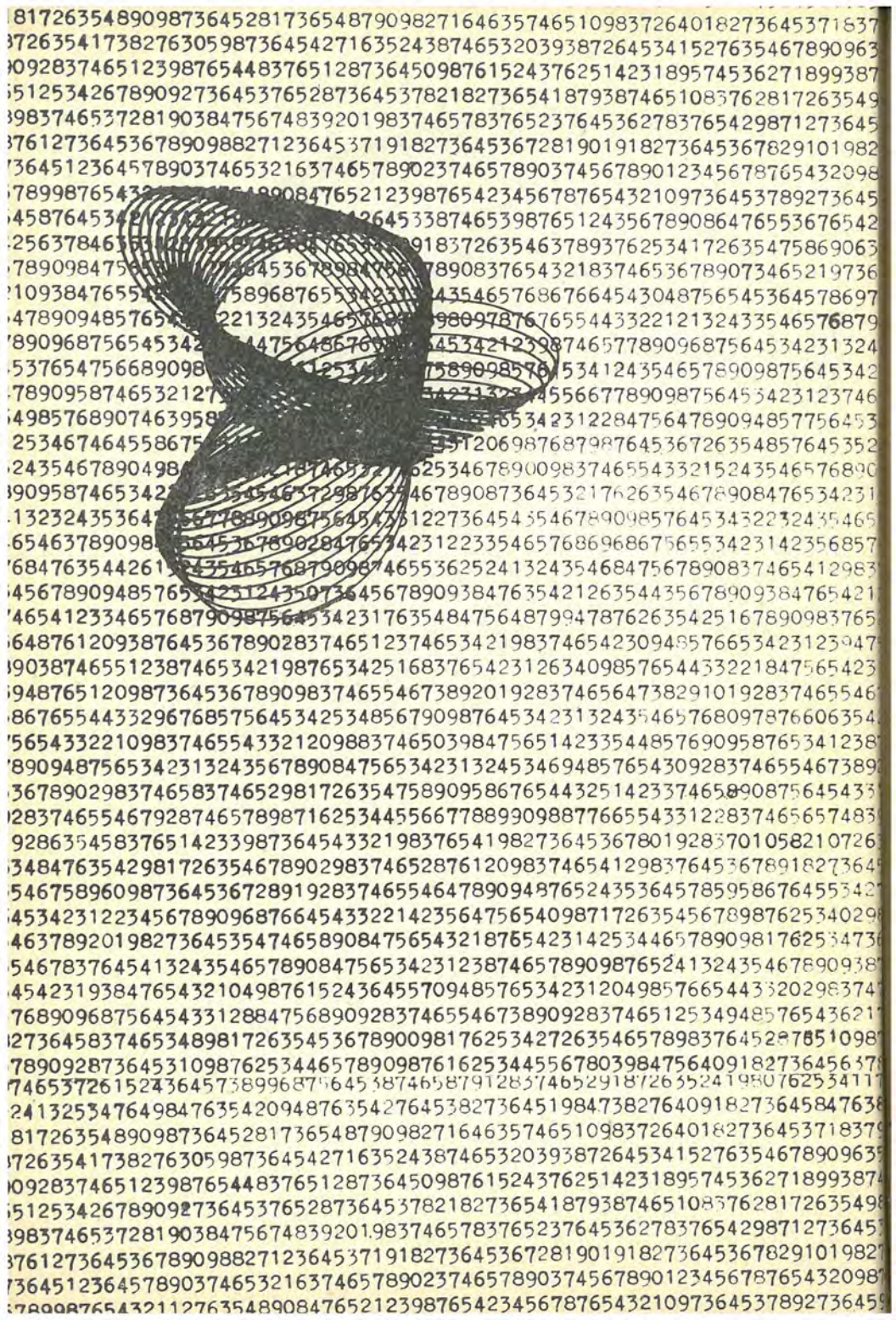
PWE

Seria wydawnicza „Informatyka w praktyce" zaspokaja potrzeby poznania literatury fachowej, poświęconej popularyzowaniu oraz wykorzystywaniu rozwiązań i zastosowań informatyki, a zwłaszcza budowania i funkcjonowania systemów informatycznych w jednostkach gospodarczych, jak też doskonaleniu sposobów uzyskiwania informacji w zarządzaniu. Poszczególne pozycje serii są przeznaczone dla pracowników służby informatycznej we wszystkich jednostkach gospodarczych, dla kadry kierowniczej tych jednostek, studentów wyższych uczelni, uczestników kursów podyplomowych oraz osób interesujących się zagadnieniami i rozwojem informatyki.

*

W rozwijającej się informatyce rodzą się nowe problemy i zjawiska, wśród których poczesne miejsce zaczyna zajmować ochrona informacji. W książce tej znajdzie Czytelnik metodyczne rozwinięcie kompleksowo ujętego problemu zapewnienia bezpieczeństw informacji znajdującej się w fazie przetwarzania. Znalazły tu odbicie różnorodne kwestie, poczynając od przeglądu potencjalnych zagrożeń, poprzez metody i środki zabezpieczeń stosowane w poszczególnych fazach APD, aż do zasad nadzoru i utrzymania systemu ochrony. Rozważania są poparte praktycznymi wskazówkami oraz licznymi przykładami, zaczerpniętymi z literatury zagranicznej, a także opartymi na doświadczeniach krajowych.
Proponowana pozycja stanowi — jako pierwsza na polskim rynku wydawniczym poświęcona temu tematowi — pouczającą lekturę dla kadry kierowniczej, może być wykorzystywana zarówno jako materiał szkoleniowy, jak i pomoc w codziennej praktyce dla osób zajmujących się ochroną i nadzorem systemów APD oraz dla projektantów tych systemów.





INFORMATYKA
W PRAKTYCE

Ochrona informacji w procesie przetwarzania

Andrzej Z. Idźkiewicz

Państwowe Wydawnictwo Ekonomiczne
Warszawa 1979

Okładkę projektował
FRANCISZEK WINIARSKI

Redaktor książki
GRAŻYNA PIĘTAK

Korektor
TERESA RYBICKA

Spis treści

I. Wrażliwość i znaczenie informacji w organizmie społecznym

1. Wprowadzenie

Każde przedsiębiorstwo, organizacja, instytucja, a także każda osoba fizyczna dysponuje różnymi informacjami, które niezbędne jej są do normalnego funkcjonowania. Istnieje porównanie, które być może zbyt często jest już eksploatowane, nie oznacza to jednak, że traci ono na swojej celności: *informacja w każdym organizmie społecznym lub gospodarczym odgrywa taką samą rolę, jak krew w organizmie żywym, a obieg informacji można porównać do krwiobiegu.* Można rozszerzyć nieco to porównanie: podobnie jak organizm żywy umiera na skutek wykrwawienia lub zatrucia krwi, organizm gospodarczy lub społeczny może niedomagać lub zginąć, jeśli umożliwiająca mu funkcjonowanie informacja ulegnie zniszczeniu, przekłamaniu lub zostanie wykradziona, albo jeśli obieg tej informacji — ulegnie zakłóceniu.

J. L. Kulikowski pisze [10, s. 6]: *„Powoli dojrzewa sytuacja, w której kierując się szeroko i perspektywicznie rozumianymi potrzebami rozwoju społeczno-gospodarczego kraju wszelką informację: naukową, techniczną, polityczną, gospodarczą, prawno-administracyjną, organizacyjną itp., mającą jakąkolwiek wartość społeczną lub mogącą mieć w przyszłości znaczenie dla społeczeństwa i rozwoju jego gospodarki lub kultury, znajdującą się pod jakąkolwiek postacią w gestii urzędów, instytucji uspołecznionych albo jednostek gospodarczych, będziemy traktować jako wspólne ogólnonarodowe dobro podlegające ochronie prawnej oraz obligujące do jego racjonalnego zagospodarowania i wykorzystania. Nie ma istotnych powodów, aby z prawnego punktu widzenia traktować pod tym względem informację inaczej niż traktujemy dziś*

dobra naturalne kraju, jego przyrodę, zasoby wodne lub atmosferę". I dalej [10, s. 12—13]: „*Niezależnie od braku dostatecznie pełnych i jasnych przepisów prawa w tej dziedzinie istnieje też problem braku dostatecznej świadomości społecznej skutków, jakie może powodować niewłaściwe gospodarowanie informacją, a zwłaszcza brak troski o jej wiarygodność lub o jej zabezpieczenie; znany jest na przykład przypadek używania do pakowania towaru na straganie wydruków komputerowych zawierających stany kont posiadaczy rachunków bankowych, jak również przypadek tolerancyjnego potraktowania winnych upowszechnienia błędnej informacji o fizjologicznych skutkach oddziaływania leku, co spowodowało przedawkowanie leku przez lekarza i przedwczesny zgon pacjenta*".

Problem ochrony informacji nabiera coraz większej wagi w związku z rozwojem informatyki i z rosnącym komputeryzowaniem przetwarzania informacji. Rzecz polega na zmianach jakościowych i ilościowych, jakie następują w procesach gromadzenia danych, przetwarzania ich oraz dystrybucji informacji wynikowej. W tradycyjnych systemach:

1. Dane gromadzone były w sposób zdecentralizowany. Wynikało z tego, że żadne stanowisko pracy, żadna osoba nie posiadała pełnej informacji na temat określonego zagadnienia, co zmniejszało np. zagrożenie poufności informacji.

2. Przechowywanie danych było tylko w niewielkim stopniu sformalizowane. W związku z tym jedynie niewielka liczba osób bezpośrednio z określoną działalnością związanych umiała te dane wykorzystać. Dla innych były one nieprzejrzyste.

3. Jeśli chodzi o zabezpieczenie informacji, systemy te stwarzały niewątpliwie wiele okazji do wystąpienia błędów. Ponieważ jednak istniała świadomość tego, wprowadzono liczne stanowiska kontroli poprawności danych, zmniejszając w ten sposób prawdopodobieństwo, że błąd przemknie się niezauważenie i spowoduje w dalszym biegu przetwarzania narastające zniekształcenie informacji.

Wprowadzenie automatycznego przetwarzania danych (APD) spowodowało niespotykaną dotychczas centralizację zarówno informacji, jak i procesu jej przetwarzania. Pociąga to za sobą w konsekwencji uzależnienie całej działalności — w szczególności gospodarczej — od ośrodka APD. W ośrodku APD rejestrowane

(zapamiętywane) są wszystkie niezbędne do działalności danej organizacji informacje. Zarazem w tymże ośrodku koncentruje się cały system kontroli i sterowania działalnością: kontrola zapasów, planowanie produkcji i sporządzanie harmonogramów, księgowość itp.

Dodatkowo wzrasta wrażliwość systemów APD na wszelkiego rodzaju zagrożenia na skutek coraz szerszego wprowadzania systemów przetwarzania z końcówkami zdalnego dostępu (*terminalami*). Dane mogą tu być zdalnie pobierane lub modyfikowane, praktycznie bez możności zidentyfikowania, kto faktycznie dokonuje tych czynności. Z uwagi na to, że ani zarejestrowane zapisy, ani manipulowanie nimi nie może być bezpośrednio (przez np. przejrzenie) choćby pobieżnie skontrolowane, za ścisłość i prawdziwość tych zapisów odpowiadają w równej mierze ośrodek APD oraz korzystający z usług tego ośrodka użytkownik danych.

Przechowywanie danych jest realizowane w postaci ściśle formalnie zorganizowanych zbiorów, do których możliwy jest dostęp według niemal dowolnie dobranych kryteriów wyszukiwania, jeśli tylko zna się kilka prostych zasad postępowania. A zatem uzyskanie informacji nie wymaga na ogół znajomości przedmiotu tych informacji, lecz raczej ogólnie dostępnych reguł formalnych.

Jakkolwiek w naszych warunkach ustrojowych nie występuje wewnętrzna walka konkurencyjna — a zatem nie występują także, na przykład, ani usiłowania wykradania sekretów produkcyjnych, ani próby „przechwycenia" klientów jednej firmy przez drugą — trzeba jednak pamiętać, że wszędzie, gdzie ma miejsce działalność gospodarcza zachodzi również niebezpieczeństwo działalności przestępczej. Przestępstwa popełniane w środowisku elektronicznej techniki obliczeniowej należą do bardzo trudno wykrywalnych i mogą być szczególnie dotkliwe w skutkach. Zresztą, informację należy zabezpieczać nie tylko przed działalnością o charakterze przestępczym. Najczęściej istotnym problemem są błędy ludzkie i niedbalstwo, których skutki — jakkolwiek nie tak spektakularne jak skutki oszustw i malwersacji — mogą przedsiębiorstwo bardzo drogo kosztować, mimo że nie wynikają z niczyich „kryminalnych" skłonności.

Istnieją dwa zasadnicze aspekty ochrony informacji, z punktu widzenia groźby jej ujawnienia:

1. Ochrona informacji indywidualnej (ang. *privacy*); chodzi tu o prawo jednostki bądź instytucji do decydowania, komu wolno gromadzić informację dotyczącą danej osoby lub instytucji oraz komu i jaką informację z tego zakresu wolno udostępnić. Wiąże się to z zagadnieniami ochrony prawnej, etyki, swobód obywatelskich; tym aspektem ochrony informacji zajmować się tutaj nie będziemy.

2. Ochrona informacji i środowiska jej przetwarzania w ogóle (ang. *security*) — problem w zasadzie ekonomiczno-organizacyjno-techniczny. Stanowi ona jeden z warunków koniecznych, choć nie wystarczających do ochrony informacji indywidualnej, lecz zarazem wykracza poza zakres wąsko pojętej ochrony przed ujawnieniem.

Chwila zastanowienia pozwoli dojść do przekonania, że istnieje właściwie sześć „nieszczęść", które mogą przydarzyć się danym. Mogą one zostać p r z y p a d k o w o ujawnione, zmienione lub zniszczone. Mogą one również zostać u m y ś l n i e ujawnione, zmienione lub zniszczone. Tak więc zagadnienie ochrony informacji polega na uchronieniu danych przed przypadkowym lub umyślnym ujawnieniem, przekształceniem lub zniszczeniem. I tak szeroko pojęte zagadnienie ochrony informacji jest przedmiotem tej książeczki.

Robert H. Courtney, zajmujący się w największej firmie komputerowej świata („International Business Machines") sprawami ochrony informacji, sporządził listę wszystkich potencjalnych zagrożeń, na które mogą być narażone dane. Obejmuje ona 743 pozycje [4]. Jak twierdzi jej Autor, co najmniej 300 pozycji tej listy można zastosować do dowolnego konkretnego systemu. Jest rzeczą ciekawą, że na ogół najmniejszym prawdopodobieństwem wystąpienia odznaczają się zagrożenia o charakterze przestępczym. W tablicy I zostały przedstawione wyniki ankiety, przeprowadzonej w około 150 organizacjach gospodarczych przez brytyjską organizację „National Computing Centre". Powody mniej lub bardziej groźnych zakłóceń w pracy tych ośrodków obliczeniowych zostały uporządkowane w kolejności malejącej częstotliwości, z uwzględnieniem rozmiarów strat.

Jak widać, na czele listy znalazły się wydarzenia przypadkowe i błędy ludzkie. Badania IBM potwierdzają także, że ponad 50%

TABLICA I

Przyczyny zakłóceń pracy ośrodków APD

Przyczyna zakłócenia	Związane z zakłóceniem straty		
	Żadne	Niewielkie	Poważne
Sprzęt	15	121	16
Błędy operatora, błędy pisarskie	11	132	15
Oprogramowanie systemowe	24	123	12
Programy użytkowe	12	132	11
Transmisja danych	57	84	7
Zasilanie energią elektryczną, klimatyzacja	31	118	5
Pożar, szkody wodne	129	13	1
Złośliwe uszkodzenia	140	2	0
Kradzieże, oszustwa, nieuprawnione użycie	140	2	0

znanych przypadków naruszenia bezpieczeństwa informacji wiąże się z wydarzeniami przypadkowymi. Należy jednak pamiętać, że sprawcy przestępstw zacierają za sobą ślady, a wykrywalność przestępstw tzw. „komputerowych" jest mała (ocenia się ją na 25, a co najwyżej 30%).

2. Dlaczego potrzebna jest ochrona informacji?

Podchodząc metodycznie do traktowania zagadnienia ochrony informacji należy najpierw odpowiedzieć sobie wyczerpująco na pytanie postawione w tytule. Jeśli sporządzi się listę podstawowych powodów, dla których wymagana jest troska o całość i nienaruszalność informacji, ułatwi to następnie analizę zagrożeń, dokonanie oceny ryzyka i dobór środków ochrony.

Wydaje się, że w odniesieniu do każdego ośrodka APD będą słuszne następująco sformułowane motywy troski o bezpieczeństwo danych:

1. Większość organizacji posługujących się systemami informatycznymi prędzej czy później staje się niemal całkowicie zależna od nieprzerwanej dostępności systemu APD i zawartych w nim danych. Niezmiernie rzadko istnieje możliwość powrotu — w razie konieczności — do tradycyjnych metod przetwarzania danych.

2. Dane należą do ważnych i cennych zasobów. Zdobycie ich wymaga nakładów — czasem bardzo poważnych; są potrzebne do pomyślnego kontynuowania działalności; wiele może także kosztować ich odtworzenie. Pod tym względem informacja nie różni się wiele od środków materialnych.

3. Zachodzi potrzeba ochrony poufności informacji, np. rynkowej, patentowej, czy też personalnej. Nie powinna się ona dostać w ręce niepowołane.

4. Przy opracowywaniu systemu APD dokłada się wszelkich starań, aby był on łatwy w użyciu i dostępny dla tych wszystkich, którzy mają korzystać z jego usług. Niestety, jednocześnie mimowoli ułatwia się nadużycie systemu i zawartych w nim informacji ludziom nieuczciwym. Tak więc ochrona informacji i środowiska jej przetwarzania ma zarazem zmniejszyć prawdopodobieństwo, że ludzie nieuczciwi osiągną za pomocą systemu korzyść materialną.

5. Sprawa, która wiąże się z poprzednią: sprawiedliwość wymaga, aby można było uwolnić od podejrzeń wszystkich uczciwych ludzi, którzy mają do czynienia z systemem jako programiści, operatorzy czy konserwatorzy. Niezbędne jest więc zapewnienie możliwości natychmiastowego ustalenia osobowej odpowiedzialności za niedozwolone praktyki w celu zawężenia kręgu podejrzanych.

Kończąc ten krótki wstęp autor pragnie podkreślić, że omawiane w dalszej treści książki metody i środki zapewnienia ochrony informacji należy stosować obok i niezależnie od metod oraz środków nakazywanych przez ogólne i szczegółowe przepisy, dotyczące zachowania tajemnicy służbowej i państwowej w jednostkach gospodarki uspołecznionej i urzędach.

II. Ochrona środowiska przetwarzania informacji

1. Ochrona w warunkach przetwarzania wieloprogramowego

Kryteria ochrony

1. Żaden użytkownik nie może dotrzeć do danych lub programów innego użytkownika bez właściwego upoważnienia.
2. Żaden użytkownik nie może manipulować ani danymi, ani programami innego użytkownika bez właściwego upoważnienia.
3. Żaden użytkownik nie może pozbawić innego użytkownika możności korzystania z usług systemu, bez stosownego upoważnienia.

W systemach tzw. *drugiej generacji komputerów* ochrona informacji nie stanowiła poważnego problemu, ponieważ:

— tylko jeden użytkownik korzystał w danej chwili z systemu,

— zbiory każdego użytkownika znajdowały się na jego własnej taśmie magnetycznej (taśmie papierowej, kartach dziurkowanych) i mógł on je zabezpieczyć.

Systemy te miały jednak tę wadę, że nie można było oddzielić obszarów pamięci na bębnach i dyskach. Ponadto wykorzystanie systemu przy pracy jednoprogramowej było nieekonomiczne: albo pracował procesor a stały bezczynnie urządzenia wejścia i wyjścia, albo też pracowały urządzenia we/wy a próżnowała jednostka centralna.

Pojawienie się systemów *trzeciej generacji* zmieniło sytuację o tyle, że umożliwiło pracę w trybie w i e l o p r o g r a m o w y m. Z jednej strony uzyskano dzięki temu znacznie lepsze wykorzystanie zasobów systemu, z drugiej jednak strony zagadnienie ochrony informacji uległo wielkiemu skomplikowaniu. Wpłynęły na to następujące aspekty:

— zdalny, jednoczesny dostęp wielu użytkowników do jednego systemu,

— wspólne użytkowanie sprzętu, oprogramowania i banków danych przez różnych klientów — użytkowników ośrodka APD,

— użytkownicy przeważnie nie są znani osobiście operatorowi,

— system dostępny dla użytkowników potencjalnie wrogich.

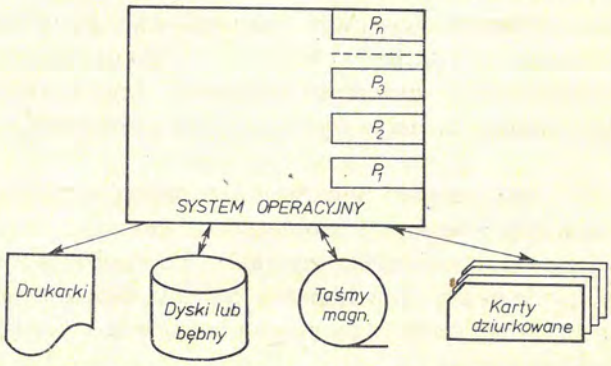
Wiele istniejących obecnie systemów częściowo rozwiązuje te problemy poprzez:

— uprzywilejowany tryb pracy tylko dla systemu operacyjnego (SO),

— architekturę systemu dostosowaną do potrzeb bezpiecznej pracy w trybie konwersacyjnym,

— zastosowanie segmentacji pamięci,

— stosowanie koncepcji tzw. *pamięci wirtualnej*.



Rys. 1. Uproszczona struktura systemu informatycznego trzeciej generacji

Na rysunku 1 została przedstawiona w sposób uproszczony organizacja typowego systemu trzeciej generacji. Programom P_1 do P_n są przydzielone obszary pamięci, poza które nie mogą one wykraczać. Programy te nie mogą inicjować podprogramów wejścia i wyjścia. Są one — przynajmniej teoretycznie — bezpieczne. Pracą całej instalacji komputerowej steruje skomplikowany system operacyjny, który między innymi:

— izoluje od siebie użytkowników,

— kontroluje dostęp do informacji własnej użytkownika,

— przydziela zasoby systemu,

— dysponuje programami usługowymi dla zapewnienia obsługi żądań użytkownika.

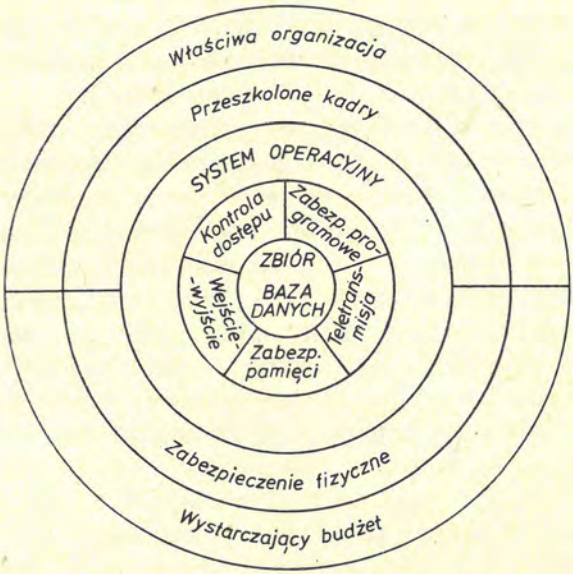
A jednak ten uprzywilejowany system operacyjny nie może być traktowany jako gwarantujący pełną ochronę informacji. Dzisiejsze systemy operacyjne bywają ogromne — ponad 200 000 instrukcji, a wszystkie uprzywilejowane — i już same ich rozmiary stanowią problem. Zdarzają się przypadki niezamierzonego uprzywilejowania pewnych działań użytkownika; istnieje czasem możliwość zastąpienia przez użytkownika pewnych procedur SO własnymi, istnieją też czasem „furtki", przez które może „przeciekać" informacja. Niezależnie od tego zweryfikowanie, sprawdzenie pełnej niezawodności SO jest, ze względu na jego rozmiary, praktycznie niewykonalne. Niewielką pociechą jest to, że świadome wykorzystanie słabości określonego SO możliwe jest tylko dla zaawansowanych specjalistów o dużym doświadczeniu w pracy z danym SO. Zawęża to jednak przynajmniej krąg osób „niepewnych".

Nowsze koncepcje systemowe przewidują wprowadzenie dla komputerów generacji *trzeciej plus* — struktury tzw. *jądrzastej* (*kernel, nucleus structure*). Jedynie mała część SO (jądro) steruje dostępem i wykonuje instrukcje uprzywilejowane. Dokładne zaprojektowanie i sprawdzenie niezawodności tego jądra w aspekcie ochrony informacji powinno być łatwiejsze. Nie należy jednak przewidywać wprowadzenia struktury jądrzastej do działających obecnie systemów trzeciej generacji. Istniejących dotychczas SO nie można dzielić, a wprowadzenie odpowiednich zmian wymagałoby gruntownej przeróbki, której wynikiem byłoby zapewne pogorszenie funkcjonalności systemu i obniżenie jego sprawności.

Ochrona w głąb

Jednak zaprojektowanie nawet najlepszego systemu operacyjnego nie wystarcza. Skuteczny system ochrony informacji musi prezentować szereg barier, które wspólnie dopiero utworzą względnie niezawodny zespół środków zabezpieczających. Taki system ochrony przedstawiono poglądowo na rys. 2. Widoczne na tym rysunku koncentryczne pierścienie przedstawiają „linie obrony" przed różnymi typami zagrożeń. Zadaniem tych linii obrony jest ochrona nienaruszalności i prawidłowej dostępności zbiorów danych, znaj-

dujących się w centrum układu. Dwa zewnętrzne pierścienie można zaliczyć wspólnie do *organizacyjnych*, czy też *administracyjnych środków ochrony*. Trzeci pierścień reprezentuje system operacyjny, który otacza i kontroluje wewnętrzne segmenty, obejmujące kontrolę dostępu, wejście i wyjście, przechowywanie informacji, sterowanie transmisją danych (teledacją) oraz programy użytkowe.



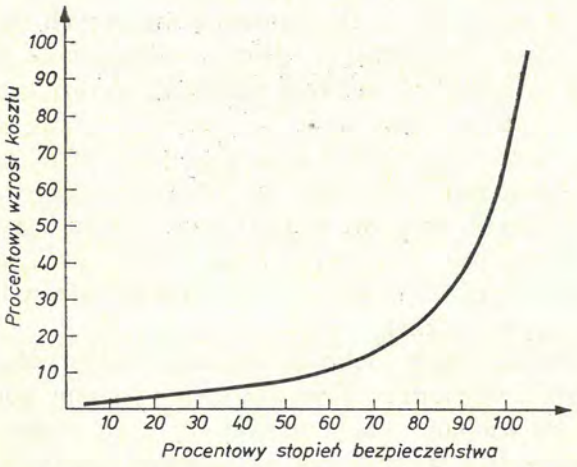
Rys. 2. Pierścieniowa struktura systemu ochrony informacji

Tę część układu można nazwać *zabezpieczeniem logicznym*. Zarazem jednak system operacyjny reprezentuje i stanowi operacyjne odbicie architektury sprzętu komputera (*hardware*), który nie jest tu osobno przedstawiony, ma jednak również pewną funkcję do spełnienia w systemie ochrony — jest to zabezpieczenie o charakterze pośrednim między fizycznym i logicznym, łączące obie te cechy. W ogóle granice między pierścieniami mają dość płynny charakter i poszczególne dziedziny ściśle zazębiają się ze sobą. Na przykład decyzja o przechowywaniu kopii określonych zbiorów danych w innym budynku, będąc w zasadzie sprawą ochrony fizycznej, rzutuje jednocześnie na budowę i sposób eksploatacji systemu APD.

Koszt ochrony

Stopień koniecznego zabezpieczenia jest wprost proporcjonalny do prawdopodobieństwa zagrożenia z jednej, a do wrażliwości informacji z drugiej strony. Tylko kierownictwo ośrodka APD może określić praktyczną wartość systemu zabezpieczeń, ponieważ tylko ono zna faktyczną wartość danych, które mają być chronione.

Koszty zabepieczenia systemu wzrastają gwałtownie (wykładniczo) wraz ze stopniem wymaganego zabezpieczenia (rys. 3). Zanim kierownictwo będzie mogło zadecydować, jakie należy zastosować środki zabezpieczenia, musi ono ustalić wartość danych albo też wielkość strat w razie dostania się ich w niepowołane ręce, uszko-



Rys. 3. Koszt zabezpieczenia w funkcji stopnia tego zabezpieczenia

dzenia lub zniszczenia. Następnie należy określić prawdopodobieństwo wystąpienia każdego z wymienionych wydarzeń. Zestawienie obu grup liczb umożliwi orientacyjne określenie wielkości nakładów, jakie należy ponieść, aby uzyskać pożądany stopień bezpieczeństwa.

Nie istnieje — i nie może istnieć — całkowicie bezpieczny ośrodek obliczeniowy, chyba że... nie pracuje się w nim. Nie można także mówić o jakimś generalnie zalecanym stopniu zabezpieczenia. Właściwy, racjonalny system zabezpieczenia będzie różny dla

różnych ośrodków, będzie zależał od wielu czynników. W książce tej omawia się wiele środków i metod prowadzących do lepszej ochrony informacji. Wszystkie one pociągają za sobą jakieś skutki — najczęściej finansowe, ale także zmniejszenie swobody a często i obniżenie wydajności pracy. Nie każda z tych metod nadaje się dla każdej instalacji. Tak więc, rozpatrując w aspekcie racjonalności i efektywności poziom zabezpieczenia danego ośrodka należy brać pod uwagę dwa podstawowe względy: prawdopodobieństwo wystąpienia określonego zagrożenia oraz rozmiary strat, jakie może pociągnąć za sobą wystąpienie tego zagrożenia.

I w tym miejscu zaczynają się zazwyczaj kłopoty i spory. Wynikają one z potrzeby określenia wartości, jaką przedstawiają sobą poszczególne rodzaje danych. Istotnie, ścisłe obliczenie kosztów związanych ze stratą lub uszkodzeniem konkretnych danych jest często niemożliwe. Po głębszym jednak zastanowieniu w każdym przypadku można sprecyzować rząd wielkości, wyrażającej te koszty. Taka przybliżona ocena może już pomóc w podjęciu decyzji, jakie środki warto zaangażować w ochronę rozważanej informacji. Dobrze jest opracować formularz, na którym znajdzie się wykaz wszystkich ważnych zbiorów, a dalej sześć kolumn (jak już powiedziano, należy brać pod uwagę sześć „nieszczęść", jakie mogą przytrafić się danym, a dla każdego z tych przypadków implikacje finansowe mogą być różne).

Krótko mówiąc, należy dokonać analizy efektywności środków ochrony, gdzie kryterium stanowi stosunek nakładów ponoszonych na te środki do wielkości potencjalnych strat, przy uwzględnieniu prawdopodobieństwa wystąpienia określonego zagrożenia.

Oczywiście, istnieją sytuacje (np. informacja dla celów zarządzania gospodarką narodową, informacja wojskowa), gdy waga informacji jest taka, że kryteria ekonomiczne przestają mieć decydujące znaczenie.

Analiza rodzajów zagrożeń, a następnie ustalenie zasad ochrony i wdrożenie ich, wchodzi w zakres obowiązków i odpowiedzialności kierownictwa ośrodka APD. Jednakże wnioski z analizy i plan zabezpieczeń muszą zostać przedstawione do zatwierdzenia naczelnemu kierownictwu zainteresowanej instytucji lub przedsiębiorstwa. Ono bowiem przede wszystkim odpowiada za ochronę wszelkich zasobów i ono musi zatwierdzić i sfinansować środki tej

ochrony. W szczególności odnosi się to do redundancji sprzętu. W tym przypadku prawo zmniejszania się efektywności ekonomicznej w miarę wzrostu nakładów związanych z zabezpieczeniem działa szczególnie ostro. Jeśli potrzeba zapewnienia niezawodności systemu nie jest dyktowana ryzykiem ogromnych strat w razie niemożności kontynuowania pracy, wydatki na zdublowanie (choćby tylko częściowo) sprzętu mogą być marnotrawstwem. Z tego szczególnie względu istnieje potrzeba zastosowania kwantyfikacji potencjalnych strat.

Prawdopodobieństwo zagrożeń

Procentowe wyrażanie efektywności ochrony informacji — obliczonej w wyniku przeprowadzonej analizy — w postaci prawdopodobieństwa wystąpienia określonego zagrożenia stwarzałoby jedynie iluzję statystycznej dokładności, która praktycznie jest nieosiągalna. Lepiej chyba wprowadzić pięć lub sześć stopni prawdopodobieństwa, poczynając od kategorii „ochrona konieczna" — gdzie środki zabezpieczenia m u s z ą być podjęte bez względu na stopień prawdopodobieństwa zagrożenia — poprzez kategorie: wysokie, średnie, niskie i zaniedbywalne prawdopodobieństwo zagrożenia.

Z dotychczasowej praktyki wynika, jak wskazują przeprowadzone ankiety i analizy statystyczne, że prawdopodobieństwo najczęściej występujących zagrożeń można uszeregować w następującym porządku (malejąco):

1. Błędy i przeoczenia personelu.

2. Nieuczciwość personelu. Na podstawie dotychczasowych doświadczeń (zebranych w różnych źródłach) można stwierdzić, że większość przestępstw popełnionych w związku z systemami APD spowodował pracownik poszkodowanej instytucji sam, albo przynajmniej uczestniczył on w nich wraz z osobami z zewnątrz. Te same źródła podają również, że na ogół wykorzystywane są nieuczciwie te dane i te funkcje systemu, do których pracownicy mają dostęp z tytułu wykonywanych zadań. Tak więc na przykład nieuczciwi pracownicy gospodarki materiałowej mogą manipulować na swoją korzyść stanem magazynów, ale nie wprowadzają oszukańczych zmian do list płacy, i vice versa, pracownicy rachuby

płac nie zniekształcają informacji o stanie magazynów. Inaczej mówiąc, malwersacje dokonywane są w dziedzinie dobrze znanej (w związku z czym często lekceważy się niebezpieczeństwo przyłapania na niedozwolonych praktykach), nie występuje natomiast na ogół, zapewne jako zbyt ryzykowne, przekraczanie barier kompetencyjnych.

3. Szkody spowodowane pożarem. Pożar nie musi wybuchnąć w pomieszczeniu komputera, aby całkowicie przerwać eksploatację ośrodka. Może bowiem np. spowodować odcięcie dopływu energii z sieci, unieruchomić urządzenia klimatyzacyjne lub uniemożliwić dostęp do formularzy niezbędnych do wydruków. O takich efektach pożaru często zapomina się. Przy planowaniu systemów wykrywania i gaszenia pożarów nie przywiązuje się dostatecznej wagi do pomieszczeń tzw. zaplecza. Znajduje się tam często znacznie więcej materiałów łatwopalnych niż w samym pomieszczeniu komputera, gdzie prawdopodobieństwo pożaru jest w istocie niewielkie. Duże natomiast jest prawdopodobieństwo przerwy w pracy ośrodka — czasem długotrwałej — spowodowanej pośrednio pożarem w pomieszczeniach zaplecza.

4. Rozgoryczenie pracowników. W instytucjach, w których panuje niewłaściwa atmosfera, a kierownictwo opieszale lub niechętnie reaguje na mniej lub bardziej słuszne życzenia pracowników, rozgoryczeni mogą „mścić się" — sabotując aktywnie lub pasywnie pracę ośrodka APD. Znanych jest szereg takich przypadków, niejednokrotnie pociągających za sobą poważne straty, nie tylko natury finansowej.

5. Szkody wodne. Zagrożenie powodziowe może być, oczywiście przy określonej lokalizacji budynku ośrodka APD, zupełnie poważne. Większość jednak szkód wodnych spowodowały dotychczas takie drobne zaniedbania, jak przeciekający dach lub pęknięta rura piętro wyżej niż zlokalizowano komputer. Szkód takich można by łatwo uniknąć, lub znacznie je ograniczyć, jeżeli ma się po prostu pod ręką rulon folii polietylenowej i parę nożyczek.

6. Inne. Są to zazwyczaj zagrożenia ze strony osób, nie mających obecnie (lub do niedawna) bezpośredniego kontaktu z systemem. Na ogół straty połączone z tymi zagrożeniami są niewielkie. Odnotowano szereg okoliczności, kiedy utalentowani studenci informatyki lub matematyki przełamywali dla sportu logiczne bariery do-

stępu do komputera. W przeciwieństwie do zagrożeń przestępczych, te „sportowe" zagrożenia szybko zazwyczaj są ujawniane przez samych sprawców („sława mołojecka" tego wymaga!). Zazwyczaj sprawcy ci nie chcą wcale (lub nie mogą) wykorzystywać „swojego" dostępu w sposób przynoszący komukolwiek szkodę.

Planowanie systemu zabezpieczeń

Pierwszym krokiem w procesie planowania systemu zabezpieczeń powinno być ustalenie osoby odpowiedzialnej za opracowanie, a następnie wdrożenie planu ochrony informacji i środowiska jej przetwarzania. Ta sama zazwyczaj osoba będzie następnie na bieżąco nadzorowała pracę ośrodka APD z punktu widzenia bezpieczeństwa informacji. Taki specjalista od ochrony informacji (ang. *Data Security Manager*) powinien być członkiem kierownictwa ośrodka i mieć decydujący głos we wszelkich sprawach związanych z bezpieczeństwem informacji.

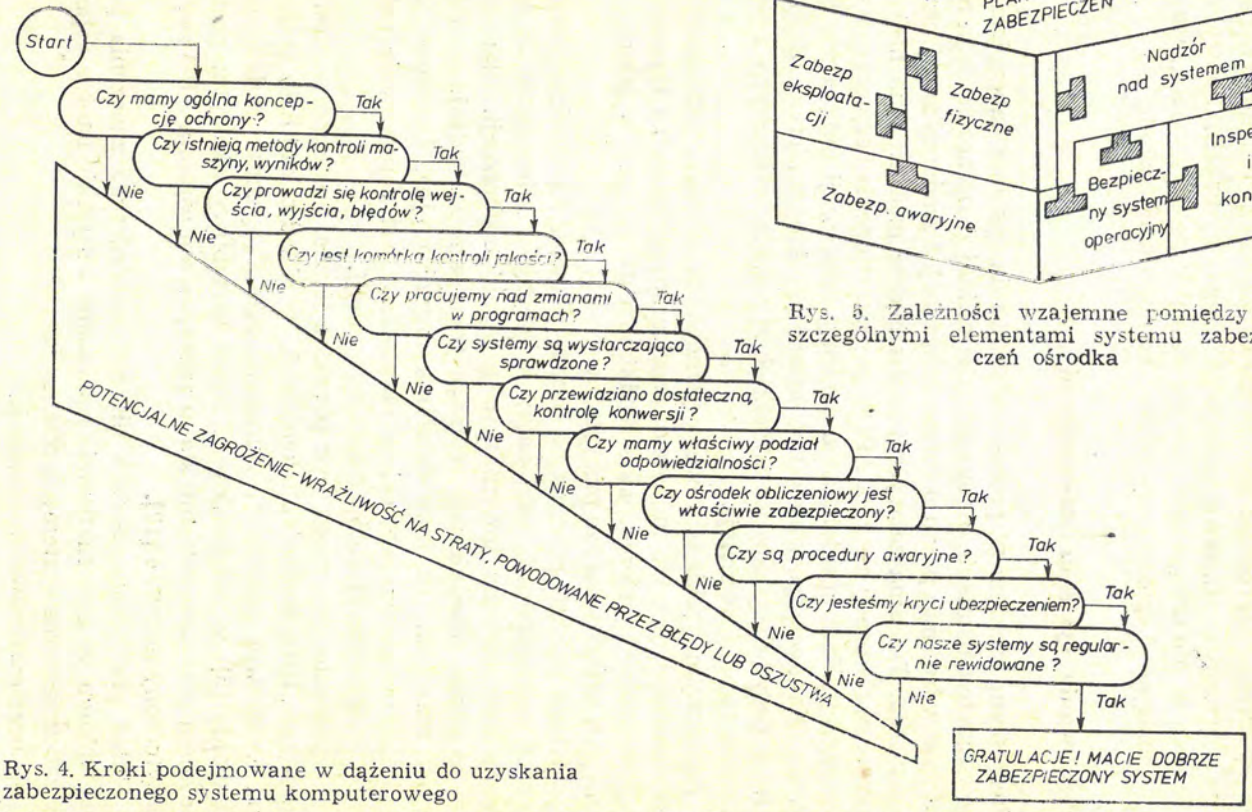
Następnym krokiem procesu planowania systemu zabezpieczeń powinna być, jak już mówiono, analiza specyficznych i typowych zagrożeń oraz ustalenie, jakie środki zabezpieczenia i w jakich sytuacjach należy uznać za priorytetowe.

Od tego punktu poczynając proces planowania powinien polegać na podejmowaniu racjonalnych decyzji w odniesieniu do zabezpieczeń systemu informacyjnego danej organizacji. Planowanie systemu zabezpieczeń wymaga tego samego rodzaju wnikliwych rozważań, co inne działania organizacyjne. Podobnie jak w innych przypadkach, celem planowania jest zapewnienie osiągnięcia określonych celów danej organizacji.

W procesie tym mogą być pomocne liczne, dostępne w literaturze tzw. *listy kontrolne* (*checklists*). Przykład takiej listy podano (na podstawie publikacji Europejskiego Programu Badawczego Diebolda [5]) w załączniku A. Nieco żartobliwy algorytm postępowania przy sprawdzaniu stanu zabezpieczeń ośrodka APD został przytoczony na rys. 4 [12].

Układ planu zabezpieczeń nie ma zasadniczego znaczenia pod warunkiem, że systematycznie rozważono wszystkie istotne aspekty zabezpieczenia systemu, a mianowicie:

— bezpieczeństwo eksploatacji,



Rys. 4. Kroki podejmowane w dążeniu do uzyskania zabezpieczonego systemu komputerowego

Źródło: J. J. Wasserman „Plugging the leaks in computer security". Harvard Business Review, 1969

Rys. 5. Zależności wzajemne pomiędzy poszczególnymi elementami systemu zabezpieczeń ośrodka

— „wewnętrzne" zabezpieczenie komputera,
— bezpieczeństwo fizyczne,
— kontrola i inspekcja,
— nadzór nad systemem,
— plan usuwania skutków awarii.

Wzajemną zależność między tymi elementami zilustrowano na rys. 5.

Plan przebiegu wznawiania działalności po katastrofie stanowi w gruncie rzeczy najlepszą gwarancję, że w obliczu najgroźniejszej nawet awarii organizacja oraz jej system obiegu informacji jakoś przetrwają.

2. Zabezpieczenie nowo projektowanego ośrodka APD

Ze zrozumiałych względów projektowanie nowego ośrodka obliczeniowego jest najwłaściwszym momentem do racjonalnego zaprojektowania kompleksowego systemu ochrony informacji. Sytuacja jest idealna, jeśli można sobie pozwolić na postawienie specjalnego budynku tak zaprojektowanego, aby spełniał wszystkie wymagania funkcjonalne. Uwzględnienie w projekcie wymagań ochrony informacji jest stosunkowo łatwe, a nakłady finansowe na środki zabezpieczające są — w stosunku do całkowitego kosztu inwestycji — nieznaczne. Nieco inaczej wygląda sprawa, gdy do potrzeb nowo instalowanych urządzeń APD muszą zostać przystosowane istniejące już budynki lub pomieszczenia. Występuje wówczas szereg czynników ograniczających swobodę planowania zabezpieczeń. Warto zwrócić uwagę na następujące z wyłaniających się wówczas problemów:

1. Przestrzeń. Wiele urządzeń zabezpieczających wymaga miejsca, o które często niełatwo w istniejących już budynkach. Do takich urządzeń należą np. tzw. „śluzy" lub sprzęt awaryjny i urządzenia dublujące. Nawet w nowo projektowanych budynkach koszt dodatkowej powierzchni może decydować o zaniechaniu określonych poczynań.

2. Trudności techniczne. Niejednokrotnie pożądane środki ochrony są nierealizowalne w istniejących budynkach z powodu trudności budowlanych lub instalacyjnych.

3. Istniejące ciągi ruchu. Drogi ruchu materiałów oraz ruch osobowy mogą zostać utrudnione przez zainstalowanie urządzeń zabezpieczających. Nie zawsze udaje się przezwyciężyć zakorzenione, tradycjonalne nawyki.

4. Niedocenianie ważności problemu. W wielu przypadkach decyzje dotyczące przedsięwzięć zabezpieczających delegowane są do szczebla, który nie ma dostatecznego wpływu na całokształt projektu.

Wymienionych czynników nie należy lekceważyć. A jednak często okazuje się, że warunki użytkowania nowo uruchomionego ośrodka nakazują wprowadzenie środków ochrony do istniejącej już instalacji i wówczas koszty z tym związane okazują się wielokrotnie wyższe niż te, jakie poniesiono by w przypadku kompleksowego projektowania systemu — pomijając już straty na skutek zakłóceń pracy funkcjonującego ośrodka, powodowanych instalowaniem zabezpieczeń.

Z uwagi na szybki postęp techniczny oraz zmieniające się potrzeby nie można wymagać od przeciętnego użytkownika APD, aby w czasie opracowywania projektu ośrodka dysponował wszystkimi informacjami, które pozwoliłyby mu na optymalne opracowanie planu zabezpieczeń oraz przeprowadzenie jego realizacji. Należy tu uwzględniać zbyt wiele czynników, których ciężar gatunkowy ocenić mogą tylko fachowcy. Dlatego projekt ośrodka obliczeniowego powinien być wykonywany przez wyspecjalizowane biuro projektowe.

W opracowywaniu założeń do projektu ośrodka APD może i powinien współuczestniczyć — między innymi w zakresie zagadnień ochrony środowiska przetwarzania informacji — dostawca komputera. Doświadczone firmy komputerowe zatrudniają specjalistów z dziedziny tzw. *site planning*, których zadaniem jest udzielenie pomocy w opracowaniu założeń projektowych.

Decyzyjne kryteria wyboru środków ochrony

Przystępując do opracowania założeń projektowych w części dotyczącej środków ochrony informacji projektant musi wiedzieć, jaki stopień zabezpieczenia potrzebny jest użytkownikowi. Jeśli przeciętnemu użytkownikowi systemu APD postawi się takie pytanie,

z pewnością wprawi się go w zakłopotanie. A przecież problem ten ma zasadnicze znaczenie! Pomocne mogą tu być pytania uzupełniające:

1. Jaka jest wartość i znaczenie projektowanego systemu? Odpowiedź musi uwzględniać nie tylko koszt instalacji, ale również rodzaj wykonywanej pracy. Jeśli jest to np. system kontroli ruchu samolotów, od niezawodności jego pracy zależy życie lub śmierć wielu ludzi. Jeśli jest to system sterowania produkcją — przerwa w jego pracy może spowodować ogromne straty finansowe. W obu tych przypadkach potrzebny będzie inny stopień pewności zabezpieczenia, aniżeli w przypadku systemu, którego awaria może wprawdzie być przykra w skutkach, ale nie spowoduje katastrofalnych konsekwencji, a stracony w efekcie przestoju czas — można później nadrobić.

2. Jakie zagrożenia — oprócz tych, z którymi zawsze trzeba liczyć się — są charakterystyczne dla danego systemu? W odpowiedzi trzeba uwzględnić podział na dwa rodzaje zagrożeń:

Zagrożenia typowe
- pożar,
- szkody wodne,
- sabotaż,
- kradzież,
- przerwa w dopływie energii.

Zagrożenia specjalne
- obce pola magnetyczne,
- wstrząsy,
- eksplozje,
- uszkodzenia łączy transmisyjnych itp.

Istnieje wiele sposobów dokonywania analizy, prowadzącej do opracowania skutecznego planu zabezpieczeń. Ilustracją może tu być sposób postępowania zaproponowany przez W. Flory z firmy „Sperry UNIVAC" podczas seminarium (1973 r.) na temat „Bezpieczeństwo instalacji EPD" [8]. Opisana metoda postępowania sprawdziła się w praktyce. Na czym w ogólnych zarysach polega to postępowanie, wyjaśniają następujące zalecenia:

1. Sporządzić pełną listę możliwych zagrożeń.

2. Dokonać oceny ewentualnego wpływu tych zagrożeń na instalację i na proces przetwarzania.

TABLICA II (1)

Analiza zagrożeń i plan zabezpieczeń

Rodzaj zagrożenia	Zabezpieczenie konieczne (niezależnie od prawdopodobieństwa wystąpienia zagrożenia)	Przewidywane skutki	Podział kosztów i odpowiedzialności
1. Pożar, eksplozja Dotknięty cały budynek		Przerwa w pracy ośrodka, trwająca tygodnie lub miesiące Koszt: powyżej 15 mln dol.	A — w koszty budowy B — w koszty komputera C — z budżetu służby ochrony

Lp.	Środki ochrony	Komentarz i decyzje	Zalecenia dodatkowe	Podział kosztów	Odpowiedzialność
1	System alarmowy ppoż. w całym budynku (P)*	Sala komputera, korytarze, pom. technologiczne	Dofinansowanie budowy	B	Biuro projektów
2	Zasuwy ogniowe w przewodach klimatyzacyjnych (P)	Zgodnie z instrukcjami Straży Pożarnych	Dofinansowanie na instalację gaśniczą	A	Biuro projektów
3	Hydranty (P)	Zgodnie z instrukcjami Straży Pożarnych		A	Biuro projektów
4	Szczelne stropy dla uniknięcia szkód wodnych	Zgodnie z przepisami budowlanymi		A	Biuro projektów
5	Strefy ogniowe (P)	Zostaną wprowadzone w czasie prac instalacyjnych		C	Biuro projektów Kier. budowy

TABLICA II (1) cd.

Lp.	Środki ochrony	Komentarz i decyzje	Zalecenia dodatkowe	Podział kosztów	Odpowiedzialność
6	Przechowywanie nośników w szafach ogniotrwałych (P)	Przewidziane. Dodatkowo: składowanie w innym budynku		B	Dział APD
7	Plan akcji ppoż. (P)	Musi zostać opracowany przed instalacją komputera		—	Dział APD
8	Zakaz palenia (P)	Tylko w sali komputera		—	Dział APD
9	Urządzenia gaszące na CO_2 lub halon w pomieszczeniach APD (P)	Dodatkowo: gaśnice przenośne		B	Dział APD
10	Przetwarzanie w innym ośrodku APD (L)*	Należy uzgodnić z dostawcą komputera	Zawrzeć porozumienie na piśmie	—	Dział APD
11	Ogniotrwałe materiały budowlane (P)	Uwzględnić przy wyposażaniu wnętrz		B	Biuro projektów

Objaśnienia: *) P — środki prewencyjne, L — likwidacja skutków: dotyczy tablicy od II (1) do II (14)

TABLICA II (2)

Analiza zagrożeń i plan zabezpieczeń

Rodzaj zagrożenia	Prawdopodopieństwo zagrożenia małe	Przewidywane skutki	Podział kosztów i odpowiedzialności
2. Pożar, eksplozja, zadymienie Dotknięte urządzenia komputera lub ich części		Przerwa w pracy trwająca godziny, dni lub tygodnie Koszt: do 5 mln dol.	A — w koszty budowy B — w koszty komputera C — z budżetu służby ochrony

Lp.	Środki ochrony	Komentarz i decyzje	Zalecenia dodatkowe	Podział kosztów	Odpowiedzialność
1	Patrz punkty 1÷11 tablicy II (1) (P)	Patrz punkty 1÷11 tablicy II (1)		—	—
2	Gaśnice przenośne (P)	Przewidziano w wystarczającej liczbie		A	Dział APD
3	Dublowanie sprzętu (P)	Przewidziano na pierwszym etapie rozbudowy komputera		—	—
4	Szybka wymiana uszkodzonych części (L)	Zostanie uzgodniona z dostawcą sprzętu		—	Dział organizacji
5	Praca w ograniczonym rozmiarze godzin (L)	Możliwa. Należy omówić i ustalić na piśmie z Wydziałem Programowania i Działem Produkcji.		—	Dział APD

TABLICA II (3)

Analiza zagrożeń i plan zabezpieczeń

Rodzaj zagrożenia	Prawdopodobieństwo zagrożenia średnie	Przewidywane skutki	Podział kosztów i odpowiedzialności
3. Pożar, eksplozja, zadymienie Dotknięte zaplecze techniczne		Przerwa w pracy, zależnie od zakresu szkód Koszt: ok. 250 tys. dol.	A — w koszty budowy B — w koszty komputera C — z budżetu służby ochrony

Lp.	Środki ochrony	Komentarz i decyzje	Zalecenia dodatkowe	Podział kosztów	Odpowiedzialność
1	Patrz p. 1÷11 tablicy II (1) oraz 2÷5 tablicy II (2) (P)	Patrz p. 1÷11 tablicy II (1) oraz 2÷5 tablicy II (2)	Przewidzieć zapasową powierzchnię	—	—
2	Dublowanie awaryjne (P)	Przewidziano przy dublowaniu sprzętu		C	Wydział techniczny
3	Możliwość przełączenia zasilania (P)	Zakłady Energetyczne: zasilanie dwustronne		A	Biuro projektów
4	Szybka wymiana uszkodzonych urządzeń (L)	Wyjaśnić możliwości z dostawcami	Wyjaśnić przed zawarciem kontraktu i ustalić na piśmie	—	Wydział techniczny
5	Praca w ograniczonym rozmiarze godzin (L)	Częściowo możliwa			

TABLICA II (4)

Analiza zagrożeń i plan zabezpieczeń

Rodzaj zagrożenia	Prawdopodobieństwo zagrożenia duże	Przewidywane skutki	Podział kosztów i odpowiedzialności
4. Woda Szkody wodne. Brak dopływu		Przerwa w pracy: od kilku godzin do paru tygodni Koszt: rzędu 150 tys. dol.	A — w koszty budowy B — w koszty komputera C — z budżetu służby ochrony

Lp.	Środki ochrony	Komentarz i decyzje	Zalecenia dodatkowe	Podział kosztów	Odpowiedzialność
1	Sprawdzić przebieg przewodów wodociągowych (P)	W obrębie sali komputera: żadnych		—	Biuro projektów
2	Odpływ z podwieszonego sufitu i spod podwójnej podłogi (P)	Zbyteczne		—	Biuro projektów
3	Szczelność stropów (P)	W sali komputera stropy bez łączeń		—	Biuro projektów
4	Zbiornik wody nawilżającej (P)	Przewidziano w projekcie klimatyzacji		C	Wydział techniczny
5	Osłony na urządzenia z folii (L)	Zostaną zamówione		C	Dział APD
6	Sala komputera na piętrze (P)	I piętro i parter	Sprawdzić sytuację powodziową w okolicy; ewentualnie przewidzieć zabezpieczenie parteru	—	—
7	Plan akcji powodziowej (L)	Zostanie opracowany przed uruchomieniem ośrodka		—	Dział APD
8	Ochrona pomieszczeń technicznych w suterenie (P)	Zaplanowano agregat pompowy		A	Biuro projektów

TABLICA II (5)

Analiza zagrożeń i plan zabezpieczeń

Rodzaj zagrożenia	Prawdopodobieństwo zagrożenia małe	Przewidywane skutki	Podział kosztów i odpowiedzialności
5. Wilgotność		Za duża: tworzenie się kondensatu Za mała: ładunki elektrostatyczne Uszkodzenie urządzeń, awaria instalacji Koszt: poniżej 100 tys. dol.	A — w koszty budowy B — w koszty komputera C — z budżetu służby ochrony

Lp.	Środki ochrony	Komentarz i decyzje	Zalecenia dodatkowe	Podział kosztów	Odpowiedzialność
1	Kontrola i sygnalizacja alarmowa (P)	Zaplanowano rejestrację z kilkoma punktami pomiaru		B	Wydział techniczny
2	Zdublowana kontrola (P)	Przewidziano w I fazie rozbudowy komputera		C	Wydział techniczny
3	Zapewnienie nieprzerwanego zasilania wodą (P)	Przewidziano		C	Wydział techniczny
4	Naprawa (L)	Kontrakt na konserwację		B	Dział APD

TABLICA II (6)

Analiza zagrożeń i plan zabezpieczeń

Rodzaj zagrożenia	Prawdopodobieństwo zagrożenia małe	Przewidywane skutki	Podział kosztów i odpowiedzialności
6. Zapylenie		Przerwy w pracy, wpływ na dokładność odczytu, wpływ na trwałość nośników danych Koszt: poniżej 10 tys. dol.	A — w koszty budowy B — w koszty komputera C — z budżetu służby ochrony

Lp.	Środki ochrony	Komentarz i decyzje	Zalecenia dodatkowe	Podział kosztów	Odpowiedzialność
1	Ochrona nośników (P)	Archiwum nośników z odrębną klimatyzacją		B	Dział APD
2	Zakaz palenia w sali komputera (P)	Będzie egzekwowany	Przewidzieć palarnię	—	Dział APD
3	Filtry, wymiana filtrów (P)	Przewidziano w projekcie klimatyzacji		B	Wydział techniczny
4	Regularne sprzątanie (P)	Osobna sprzątaczka dla pomieszczenia komputera	Poinstruować sprzątaczkę, opracować zasady zachowania w pomieszczeniu komputera	B	Dział administracyjny
5	Nadciśnienie w sali komputera (P)	Przez dopływ świeżego powietrza		B	Wydział techniczny
6	Nieścieralna wykładzina podłogowa (P)	Podłogi w budynku lakierowane		B	Biuro projektów
7	Izolacja dźwiękochłonna szczelnie zapakowana (P)	Wprowadzić do warunków dostawy		B	Biuro projektów
8	Usunąć sprawcę zapylenia (L)	—		—	—
9	Przeprowadzić gruntowne sprzątanie	—		—	—

TABLICA II (7) *Analiza zagrożeń i plan zabezpieczeń*

Rodzaj zagrożenia	Prawdopodobieństwo zagrożenia znikome	Przewidywane skutki	Podział kosztów i odpowiedzialności
7. Obce pola magnetyczne		Zniszczenie danych Koszt: poniżej 10 tys. dol.	A — w koszty budowy B — w koszty komputera C — z budżetu służby ochrony

Lp.	Środki ochrony	Komentarz i decyzje	Zalecenia dodatkowe	Podział kosztów	Odpowiedzialność
1	Ekranowanie przewodów wysokiego napięcia (P)	Według specyfikacji dostarczonej przez dostawcę komputera		B	Wydział techniczny
2	Skontrolować otoczenie na możliwe źródła zakłóceń (P)	Zlecić wydz. technicznemu i dostawcy komputera	Jeśli potrzebne pomiary wykażą wartości przekraczające dopuszczalne — natychmiast przewidzieć przeciwśrodki — np. *klatki Faradaya*	B	Wydział techniczny
3	Pomiary (jeśli stwierdzono wg p. 2 występowanie źródeł zakłóceń) (P)	Zależnie od p. 2, wg naszego rozeznania niepotrzebne		—	—
4	Antystatyczna wykładzina podłogowa i materiały budowlane (P)	Przewidzieć w projekcie budynku, zgodnie ze specyfikacją dostawcy komputera		B	Biuro projektów

TABLICA II (8)

Analiza zagrożeń i plan zabezpieczeń

Rodzaj zagrożenia	Prawdopodobieństwo zagrożenia znikome	Przewidywane skutki	Podział kosztów i odpowiedzialności
8. Wstrząsy		Zakłócenia w pracy instalacji, utrata danych (jednostki dyskowe) Koszty: nieznaczne	A — w koszty budowy B — w koszty komputera C — z budżetu służby ochrony

Lp.	Środki ochrony	Komentarz i decyzje	Zalecenia dodatkowe	Podział kosztów	Odpowiedzialność
1	Sprawdzić, czy występują wstrząsy (P)	Autostrada w pobliżu		—	—
2	Przeprowadzić pomiary (P)	Zlecono pomiary odpowiedniej jednostce		B	Biuro projektów
3	Podjąć środki stosowne do wyników pomiarów (P)	Wyników pomiarów jeszcze nie otrzymano		B	Biuro projektów
4	Sprawdzić, czy instalacje pomocnicze nie wywołują wstrząsów (P)	Biuro projektów obliczyło ułożyskowanie dla agregatu Diesla		C	Biuro projektów

TABLICA II (9)

Analiza zagrożeń i plan zabezpieczeń

Rodzaj zagrożenia	Prawdopodobieństwo zagrożenia średnie	Przewidywane skutki	Podział kosztów i odpowiedzialności
9. Przerwa w zasilaniu energią Wahania napięcia zasilania		Przerwa w pracy. Powtarzanie prac. Uszkodzenie urządzeń. Koszt: poniżej 10 tys. dol.	A — w koszty budowy B — w koszty komputera C — z budżetu służby ochrony

Lp.	Środki ochrony	Komentarz i decyzje	Zalecenia dodatkowe	Podział kosztów	Odpowiedzialność
1	Dwustronne zasilanie (P)	Uzgodniono z Zakładem Energetycznym		—	—
2	Buforowanie zasilania (P)	Przewidziano przy rozbudowie komputera		B/C	Wydział techniczny
3	Zasilanie awaryjne (P)	Przewidziano przy rozbudowie komputera		C	Wydział techniczny

TABLICA II (10)

Analiza zagrożeń i plan zabezpieczeń

Rodzaj zagrożenia	Prawdopodobieństwo zagrożenia średnie	Przewidywane skutki	Podział kosztów i odpowiedzialności
10. Uszkodzenia urządzeń: modemy		Przerwa w pracy Koszt: nieznaczny	A — w koszty budowy B — w koszty komputera C — z budżetu służby ochrony

Lp.	Środki ochrony	Komentarz i decyzje	Zalecenia dodatkowe	Podział kosztów	Odpowiedzialność
1	Konserwacja zapobiegawcza (P)	Kontrakt na konserwację		B	Dział APD
2	Jednostki zamienne (L)	Przyjęto do magazynu 2 modemy		0,5 B + + 0,5 C	Dział APD

TABLICA II (11)

Analiza zagrożeń i plan zabezpieczeń

Rodzaj zagrożenia	Prawdopodobieństwo zagrożeń znikome	Przewidywane skutki	Podział kosztów i odpowiedzialności
11. Sabotaż, złośliwe uszkodzenie		Przerwa w pracy o czasie trwania zależnym od rodzaju uszkodzenia Koszty: mogą przekraczać 100 tys. dol.	A — w koszty budowy B — w koszty komputera C — z budżetu służby ochrony

Lp.	Środki ochrony	Komentarz i decyzje	Zalecenia dodatkowe	Podział kosztów	Odpowiedzialność
1	Zabezpieczenie fizyczne ośrodka (P)	Lokalizacja ośrodka eksponowana ze względów niezależnych od projektanta. Okna wyposażono w szyby pancerne		C	Biuro projektów
2	Kontrola dostępu do komputera (P)	Przewidziano system na karty kodowane		C	Biuro projektów
3	Ograniczenie kręgu uprawnionych do dostępu (P)	Zostanie uzyskane za pomocą kodowanych kart wejściowych		—	Dział APD
4	Troskliwy dobór personelu i okresowa kontrola (P)	—		—	Dział kadr
5	Dobra atmosfera w pracy (P)	—		—	—

TABLICA II (12)

Analiza zagrożeń i plan zabezpieczeń

Rodzaj zagrożenia	Prawdopodobieństwo zagrożenia średnie	Przewidywane skutki	Podział kosztów i odpowiedzialności
12. Kradzież danych (przez personel lub osoby obce)		Zakłócenie pracy Koszt: nieznaczny	A — w koszty budowy B — w koszty komputera C — z budżetu służby ochrony

Lp.	Środki ochrony	Komentarz i decyzje	Zalecenia dodatkowe	Podział kosztów	Odpowiedzialność
1	Ograniczony dostęp do archiwów (P)	Zakaz wstępu do archiwów (z wyjątkiem bibliotekarza)		—	Dział APD
2	Zabezpieczenie zbiorów (P)	Stosowanie kluczy do zbiorów wrażliwych		—	Wydział systemów operacyjnych
3	Niszczenie makulatury (P)	Zakupić „wilki" do makulatury		C	Dział administracyjny
4	Godne zaufania sprzątaczki (P)	—		—	Dział kadr
5	Ubezpieczenie (L)	Wstawiono do polisy ubezpieczeniowej		B	Dział APD

TABLICA II (13)

Analiza zagrożeń i plan zabezpieczeń

Rodzaj zagrożenia	Prawdopodobieństwo zagrożenia znikome	Przewidywane skutki	Podział kosztów i odpowiedzialności
13. Błędy wprowadzone celowo do oprogramowania		Przerwy w pracy Koszt: może przekroczyć 10 tys. dol.	A — w koszty budowy B — w koszty komputera C — z budżetu służby ochrony

Lp.	Środki ochrony	Komentarz i decyzje	Zalecenia dodatkowe	Podział kosztów	Odpowiedzialność
1	Klucze do zbiorów programów (P)	—		—	Wydział systemów operacyjnych
2	Ograniczenie dostępu do taśm z programami (P)	Zakaz wstępu do archiwum i biblioteki nośników		—	Dział APD
3	Rotacja programistów (P)	—		—	Kierownictwo zespołów

TABLICA II (14)

Analiza zagrożeń i plan zabezpieczeń

Rodzaj zagrożenia	Prawdopodobieństwo zagrożenia duże	Przewidywane skutki	Podział kosztów i odpowiedzialności
14. Awarie linii transmisji danych		Część instalacji: przerwy w pracy Koszt: poniżej 10 tys. dol.	A — w koszty budowy B — w koszty komputera C — z budżetu służby ochrony

Lp.	Środki ochrony	Komentarz i decyzje	Zalecenia dodatkowe	Podział kosztów	Odpowiedzialność
1	Sprawdzić łącza zewnętrzne (P)	Zostanie uzgodnione z UPTiT		—	Wydział techniczny
2	Wyeliminować ewentualne źródła zakłóceń (P)	Zostanie uzgodnione z UPTiT		—	Wydział techniczny
3	Sprawdzić łącza wewnątrz budynku (P)	Wejście linii bezpośrednio do sali komputera		—	Wydział techniczny
4	Połączenia okrężne (L)	Należy wyjaśnić szczegóły		C	Wydział techniczny

3. Dla każdego rodzaju zagrożenia — z uwzględnieniem rodzaju zagrożonych obiektów oraz rozmiarów skutków (strat) — sporządzić plan zabezpieczenia w podziale na dwie kategorie kroków zabezpieczających:

a) kroki prewencyjne,

b) kroki do podjęcia w przypadku wystąpienia zagrożenia.

4. Ustalić osoby (stanowiska) odpowiedzialne za podjęcie poszczególnych kroków oraz sposób pokrycia kosztów, związanych z odpowiednimi pozycjami planu.

Sporządzając plan zabezpieczenia zgodnie z p. 3, należy uwzględnić istniejącą sytuację. W szczególności chodzi o to, czy jest to całkowicie nowy projekt, czy też ma być zbadana i poprawiona sytuacja w funkcjonującym już ośrodku APD.

W tablicach II(1)—II(14) pokazano przykład analizy przeprowadzonej przy założeniu, że dany ośrodek — zlokalizowany w budynku o konstrukcji żelbetowej, gotowy w stanie surowym — ulega rozbudowie (podwojeniu). Lokalizacja ośrodka APD: parter i pierwsze piętro. Działalność ośrodka nie zostaje przerwana; należy zapewnić możliwie najswobodniejszy dostęp osobom upoważnionym, nie dopuszczając osób niepowołanych.

3. Problemy zabezpieczenia istniejącego i funkcjonującego ośrodka APD

Przystępując do wprowadzania w życie zasad ochrony informacji i środowiska jej przetwarzania w istniejącym już ośrodku obliczeniowym, należy zacząć od podjęcia pewnych natychmiastowych kroków zabezpieczających. Nie wymagają one praktycznie żadnych nakładów finansowych, a ich wprowadzenie pozwoli na względnie spokojne opracowanie bardziej szczegółowego planu poczynań zabezpieczających, przeszkolenie personelu, opracowanie zabezpieczeń logicznych (programowych) i podjęcie poważniejszych kroków, często wiążących się z pewnymi kosztami.

Wykaz takich natychmiastowych działań, w podziale na osobowe, fizyczne i proceduralne, może mieć postać następującą [4]:

OSOBOWE

1. Wyznaczyć kogoś do opracowania, a następnie nadzorowania realizacji programu ochrony.

2. Przeszkolić właściwy personel w zwalczaniu ognia.

3. Spowodować, aby wszystkie nośniki danych znalazły się pod opieką personelu biblioteki.

4. Sporządzić listę osób upoważnionych do przekraczania progu pomieszczenia komputera i biblioteki (lista ta powinna zawierać możliwie najmniejszą liczbę osób, wynikającą z potrzeb eksploatacji).

5. Zapewnić, aby żadni goście (nie wyłączając członków kierownictwa, ekip konserwujących itp.) nie byli wpuszczani do sali komputera czy biblioteki bez towarzyszącej osoby spośród upoważnionego personelu operacyjnego. Eliminować i ograniczać zwiedzanie do niezbędnego minimum.

6. Wprowadzić (i egzekwować) obowiązek rejestrowania przyjścia i wyjścia wszystkich osób odwiedzających pomieszczenie komputera.

FIZYCZNE

7. Zaryglować wszystkie okna i wszystkie drzwi zewnętrzne (z wyjątkiem dwojga), prowadzące do pomieszczeń komputera.

8. Usunąć wszystkie zewnętrzne znaki wskazujące drogę do ośrodka komputerowego.

9. Poddać badaniu działanie wszystkich gaśnic (najlepiej, żeby wykonał to dostawca).

10. Usunąć z pomieszczenia komputera wszelkie składy kart perforowanych, taśm, wydruków itp. Przekazywać wszystkie wykorzystane już dyski, taśmy itp. natychmiast do biblioteki i zatrzymywać w sali komputera tylko te, które są niezbędne w danej chwili do sprawnej eksploatacji.

11. Sporządzić wtórniki programów, dokumentacji oraz oprogramowania systemowego i magazynować w oddalonym terenowo składzie.

12. Wywiesić alarmowe numery telefonów itp.

13. Sprawdzić postępowanie awaryjne przez ogłoszenie próbnych alarmów pożarowych lub awaryjnych.

14. Egzekwować surowo i często wyrywkowo kontrolować przestrzeganie obowiązujących przepisów.
15. Wprowadzić zasadę „zamkniętego obszaru pracy".
16. Zabronić palenia, jedzenia i picia w sali komputera.
17. Wprowadzić i egzekwować zasadę sporządzania i bezpiecznego przechowywania awaryjnych kopii zbiorów danych.
18. Zabronić wstępu do biblioteki osobom nie należącym do personelu bibliotecznego.
19. Wprowadzić i egzekwować procedurę formalnego upoważnienia do pobierania materiałów z biblioteki.
20. Zapewnić, aby zawsze w sali komputera były obecne co najmniej dwie osoby.
21. Zabronić wnoszenia teczek i dużych toreb do sali komputera i biblioteki.
22. Wprowadzić i egzekwować zasadę regularnego sprawdzania dziennika konsolowego przez personel spoza eksploatacji.

4. Stanowisko do spraw ochrony informacji

Jak już wspomniano, jest to stanowisko na najwyższym szczeblu zarządzania w organizacji (instytucji lub przedsiębiorstwie), wiążące się z bezpośrednią odpowiedzialnością za wszystkie elementy ochrony informacji i środowiska jej przetwarzania. Jeśli nie sprawuje tej funkcji wicedyrektor (zastępca dyrektora), to powinien to być wykwalifikowany specjalista, podlegający bezpośrednio dyrektorowi naczelnemu. Specjalista ten powinien dysponować następującymi kwalifikacjami:

1. Umiejętność kierowania ludźmi.
2. Znajomość fizycznych, logicznych i organizacyjnych zasad ochrony.
3. Znajomość systemu (*software i hardware*) dostateczna dla codziennej działalności nadzorczej i audytorskiej w odniesieniu do bieżącej eksploatacji systemu i urządzeń.
4. Umiejętność dokonywania selekcji personelu z punktu widzenia bezpieczeństwa informacji.
5. Biegłość w posługiwaniu się specjalnymi procedurami, charakterystycznymi dla konkretnego ośrodka APD.

6. Znajomość przepisów dotyczących organizacji ochrony tajemnicy państwowej i służbowej.

Specjalista do spraw ochrony informacji sprawuje funkcje doradcze i nadzorcze, a jeśli jest członkiem dyrekcji — również wykonawcze.

Przykładowy zakres obowiązków SOI

1. Uczestniczy w pracach komisji standardów i odbioru dokumentacji z głosem decydującym w sprawach ochrony informacji i środowiska jej przetwarzania.

2. Planuje i organizuje działalność prewencyjną w zakresie ochrony informacji i operatywnie nadzoruje realizację wszelkich poczynań w tym kierunku.

3. Organizuje i prowadzi działalność szkoleniową w zakresie ochrony informacji.

4. Współpracuje z kierownictwem innych ośrodków obliczeniowych w zakresie prewencji ogólnej i wymiany doświadczeń z zakresu ochrony informacji i środowiska jej przetwarzania.

5. Współpracuje z dostawcami sprzętu i oprogramowania oraz z użytkownikami podobnych komputerów w dziedzinie wymiany doświadczeń z zakresu ochrony informacji i środowiska jej przetwarzania, a także wzajemnej pomocy w sytuacjach awaryjnych.

6. Koordynuje działalność administracyjno-budżetową w aspekcie ochrony fizycznej i zabezpieczenia przed pożarem pomieszczeń ośrodka APD.

7. Inicjuje i koordynuje prace nad doskonaleniem metod i techniki ochrony informacji.

8. Inicjuje i nadzoruje próbne alarmy i ćwiczenia, mające na celu utrzymanie i kontrolę gotowości w zakresie ochrony informacji i środowiska jej przetwarzania.

9. Prowadzi działalność doradczą z zakresu zagadnień ochrony informacji i środowiska jej przetwarzania.

10. Prowadzi rejestr i kontrolę wydawanych zezwoleń wstępu, identyfikatorów, haseł, kodów, kluczy itp.

11. Czuwa nad przestrzeganiem obowiązujących przepisów o ochronie tajemnicy państwowej i służbowej.

III. Przegląd potencjalnych zagrożeń

1. Podstawowe pojęcia i definicje

Ochrona informacji i środowiska jej przetwarzania wiąże się — jak powiedziano — ze sprawdzeniem wszystkich możliwych źródeł zagrożenia — zadaniem bardzo odpowiedzialnym, ale realnym do wykonania.

Jednym z czynników, które utrudniają realizację tego zadania jest na ogół brak świadomości ze strony kierownictwa, jak ważne jest to zagadnienie. Systemy APD stanowią ciągle jeszcze taką nowość, że niewielu członków kadry kierowniczej może się pochwalić bogatszym doświadczeniem w tej dziedzinie. Pociąga to za sobą czasem takie podejście, że eliminuje się np. w przedsiębiorstwie wprowadzającym systemy APD nawet niektóre istniejące dotychczas techniki kontroli obliczeń dokonywanych przez ludzi, wychodząc z założenia, że „komputer się nie myli". Jednakże komputer jest programowany i eksploatowany przez omylnych przecież ludzi.

Aż nazbyt często również kierownictwo ośrodka APD przywiązuje większą wagę do sprawnej i niezawodnej działalności instalacji komputerowej, niż do jej bezpieczeństwa. Uwidacznia się to szczególnie wyraziście w treści instrukcji technologicznych. norm itp.

Należy pamiętać, że wartość informacji w różnych punktach procesu przetwarzania jest bardzo różna. Dlatego też — jakkolwiek największe zagrożenie występuje tam, gdzie jest najsłabsze zabezpieczenie — miejsce takie nie musi wcale stanowić zarazem „najwrażliwszego" punktu obiegu. Z reguły np. wartość informacji przetworzonej (na wyjściu systemu), a także jej wrażliwość, są

znacznie większe niż wartość i wrażliwość (poufność) danych źródłowych wchodzących do systemu.

Zanim przystąpi się do bardziej szczegółowej analizy niefortunnych wydarzeń, jakie mogą zagrozić ośrodkowi APD, trzeba spróbować dokonać pewnej klasyfikacji i zdefiniować określenia, jakimi będzie się operować w dalszej treści tej książki.

Wymienionych w pierwszym rozdziale sześć podstawowych szkód (zamierzonych i przypadkowych) może zagrozić następującym elementom składowym systemu komputerowego:

— sprzętowi (*hardware*),
— oprogramowaniu,
— danym (nośnikom),
— urządzeniom transmisyjnym,
— środowisku (otoczeniu),
— strukturze organizacyjnej,
— zapleczu.

Przez *hardware* należy rozumieć wszelkie urządzenia konieczne do realizowania procesów obliczeniowych i przetwarzania, ale z wyłączeniem urządzeń do transmisji danych oraz do kontroli środowiska.

Do *oprogramowania* należą wszystkie niezbędne systemowi programy, włączając *software podstawowy* (system operacyjny), programy użytkowe, programy usługowe i pomocnicze, programy sprawdzające (testowe) itp.

Dane i *nośniki* — wszelkie dane wprowadzane do systemu, przechowywane w systemie, przetwarzane przez system i wychodzące z systemu wraz z nośnikami (karty, taśmy magnetyczne), na których się znajdują.

Urządzenia transmisyjne — wszystko, co służy do przesyłania danych, informacji oraz programów do komputera i z komputera, a więc modemy, linie kablowe, łącza radiowe, końcówki terminalowe itp.

Środowisko — wszystkie elementy związane z regulacją i sterowaniem otoczeniem, w którym znajduje się system komputerowy, takie jak: klimatyzacja, instalacja przeciwpożarowa sygnalizacyjna i gaśnicza, fizyczne środki kontroli dostępu itp.

Struktura organizacyjna — jest to struktura wprowadzona w związku z eksploatacją systemu komputerowego. Należą do niej

ludzie, schemat obowiązków i odpowiedzialności, procedury standardowe itp.

Zaplecze obejmuje wszystkie środki, które zasilają lub obsługują system komputerowy na zasadzie zlecenia lub kooperacji. Należą tu: zasilanie energią i wodą, konserwacja sprzętu, utrzymanie czystości, zapewnienie transportu itp.

Analizę różnych typów zagrożeń, na jakie narażony jest ośrodek APD, można zacząć od podkreślanego już ich podziału na dwie kategorie: szkody będące dziełem przypadku i szkody wywołane rozmyślnie. To rozróżnienie jest ważne. Zabezpieczenie ośrodka przed szkodami przypadkowymi może być na ogół uzyskane środkami statycznymi i często wystarczy jedna skuteczna bariera. Inaczej sprawa wygląda ze szkodami umyślnymi: z definicji wynika, że sprawca jest zdecydowany zwalczać przeszkody na swej drodze, jedną po drugiej. Powstrzyma go dopiero nadmiar trudności, wysoki koszt lub brak czasu.

2. Zagrożenia wywołane umyślnie

Zagrożenia wywołane celowo można rozpatrywać w dwóch grupach:

1. Akcje sabotażowe, których jedynym celem jest wyrządzenie szkody, niezależnie od motywów (należą tu również wyczyny „sportowe" młodych, zdolnych programistów).
2. Oszustwo lub kradzież, gdzie celem jest osiągnięcie jakiegoś zysku przez sprawcę lub zespół, do którego ten sprawca należy.

A k c j e s a b o t a ż o w e stanowią poważny problem w zagadnieniach ochrony ze względu na ich bezwzględność i pozorną irracjonalność. Działania oszukańcze są w jakiś sposób mitygowane przez obawę „wpadki".

Sabotowanie przez osoby lub grupy z zewnątrz ośrodka ma najczęściej charakter polityczno-radykalny i jest mało prawdopodobne w krajach politycznie ustabilizowanych. Natomiast dość duże zagrożenie może stanowić sabotaż uprawiany przez rozgoryczone osoby, pracujące w zainteresowanej instytucji. Osoby takie mają ułatwione zadanie — łatwy dostęp, znajomość procedur wewnętrznych, a przy tym na ogół nie wzbudzają podejrzeń, co utrudnia

wykrycie szkody i sprawcy, nim będzie za późno. Znane są przypadki zniszczenia ważnych zbiorów. Opisywane są również sytuacje, gdy w programach list płacy znajdowały się ukryte podprogramy, które były automatycznie uruchamiane dopiero po skreśleniu z listy nazwiska lub numeru ewidencyjnego autora — programisty.

K r a d z i e ż. Ośrodki APD mogłyby zasłużyć na nazwę „raju złodziei", ponieważ kradzież pozostaje całkowicie nieujawniona. Jak w każdym przypadku kradzieży informacji, wystarczy tylko wykonać kopię oryginału. Oryginał zaś pozostaje i nie ma na nim żadnych śladów.

Kradzież urządzeń nie wchodzi z reguły w rachubę — z uwagi na ciężar i brak możliwości sprzedaży. Można natomiast — gdy brak dozoru — wynieść np. rolkę taśmy magnetycznej lub pakiet dysków. Są to cenne przedmioty, lecz również niełatwe do sprzedania. W niektórych krajach (szczególnie w Stanach Zjednoczonych) dość rozpowszechniona jest kradzież czasu pracy maszyny. Nie różni się to w sposób zasadniczy od używania telefonu służbowego do rozmów prywatnych — może jednak znacznie drożej kosztować.

W literaturze (m.in. [12]) przytoczone są przykłady: operatorzy komputera należącego do Rady Oświatowej w Chicago zostali oskarżeni w 1970 r. o nielegalne wykorzystywanie czasu komputera dla potrzeb swojego „biura usług obliczeniowych"; system rezerwacji miejsc opracowany przez brytyjskie linie lotnicze BOAC kosztem 100 milionów dolarów omal nie został skradziony w 1968 r. i sprzedany innej linii lotniczej. Na szczęście uczciwa konkurencja powiadomiła BOAC o otrzymanej ofercie. Nie zawsze rzecz kończy się tak szczęśliwie; np. pewien programista angielski skradł w 1971 r. jedyną taśmę zawierającą ważne informacje, wywiózł ją za granicę i zażądał wypłacenia okupu w wysokości 26 000 dol. na numerowane konto w banku szwajcarskim. Zainteresowana firma nie miała innego wyjścia i okup zapłaciła.

Najgroźniejsze w skutkach mogą być jednak kradzieże informacji dokonywane przez obcy wywiad (wojskowy, gospodarczy, przemysłowy).

Celowe (umyślne) wtargnięcie do zasobów informacyjnych może mieć następujące motywacje:

1. Uzyskanie dostępu do informacji w zbiorach.
2. Zapoznanie się z potrzebami i zainteresowaniami użytkowników w zakresie informacji.
3. Dokonanie zmian informacji lub zniszczenie zbiorów.

Można mówić o infiltracji biernej lub aktywnej. Infiltrację bierną można porównać do podsłuchu; polega ona na śledzeniu informacji w pewnym punkcie jej obiegu. Do metod b i e r n e j infiltracji należą:

1. Przechwytywanie elektromagnetyczne (z jednostki centralnej lub peryferyjnych urządzeń wejścia/wyjścia).
2. Dołączenie się do łączy transmisji danych.
3. Ukryte nadajniki (w jednostce centralnej, urządzeniach peryferyjnych lub na łączach transmisyjnych).

Można także wśród tych metod wymienić okresowe przeglądanie zawartości pojemników na makulaturę, znajdujących się w okolicy komputera lub końcówek (terminali).

Metody a k t y w n e:

1. Szperanie.
2. Maskowanie się.
3. Wykrywanie i wykorzystywanie „furtek" w oprogramowaniu systemu.
4. Dołączenie się do aktywnego kanału transmisyjnego.
5. Środki fizyczne.

Szperanie wiąże się z wykorzystaniem legalnego dostępu do systemu w celu uzyskania informacji, do której nie ma się uprawnienia.

Maskowanie się polega na uzyskaniu właściwych kluczy identyfikacyjnych (identyfikatory, hasła itp.) metodami nielegalnymi (np. przez podsłuch) i „podszywanie się" pod uprawnionego użytkownika.

Furtki są to cechy sprzętu lub oprogramowania (czasem są to celowo umieszczane w programie punkty wejścia), które umożliwiają osobie nie upoważnionej dostęp do systemu. Często udaje się wykryć takie furtki przez systematyczne wypróbowywanie różnych kombinacji zmiennych kontrolnych systemu.

Aktywny kanał transmisyjny może zostać nielegalnie wykorzystany przez dołączenie specjalnego terminala i udawanie jednego z legalnych użytkowników.

Środki fizyczne — uzyskanie i analiza wydruków tzw. *core dumps* (zawartość pamięci głównej), kradzież przenośnych nośników magnetycznych.

Generalnie biorąc, intruzów w ośrodkach APD można by podzielić na trzy typy:

1. Intruz przypadkowy: może wejść z ulicy, mając nadzieję, że coś zyska, bez konkretnie zarysowanego planu i celu. Wejdzie, jeśli drzwi nie są zamknięte lub jeśli nie ma przy nich strażnika.

2. Intruz zdecydowany. Ten typ intruza jest gotów do sforsowania drzwi lub okna. Wie czego chce. Na ogół woli nie atakować personelu, ale nie można wykluczyć, że w razie potrzeby zaatakuje. Przypadek rzadki.

3. Intruz podszywający się. Zachowuje się tak, jakby miał uprawnienia do wejścia, wzbudzając pewnością siebie zaufanie; wchodzi otwarcie i spodziewa się życzliwego powitania. Zanotowano m.in. następujący przypadek: zjawił się ktoś, pytając o inżyniera-konserwatora komputera; pogadał z nim na tematy techniczne i poznał jego nazwisko. Następnie dzwonił kilkakrotnie, pytając o tego inżyniera. Gdy dowiedział się, że inżynier wyszedł i już danego dnia nie wróci, zjawił się w pomieszczeniu komputera jako kolega konserwatora, twierdząc, że został przysłany po jakiś sprzęt. Wziął upatrzone taśmy i dyski, usunął z nich etykiety i usiłował wynieść, twierdząc, że są to inżynierskie programy testujące.

O s z u s t w o. Podczas gdy przypadki kradzieży „komputerowej" prędzej czy później wychodzą na jaw, wykrywalność oszustw popełnionych za pomocą komputera jest oceniana przez specjalistów na nie więcej niż 20%. Niemal wszystkie zarejestrowane przypadki oszustw komputerowych wyszły na jaw dopiero wtedy, gdy z jakiegoś powodu trzeba było przejściowo powrócić do tradycyjnego „ręcznego" systemu przetwarzania. Na ogół metody zastosowane w wykrytych przypadkach przestępstw nie okazywały się zbyt pomysłowe — wydawały się wręcz prymitywne osobom znającym dobrze system. Niewątpliwie jedną z przyczyn niskiej wykrywalności tych oszustw jest to, że wdrożone i uruchomione systemy APD są rzadko kontrolowane podczas eksploatacji; taka kontrola zresztą jest bardzo trudna. Natomiast najczęściej wcale

nie jest trudne wprowadzenie „nielegalnej" procedury do już eksploatowanego systemu. Nasuwa się jednak przypuszczenie, że istotną przyczyną niskiej wykrywalności oszustw może być to, że większość przestępców pracuje metodami znacznie bardziej pomysłowymi i ich działalność nie zostaje po prostu ujawniona. Z drugiej strony wiele dokonanych oszustw nigdy nie znajduje odbicia w statystykach, ponieważ rozgłaszanie tego nie jest w interesie poszkodowanych firm.

W istocie, jeśli zastosowane zostaną właściwe środki kontroli, komputer może przyczynić się do znacznego utrudnienia tradycyjnych metod oszustwa. Urzędnicy i księgowi, którzy potrafiliby fałszować księgi, na ogół nie wiedzą, jak fałszować zapisy komputerowe. Gdyby próbowali jakichś nieudolnych metod, komputerowe środki kontroli najprawdopodobniej odkryłyby to natychmiast.

Szczególnie krytyczna jest faza testowania i wdrażania nowo zaprojektowanego systemu APD. W tym właśnie okresie mogą mieć miejsce np. próby wprowadzenia nielegalnych (nie zatwierdzonych) programów lub fikcyjnych kont. Jest to szczególnie ułatwione ze względu na towarzyszący na ogół działaniom w tej fazie pośpiech, wprowadzane ad hoc zmiany i modyfikacje oraz fakt, że mało jest jeszcze wówczas osób, które znają szczegóły systemu; większość zainteresowanych nie wie zbyt dokładnie, jak pracują procedury sprawdzające, a personel eksploatacji (operatorzy) nie zna jeszcze szczegółowo działania danego systemu. Dlatego może czasem okazać się celowe wprowadzenie w tym okresie specjalnych procedur kontrolnych i specjalnych raportów przebiegu procesu *(transaction reporting)*. Procedury te mogą okazać się zbędne i zostać zaniechane po wdrożeniu i uruchomieniu normalnej eksploatacji.

3. Zagrożenia przypadkowe

Kradzież i oszustwa komputerowe, podobnie jak akty sabotażu, uzyskują rozgłos. A jednak szkody spowodowane przez przypadek są znacznie liczniejsze, a mogą być równie — a czasem bardziej — dotkliwe. Należą tu zarówno milionowe szkody spowodowane poża-

rami, jak i niewielkie uszkodzenia zbiorów, wywołane wprowadzeniem niedokładnych (lub błędnych) danych.

Nie istnieją instalacje całkowicie zabezpieczone przed ogniem. Oczywiście wielkość szkód jest na ogół proporcjonalna do rozmiarów pożaru; należy jednak podkreślić, że czasem niewielki nawet pożar może pośrednio wywołać katastrofalne skutki — jeśli np. instalacja komputerowa steruje procesami w dużym zakładzie produkcyjnym (np. w rafinerii) lub też bieżąca działalność instytucji zależy od pracy komputera w czasie rzeczywistym (np. rezerwacja miejsc w ruchu lotniczym).

Przypadkowe ujawnienie informacji lub uszkodzenie zbiorów może być wynikiem wad lub uszkodzenia sprzętu, może też być spowodowane błędami oprogramowania wynikającymi z niepełnego przetestowania i skorygowania programów lub z błędnej ich logiki; wreszcie zaistnieć może taki błąd operatora, jak założenie niewłaściwej szpuli taśmy magnetycznej lub pakietu dyskowego.

Wśród innych szkód przypadkowych można np. wymienić: uderzenie pioruna, powódź, awaria urządzenia itp. Podczas gdy wszystkie zagrożenia umyślne związane są z działaniem ludzi — wiele zagrożeń przypadkowych występuje bez udziału człowieka. Te w których człowiek ma swój udział, spowodowane są najczęściej pomyłkami i zaniedbaniami w rozwiązaniu projektowym, konstrukcji, instalacji, eksploatacji, konserwacji lub modyfikacji jakiejś części składowej systemu komputerowego. Niestety, tego rodzaju zagrożenia przypadkowe, choć nie tak „efektowne" jak rozmyślne, występują znacznie częściej i powodują wcale nie mniejsze straty.

Jest rzeczą oczywistą, że ogromną rolę w zapobieganiu takim szkodom odgrywa gruntowne szkolenie konstruktorów, projektantów, programistów i operatorów, a następnie stworzenie właściwej atmosfery pracy i właściwa motywacja pracowników.

Zagrożenie pożarem

Ogień należy do poważnych zagrożeń w ośrodku APD z kilku powodów:

a) w pomieszczeniu komputera jest zazwyczaj wiele materiałów łatwo palnych, takich jak papier, karty dziurkowane, taśmy dziurkowane, pudła kartonowe,

b) pożar urządzeń elektronicznych jest często trudny do opanowania, ponieważ niektóre podzespoły, uzwojenia, taśmy magnetyczne wydzielają, paląc się, gęste trujące dymy, które zmuszają ludzi do wycofania się,

c) w celu niezbędnego ograniczenia dostępu większość sal komputerowych ma jedno, najwyżej dwa wyjścia; przy gęstym zadymieniu stanowi to duże utrudnienie ewakuacji personelu,

d) systemy zwalczania ognia same bywają źródłem zagrożenia: woda uszkadza urządzenia elektroniczne, a środki chemiczne mogą powodować zatrucie personelu,

e) ogień może być przyczyną całkowitego zniszczenia zbiorów danych, programów i dokumentacji; może to pociągnąć za sobą nieobliczalne następstwa,

f) wszystkie obecne komputery wymagają klimatyzacji; same urządzenia klimatyzacyjne bywają niekiedy źródłem pożaru; przewody wentylacyjne mogą pośredniczyć w przenoszeniu ognia, dymu, a nawet wody,

g) pomieszczenia komputera mają zazwyczaj podniesione podłogi i podwieszone stropy; ogień tam zaprószony może swobodnie rozprzestrzeniać się przez pewien czas, zanim zostanie zauważony,

h) instalacje elektryczne (zasilające), a zwłaszcza wyłączniki, są częstym źródłem iskier; izolacja kabli, nawet jeśli w zasadzie niepalna, wydziela przy podgrzewaniu trujące i powodujące korozję dymy.

Kierownictwo większości ośrodków zdaje sobie z tego sprawę i nie żałuje środków na dobre zabezpieczenie przeciwpożarowe pomieszczeń. Efekt jest taki, że zniszczenia i szkody powodowane są obecnie częściej przez pożary zaistniałe w pomieszczeniach i budynkach przylegających do ośrodka. Nasuwa to logiczny wniosek, że nie zaniedbując dobrze przemyślanego systemu ochrony przeciwpożarowej na terenie ośrodka APD, należy dobrze przeanalizować lokalizację tego ośrodka w stosunku do innych obiektów, a w razie potrzeby wprowadzić odpowiednie zabezpieczenia konstrukcyjne (ściany ogniotrwałe) wokół ośrodka.

W zasadzie ośrodki obliczeniowe powinny mieścić się w oddzielnych, ognioodpornych budynkach, ale ponieważ zwykle nie jest to możliwe, dane pomieszczenie (lub pomieszczenia) powinno mieć niepalną konstrukcję.

Wskazane jest nawiązanie kontaktu z miejscową strażą pożarną (zanim zaistnieje „okazja" alarmowa po temu). Przedstawiciele straży powinni być w pełni świadomi wrażliwości systemu, aby prowadząc akcję ratowniczą umieli ograniczyć dostęp wody i dymu do wrażliwych urządzeń. Ponadto strażacy zazwyczaj mogą udzielić bardzo cennych rad co do kroków, jakie należy podjąć, aby zmniejszyć groźbę pożaru.

Urządzenia komputerowe wrażliwe są nie tylko na ogień, ale także na dym i ogólnie wzrost temperatury.

Dym, szczególnie utworzony z ciężkich czarnych cząstek koloidalnych, może być bardzo szkodliwy dla urządzeń i powoduje konieczność długotrwałych i kosztownych operacji czyszczenia. Dym ten najczęściej pochodzi z zewnątrz ośrodka obliczeniowego i często przedostaje się przez otwory nawiewowe urządzeń klimatyzacyjnych. Możliwość istnienia takiego niebezpieczeństwa należy przeanalizować i zastosować odpowiednie kroki zapobiegawcze (np. klapy dymowe w instalacji klimatyzacyjnej).

Wielu szkód można uniknąć stosując dopasowane osłony plastykowe na urządzenia, tanie i łatwe do wykonania. Należy je dokładnie poznaczyć i przechowywać w sposób łatwo dostępny, tak aby można je było szybko założyć w warunkach napięcia nerwowego. Osłony te stanowią jednocześnie doskonałą ochronę przed szkodami wodnymi, powstającymi podczas gaszenia pożarów lub z innych przyczyn.

Wpływ temperatury na nośniki magnetyczne

Należy wyjaśnić często spotykane nieporozumienie: nie istnieje jakaś dokładna wartość temperatury otoczenia (najczęściej podawana: 150°F, czyli ok. 65°C), powyżej której nośniki magnetyczne ulegają zniszczeniu, a poniżej której są bezpieczne. Krytyczne warunki temperaturowe zależą od wilgotności względnej. Nawet niezbyt znaczne podniesienie temperatury przy zbyt dużej wilgotności może spowodować poważne szkody w nośnikach magnetycznych, podczas gdy, przeciwnie, przy niewielkiej wilgotności nawet stosunkowo wysoka temperatura może nie spowodować poważniejszych uszkodzeń. Do około 50÷55°C, przy normalnych dla ośrodków APD warunkach wilgotności, nie ma problemów. Przy wyż-

szych temperaturach zostało stwierdzone częstsze występowanie błędów odczytu. Powyżej 65°C zaczyna się energiczniejszy rozkład termiczny nośników.

Nośniki magnetyczne są również wrażliwe na niskie temperatury. Znane są np. przypadki kłopotów z odczytem danych z pakietu dyskowego, pozostawionego w mroźny dzień na pewien czas w bagażniku samochodu.

Szkody wodne

Woda przynosząca szkody ośrodkom APD może pochodzić z różnych źródeł. Najgroźniejsze szkody, jakie dotychczas zanotowano, zostały spowodowane przez tropikalne burze i huragany. W wyniku działania huraganu Agnes setki ośrodków obliczeniowych na środkowoatlantyckim wybrzeżu Stanów Zjednoczonych zostało zalanych tonami wody i błota. W roku 1970 huragan Celia wyrządził ogromne szkody użytkownikom komputerów w Teksasie. Oprócz huraganowych, notowano szkody spowodowane przez powodzie, działania straży ogniowej na wyższych piętrach, pęknięte rury, zraszacze przeciwpożarowe zainstalowane w hali komputera, „cofkę" wód opadowych z kanalizacji, wody podskórne, a nawet przecieki wody z instalacji klimatyzacyjnej. W przypadku wielu pożarów szkody wyrządzone przez wodę przekraczały szkody spowodowane ogniem.

4. Radiacja, obce pola elektromagnetyczne

Należy tu rozpatrzyć dwa rodzaje problemów.

I. Wrażliwość sprzętu komputera na generowane z zewnątrz silne pola elektromagnetyczne. Znane są przypadki, gdy sygnały radarowe zakłóciły chwilowo pracę komputera znajdującego się bezpośrednio w polu działania potężnego nadajnika, bez przesłaniających drogę sygnału budynków (np. w pobliżu lotniska lub portu morskiego). Są to oczywiście przypadki rzadkie. Na ogół jeśli natężenie pola otaczającego komputer nie przekracza wartości 1 V/m, większość systemów pracuje bez żadnych problemów. Przy wartościach natężenia pola w granicach 1÷5 V/m wpływ pola jest jeszcze pomijalny. Dopiero przy wartości otaczającego pola prze-

kraczającej 5 V/m mogą wystąpić istotne trudności. W większości przypadków wystarczy jednak ekranowanie instalacji uziemioną siatką metalową.

Spotykane w prasie doniesienia, że ze specjalnie wyposażonej ciężarówki ustawionej na ulicy przed budynkiem komputera można działać silnym polem magnetycznym, które spowoduje wymazanie zapisów na taśmach i dyskach, są wyssane z palca. W najgorszym razie tak rzucające się w oczy i kosztowne urządzenie mogłoby wywołać sporadyczne błędy procesora lub pamięci operacyjnej. które to błędy zostaną automatycznie wykryte. Byłaby to więc całkowicie nieopłacalna zabawa.

Ze strony sprzętu rentgenowskiego i radarowego nie istnieje niebezpieczeństwo zniszczenia danych na żadnym z nośników pamięci. Źródła te mogą spowodować zniszczenie w wyniku efektów cieplnych, wywołanych na nośniku poddanym bezpośredniemu działaniu promieniowania wysyłanego przez ten sprzęt.

Należy jeszcze poświęcić nieco uwagi wpływowi pól magnetycznych wytwarzanych przez elektromagnesy i magnesy stałe. Pola magnetyczne wytwarzane przez urządzenia zasilane prądem zmiennym, takie jak froterki, silniki elektryczne, telewizory itd. nie stanowią niebezpieczeństwa dla taśm magnetycznych, jeżeli ich użycie jest zgodne z zasadami ich eksploatacji. Z uwagi na to należy przeprowadzać okresowe badania wszelkiego sprzętu, sprowadzanego do ośrodka komputerowego, w celu stwierdzenia czy ekranowanie tych urządzeń spełnia swoje zadanie.

Bardziej szkodliwe efekty mogą być wywoływane w samym momencie włączania froterki lub odkurzacza, gdyż generowane są wtedy ogromne szumy.

Ważnym parametrem nośników magnetycznych jest ich *koercyjność*. Wielkość ta jest wyrażana w jednostkach zwanych erstedami. Koercyjność decyduje o trwałości zapisu na taśmie magnetycznej. Koercyjność typowej taśmy komputerowej zawiera się w zakresie 250÷300 erstedów. Taśma o koercyjności 250 erstedów może być skasowana przez pole magnetyczne np. o natężeniu 800 erstedów. Jeżeli magnes wytwarzający pole o natężeniu 100 erstedów zostanie przyłożony do tej taśmy, to zapis na niej nie zostanie skasowany, jakkolwiek w tle pojawi się szum. Dopóki nie odbywa się kasowanie, nie ma znaczenia, czy magnes znajduje się w pobliżu

taśmy przez minutę czy przez tydzień. Będzie natomiast stopniowo wzrastał szum, który jednak ma znaczenie tylko w przypadku taśm z zapisem typu akustycznego (analogowego), a nie jest istotny w przypadku stosowanego w przetwarzaniu danych zapisu cyfrowego.

Zapis na dysku może zostać skasowany przez umieszczenie na nim cienkiej folii plastykowej i przesunięcie bezpośrednio nad powierzchnią dysku magnesu wytwarzającego natężenie pola 1500 erstedów.

Czy osoba zwiedzająca (lub pracownik) może, przechadzając się w ośrodku komputerowym parę metrów od nośnika magnetycznego z ukrytym magnesem, spowodować jakiekolwiek uszkodzenie? Zdecydowanie nie! Nie z odległości paru metrów. Odległość jest naszym największym sprzymierzeńcem. Natężenie pola magnetycznego maleje proporcjonalnie do sześcianu odległości od źródła tego pola.

Natężenie pola mierzone np. na osi prostopadłej do odcinka łączącego bieguny dipola magnetycznego utworzonego przez magnes podkowiasty wynosi na poziomie biegunów 800 erstedów: w odległości 50 mm — 100 erstedów, a w odległości 100 mm spada do 12 erstedów.

II. Przechwytywanie emitowanych przez sprzęt sygnałów elektromagnetycznych. Jest faktem, że urządzenia elektryczne emitują energię elektromagnetyczną. Z punktu widzenia ochrony danych jest to problem, którego znaczenie było dotychczas niewielkie, i najprawdopodobniej nie będzie rosło. Coraz powszechniejsze stosowanie układów scalonych wielkiej skali integracji (LSI) i mikroelektroniki prowadzi do tego, że sprzęt komputerowy wprawdzie w pewnym zakresie staje się bardziej czuły na otaczające pole elektromagnetyczne, ale jednocześnie nowoczesne układy promieniują coraz mniej energii na zewnątrz. Jeżeli weźmie się pod uwagę, że we współczesnych komputerach wieloprogramowych i wieloprocesorowych słabe i tak sygnały zachodzących równolegle procesów interferują ze sobą i częściowo znoszą się — staje się rzeczą jasną, że jedynie w ośrodkach przetwarzających informacje szczególnie wrażliwe warto zadawać sobie trud mierzenia wartości generowanych sygnałów i przedsiębrać odpowiednie do sytuacji środki zabezpieczające — ekranowanie urządzeń itp.

Osobnym zagadnieniem jest sprawa ochrony łączy transmisyjnych i końcówek zdalnego dostępu, o czym będzie szerzej mowa w rozdziale piątym.

5. Zagrożenia szczątkowe

Każdy ośrodek obliczeniowy podlega pewnym zagrożeniom, przed którymi praktycznie nie można się zabezpieczyć. W przypadku każdej zainstalowanej maszyny mogą one być inne; chodzi o to, aby uznawać ich istnienie i uwzględniać ewentualny wpływ przy różnego rodzaju decyzjach. Jeśli stwierdzi się np., że określone zagrożenie jest możliwe, lecz wielce mało prawdopodobne, lub też koszty niezbędne dla zabezpieczenia się przed tym zagrożeniem są niewspółmiernie duże, można świadomie zrezygnować z kroków zabezpieczających. Słowem kluczowym jest tu: „świadomie". Chodzi o to, aby pozostała świadomość, że przed tym właśnie zagrożeniem nie jesteśmy wcale chronieni. Takie zagrożenia zostały nazwane „szczątkowymi".

IV. Przegląd środków i metod zabezpieczania

1. Zasady ogólne wyboru środków i klasyfikacja metod zabezpieczenia

Jak wynika z dotychczasowych rozważań, skuteczność systemu zabezpieczeń w ogromnej mierze zależy od konkretnych — zwykle bardzo różnych — okoliczności. Istnieje jednak cały szereg zasad ogólnych, przydatnych w każdych okolicznościach. Oto najważniejsze spośród nich:

1. Kroki zabezpieczające należy podejmować w taki sposób, aby każda szkoda (strata) mogła zostać natychmiast spostrzeżona.

2. Pierwszym naruszeniem zasad bezpieczeństwa jest sam fakt rozpowszechnienia się wiadomości o istnieniu czegoś, co ma wystarczająco dużą wartość, aby to chronić.

3. Za ochronę informacji odpowiada jej posiadacz lub strażnik.

4. Najlepiej zabezpieczy każde dobro jego posiadacz — zabezpieczenie jest tym efektywniejsze, im większe bezpośrednie zainteresowanie osobiste.

5. Środki zabezpieczające powinny być proporcjonalne do zagrożenia; nie należy ochraniać rzeczy, którym nic nie zagraża.

6. Skupienie ryzyka w jednym miejscu zwiększa wprawdzie niebezpieczeństwo, ale obniża koszt zabezpieczenia.

7. Każda z zainteresowanych osób powinna dysponować informacjami i swobodnym dostępem tylko w takim stopniu, w jakim jest to niezbędne do wykonywania powierzonych jej zadań.

8. Sprawy bezpieczeństwa muszą mieć odpowiedni prestiż i zrozumienie.

9. Jedno zabezpieczenie nie stanowi jeszcze ochrony; zabezpie-

czenie „w głąb" jest sumą możliwych i celowych środków bezpieczeństwa.

10. Każdy ze środków zabezpieczenia sam również wymaga ochrony.

11. System zabezpieczeń jest tak pewny, jak jego najsłabsze ogniwo.

12. Wszystkie systemy, mające na celu ochronę przed rozmyślnym naruszeniem, powinny cechować się elementem zaskoczenia ewentualnego intruza.

13. Jakość środków zabezpieczenia jest ważniejsza od ich liczby.

14. Pełne zabezpieczenie wymaga współpracy strony trzeciej — np. instytucji posiadającej podobny zestaw komputerowy lub towarzystwa ubezpieczeniowego.

15. Trudniej jest naruszyć przepisy bezpieczeństwa, kiedy nie da się uniknąć wspólnika; dlatego warto zadbać o to, aby znajomość sekretu była podzielona (jedna osoba zna część, druga — resztę).

16. Dobry system zabezpieczenia powinien umożliwiać zawężenie odpowiedzialności za szkody do jednej lub dwóch osób.

17. Dbałość o bezpieczeństwo stanowi nierozdzielną część obowiązków każdego pracownika; nie powinien on jednak odpowiadać za bezpieczeństwo spraw, którymi bezpośrednio nie zajmuje się.

18. Ostatnia „bariera ochronna" powinna być najsilniejsza, ale najbardziej skuteczne jest to ostrzeżenie, które wystąpi najwcześniej.

19. Skuteczność „barier" ochronnych można mierzyć czasem, potrzebnym do ich przełamania — im dłuższy czas, tym większa szansa odkrycia w porę intruza.

20. Osoby nie upoważnione nie powinny mieć okazji do rozglądania się po strzeżonych pomieszczeniach.

Przegląd środków i metod zabezpieczenia należałoby rozpocząć od ich podziału na:

— fizyczne,
— logiczne,
— organizacyjne.

Zabezpieczenie fizyczne obejmuje sprzęt, personel, programy, archiwa i dokumentację. Szczególnie wymagające zabezpieczenia są urządzenia komputerowe, ponieważ stanowią ogromną koncen-

trację majątku w postaci zarówno sprzętu, jak i danych oraz informacji.

Przez *zabezpieczenie logiczne* należy rozumieć wszystkie środki ochrony wbudowane logicznie do systemu operacyjnego oraz do programów zastosowań.

Przez *zabezpieczenie organizacyjne* rozumie się wszystkie poczynania organizacyjne ukierunkowane na zmniejszenie ryzyka i na zawężenie odpowiedzialności za powstające w wyniku zagrożenia szkody.

Idea skutecznego systemu zabezpieczeń wymaga, aby każdemu z potencjalnych zagrożeń, omówionych w rozdziale trzecim, przeciwstawić jedną lub więcej metod ochrony albo procedur eksploatacyjnych. Jest warunkiem koniecznym, aby funkcja ochrony została integralnie wbudowana do szeroko pojętego systemu APD, a nie była „dorabiana" ad hoc, kiedy kierownictwo wpada w panikę.

Wśród zasadniczych czynników, wpływających na strukturę systemu zabezpieczeń, można wymienić:

— zawartość informacyjną,
— środowisko,
— łączność,
— zakres funkcjonalny systemu.

Zawartość informacyjna decyduje o wrażliwości programów i danych, w zależności od której można wybrać jedno z trzech rozwiązań:

a) ogólną dostępność danych i programów,

b) normalne ograniczenie dostępu stosownie do rzeczywistej potrzeby,

c) szczególną ochronę przed ujawnieniem.

Środowisko obejmuje użytkowników i wykorzystywane przez nich metody dostępu do systemu; różni użytkownicy mogą mieć takie same lub różne stopnie upoważnienia i mogą korzystać z systemu w trybie *on-line* lub *off-line*.

Łączność zapewnia się korzystając z usług transmisji danych; może ona np. obejmować tylko teren ośrodka APD; może to być również sieć własna lub dzierżawiona, może to wreszcie być publiczna sieć komutacyjna.

Zakres funkcjonalny systemu — usługi, jakie świadczy komputer. Od najprostszego przypadku, jakim jest wyspecjalizowany komputer sterujący procesem przemysłowym, poprzez dialogowe rozwiązywanie problemów, zdalne wprowadzanie zadań, aż do uczestniczenia w pełnej sieci przetwarzania rozproszonego (*distributed processing network*).

A zatem wybór właściwych środków ochrony przed określonym zagrożeniem bezpieczeństwa danych zależy nie tylko od rodzaju tego zagrożenia, ale także od wymienionych i zdefiniowanych czynników kluczowych.

2. Zabezpieczenie fizyczne

Dostęp

Dostępu do jednostki APD, traktowanej jako całość, powinni strzec wartownicy i formalne postępowanie identyfikacyjne.

Kamery telewizji wewnętrznej i mikrofony powinny nieustannie i automatycznie śledzić cały teren. Wszystkie szafy i magazyny, w których przechowywane są „wrażliwe" dane — muszą być zabezpieczone dobrymi zamkami, a wszelki ruch nośników powinien być troskliwie rejestrowany.

Dostęp do pomieszczeń komputera i wszystkich urządzeń pomocniczych, łącznie z systemem klimatyzacji, musi być ograniczony (może przysługiwać wyłącznie upoważnionemu personelowi).

Należy ograniczyć liczbę drzwi — o ile to możliwe do pojedynczych — pamiętając jednak o wyjściach bezpieczeństwa (na wypadek pożaru). Takie wyjścia mogą być otwierane jedynie od wewnątrz i powinny być opatrzone w głośny sygnał alarmowy. Główne drzwi nie powinny wymagać klucza do otwarcia od wewnątrz.

Osoby upoważnione do wstępu można podzielić na trzy kategorie:

— personel eksploatacji (bez programistów, projektantów itp.),
— personel konserwacji,
— goście (za każdorazowym zezwoleniem), zawsze w towarzystwie upoważnionej osoby.

Wiele ośrodków obliczeniowych stosuje politykę „otwartych drzwi" i pozwala na praktycznie nieograniczony dostęp wielu programistów i innych osób do pomieszczeń komputera. Nie tylko stanowi to zagrożenie bezpieczeństwa, ale również przyczynia się do obniżenia dyscypliny i zmniejszenia wydajności pracy. Nie powinny się zdarzać przypadki, że obsłudze komputera poleca się strzeżenie dostępu, nie instruując jej, jak ma postępować w przypadku, gdy ostrzeżenie nie pomaga i przyłapany intruz np. nie chce opuścić pomieszczenia.

Pomieszczenia komputera i jego zaplecza powinny być anonimowe. Należy uniemożliwić zaglądanie do tych pomieszczeń. Nie powinno być znaków wskazujących drogę do tych pomieszczeń. Odwiedzający powinni być odprowadzani, a nie kierowani do sali komputera.

Nie wolno zapominać o instalacjach, od których zależy praca systemu komputerowego, a szczególnie:

— o doprowadzeniu zasilania,
— o sprzęcie transmisji danych,
— o sprzęcie klimatyzującym,
— o sprzęcie chłodzenia wodą (dla niektórych maszyn).

W wielu instalacjach APD nie dość uwagi poświęca się lokalizacji czerpni świeżego powietrza. Znaczne zakłócenia w pracy lub szkody materialne mogą być spowodowane — umyślnie lub przypadkowo — przez wprowadzenie przez te wloty niepożądanych par lub gazów. Istnieje długi wykaz elementów, które nie powinny znajdować się w pobliżu czerpni — lakiernie, stacje benzynowe, magazyny paliw, rozpuszczalników i chemikaliów, urządzenia pylące itp.

Ponadto czerpnia powinna być tak umieszczona, aby nie zwracać uwagi tych, którzy mogliby być zainteresowani zakłóceniem pracy ośrodka obliczeniowego.

Kontrola dostępu do systemu APD sprowadza się w szerokim zakresie do dwóch zasadniczych funkcji: identyfikacji i upoważnienia.

1. Identyfikacja. Jeśli pragnie się w sposób selektywny ograniczyć działalność ludzi do tych tylko spraw, którymi powinni się oni zajmować, a pozbawić ich okazji do robienia rzeczy, których robić nie powinni — trzeba mieć możność nieomylnego rozpozna-

wania tych ludzi. Nie można również obciążać ludzi odpowiedzialnością za ich działanie w ramach określonego systemu, jeśli nie umie się w sposób jednoznaczny stwierdzić tożsamości tych ludzi i działań przez nich wykonywanych.

Wszystkie sposoby identyfikowania ludzi przez system APD sprowadzają się do trzech podstawowych klas. Można posłużyć się czymś, co dana osoba wie (zna), np. hasłem, cechą danej osoby — jak dźwięk głosu lub odcisk palca — wreszcie czymś, co dana osoba posiada — np. plakietka identyfikacyjna, legitymacja, specjalna karta magnetyczna.

Z tych trzech najczęściej jest stosowana — szczególnie do identyfikowania osób korzystających z terminali (końcówek) — metoda pierwsza, przede wszystkim hasło. Jest to metoda prosta i tania, niestety mało skuteczna. Ludzie mają dużą skłonność do komunikowania swojego hasła komukolwiek, z kim zdarza się im pracować i kto może im, znając to hasło, pomóc. Kontrola działania metody haseł jest trudna: i ten kto właśnie „sprzedał" swoje hasło i ten, który je dopiero co otrzymał, wyglądają tak samo, jak wyglądali przedtem. Można tę metodę rozszerzyć przez to, co Amerykanie nazywają *extended handshaking* (dosłownie: „potrząsanie ręką"), to znaczy przez zadawanie pytań, na które odpowiedź powinna znać tylko właściwa osoba. Ten sposób na ogół nie zdaje egzaminu, ponieważ wymaga czasu oraz pamięci komputera i jest irytujący (nikt nie lubi, gdy wścibska maszyna wypytuje go o imiona rodziców czy datę ślubu).

Druga metoda — rozpoznawanie cech — jest w gruncie rzeczy najstarszym sposobem, w jaki rozpoznawało się zawsze swoich bliźnich. Jest ona stale oczywiście stosowana w okienku, gdzie przyjmowane są prace w trybie wsadowym (*batch*). Jednak „nauczenie" komputera, aby rozpoznawał w ten sam sposób użytkowników nie jest łatwe. Automatyczna identyfikacja odcisków palców jest technicznie całkowicie wykonalna, jednakże ekonomicznie mało (przynajmniej na razie) realna. Istnieją urządzenia, rozpoznające kształt dłoni, czaszki, a nawet warg. Jednakże całowanie swojego komputera na dzień dobry nie wydaje się ani szczególnie ekscytujące, ani higieniczne. Najbardziej obiecujące wydaje się rozpoznawanie przez komputer głosu (zapisy oscyloskopowy głosu ludzkiego jest bardzo charakterystyczny i nosi wiele cech indywi-

dualnych). Na rozwiązanie atrakcyjne technicznie i ekonomicznie trzeba jednak jeszcze poczekać.

Przy obecnym stanie techniki stosunkowo najpewniejsza i dość racjonalna wydaje się metoda trzecia — rozpoznawanie na podstawie jakiegoś posiadanego przez daną osobę elementu. Karty z zakodowanym magnetycznie identyfikatorem stosowane są już dość szeroko, jak również dość łatwo dostępne są końcówki ekranowe, wyposażone w czytnik kart magnetycznych. Oczywiście kartę można zgubić — ale jej unieważnienie jest natychmiastowe i skuteczne. Połączenie posiadania karty magnetycznej z hasłem, numerem ewidencyjnym lub nazwiskiem — jeśli nie są one umieszczone na karcie — zwiększa zabezpieczenie.

2. Upoważnienie (autoryzacja). Autoryzacja jest to proces sterowania dostępem do określonych zasobów w zależności od tego, kim jest dana osoba. Tak więc, po zidentyfikowaniu osoby następuje sprawdzenie jej uprawnień, a następnie podjęcie decyzji. Decyzja nie musi być „zero-jedynkowa" (tak lub nie), ponieważ należy rozróżniać jeszcze rodzaje dostępu. Tak na przykład dostęp do zbioru lub jego części może zostać przyznany tylko w celu odczytania informacji, w celu zapisania informacji, wreszcie w celu zmiany (lub usunięcia) informacji; może również wystąpić dowolna kombinacja dwóch lub wszystkich trzech uprawnień. W podobny sposób dostęp może być także regulowany pod względem zakresu (do pewnych pomieszczeń lub elementów informacji tak, do innych — nie) oraz czasowo (w pewnych godzinach dozwolony, w innych nie). Autoryzacji powinna nieodłącznie towarzyszyć rejestracja kto, kiedy i co zrobił z jakim zasobem. Wreszcie autoryzacji i rejestracji powinna również towarzyszyć sygnalizacja w przypadku działań niedozwolonych. Jest to nieodzowny element odstraszenia. Większość ludzi bardziej lęka się samego przyłapania, niż kary, jaką mogą ponieść. Jedną z zasad ochrony jest: nie wystarczy utrudnić dojście — trzeba jeszcze być pewnym, że ten, kto mimo wszystkich „barier" dostanie się do systemu — zostanie przyłapany.

W tablicy III przedstawiono uproszczoną, elementarną macierz działania systemu ochrony, decyzji i skutków tych decyzji.

Każdy z pokazanych w tablicy czterech skutków pociąga za sobą pewne koszty zarówno w sensie ekonomicznym, jak i społecznym.

TABLICA III

Macierz efektów decyzji kontrolującego dostęp

Decyzja kontrolującego dostęp / Działanie systemu ochrony	Zezwolono na dostęp	Odmówiono zezwolenia na dostęp
Udzielono dostępu	Uzasadniony dostęp	Udany atak
Wzbroniono dostępu	Nieuzasadniona odmowa	Udana obrona

Zadaniem prawidłowej metody kontroli dostępu (identyfikacja + + uprawnienie) jest ograniczenie do minimum skutku „udany atak" z jednoczesnym uniknięciem skutku „nieuzasadniona odmowa".

Niektóre aspekty ochrony fizycznej — szczególnie w odniesieniu do kontroli dostępu — zostaną omówione w dalszym toku, przy okazji rozważań na temat zabezpieczeń logicznych.

W zakres zabezpieczenia fizycznego wchodzą również wszelkiego rodzaju systemy alarmowe (pojemnościowe, magnetyczne, na komórki światłoczułe itp.), stosowane powszechnie dla celów ochrony przed włamaniem. W ośrodkach APD stosuje się je w okresach, gdy nie ma na terenie personelu (po godzinach pracy). Nie będziemy się nimi tutaj zajmować szczegółowo. Zresztą ktoś pragnący dostać się na teren ośrodka APD często uznaje za łatwiejsze zadanie próbę wtargnięcia w biały dzień, w godzinach pracy. Ostatecznie, znacznie bardziej wydaje się podejrzany osobnik z łomem, zakradający się do okna o trzeciej nad ranem niż przyzwoicie ubrany pan z teczuszką, wchodzący swobodnie do gmachu instytucji, a następnie wychodzący z dwiema rolkami taśmy w teczce.

Generalnie biorąc, pragnąc skutecznie zabezpieczyć obszary ograniczonego dostępu, nie można ograniczać się do wyboru tylko jednego rodzaju środków spośród trzech możliwych (ochrony ludzkiej, środków mechanicznych i środków elektronicznych) — konieczna jest kombinacja dwóch lub trzech rodzajów.

Jeśli na przykład wartownik zobaczy grupę gości oprowadza-

nych przez dyrektora naczelnego, z pewnością zawaha się przed sprawdzeniem przepustki lub plakietki kogoś, kto wydaje się należeć do tej grupy, nawet jeśli będzie on wzbudzał pewne podejrzenia. Podobnie, poznawszy po pewnym czasie twarze stałych pracowników, zaprzestanie pytania ich co dzień o plakietkę, a np. osoba zwolniona dyscyplinarnie może łatwo skorzystać z okazji, aby bez przeszkód dostać się — jako ktoś znany wartownikowi — na salę komputera i dokonać szkody. Tak więc wartownik powinien pełniąc swą służbę nadzorować jednocześnie inne środki ochrony i sygnalizacji.

Zamki oraz klucze są tanim i pewnym środkiem ochrony dostępu. Są jednak kłopotliwe w użyciu i z reguły, przy większym ruchu, prędzej czy później ktoś może podeprzeć drzwi, aby się nie zatrzasnęły, lub zakleić taśmą zamek zatrzaskowy. Wartownik powinien temu zapobiec.

Automatyczne zamki elektroniczne są wyposażone w obwody sygnalizacyjne, które wywołują alarm (dźwiękowy lub świetlny), jeśli ktoś używa niewłaściwego kodu wejścia lub przytrzymuje drzwi, umożliwiając wejście osobom nieupoważnionym.

Wstęp do pomieszczeń komputera

Każde pomieszczenie komputera — nie tylko właściwa hala jednostki centralnej, ale także pokoje mieszczące urządzenia peryferyjne (drukarki, dziurkarki, końcówki ekranowe itp.) — powinno być objęte kontrolą ruchu osób i tylko osoby, których praca istotnie wymaga dostępu do tych urządzeń mogą mieć stały wstęp do tych pomieszczeń. Oznacza to, że również operatorzy pracujący w systemie zmianowym — nie powinni wchodzić do tych pomieszczeń poza godzinami swojej zmiany.

Osoby, które muszą doraźnie znaleźć się na terenie ograniczonego ruchu (personel techniczny, konserwatorzy, pracownicy administracyjni) powinny być pod stałą obserwacją, a godzina i data ich wejścia czy wyjścia powinny być rejestrowane.

Osobne zagadnienie dotyczy personelu innych jednostek organizacyjnych ośrodka APD (projektanci, programiści itp.). Istnieje naturalna tendencja do traktowania ich jak personelu pracującego na komputerze i zapewniania pełnego dostępu. A jednak dostęp

do komputera osób mających stały kontakt z programami i danymi, a jednocześnie dobrze zaznajomionych z logicznym i mechanicznym działaniem komputera, stanowi jeden z głównych problemów z punktu widzenia pełnej ochrony środowiska APD. Najwięcej znanych przypadków kradzieży, oszustwa i zniszczenia informacji dotyczyło tych właśnie osób.

W okresach, kiedy komputer i związane z nim urządzenia nie pracują konieczne jest zapewnienie aktywnej ochrony fizycznej tych pomieszczeń, a co najmniej układu wykrywania i sygnalizowania obecności intruzów.

W godzinach eksploatacji natomiast o prawidłowej kontroli dostępu do komputera decydować będą przede wszystkim dwa czynniki:

a) skrupulatna rejestracja ruchu wszystkich osób nie należących do obsługi komputera na danej zmianie: kto wszedł, po co, kiedy wyszedł, kto z obsługi mu towarzyszył; jest to wprawdzie dość kłopotliwe, daje jednak gwarancję, że w przypadku jakichś niepożądanych wydarzeń można ściśle ograniczyć liczbę osób przebywających w danym okresie na terenie ośrodka,

b) wyznaczenie odpowiedzialnej osoby, do której będzie należało wypraszanie obcych z pomieszczeń ośrodka; wówczas zadaniem zamków na drzwiach (które bywają zawodne) będzie nie tyle uniemożliwić całkowicie dostęp nieupoważnionym, ile ograniczyć do minimum liczbę osób, które trzeba wypraszać.

Ochrona przed pożarem

Ogień jest poważnym zagrożeniem dla ośrodka APD z szeregu przyczyn. Kilka najważniejszych wymieniono w rozdziale trzecim. Rozmiary strat finansowych spowodowanych pożarem mogą być bardzo wysokie, a jednocześnie prawdopodobieństwo wystąpienia zagrożenia nie jest, niestety, odpowiednio niskie. Z tego względu koszty zabezpieczenia przeciwpożarowego stanowią zazwyczaj bardzo znaczną część budżetu ochrony.

Większość pożarów wybucha poza obszarem ośrodka APD i ewentualnie rozszerza się, obejmując ośrodek. W sytuacji idealnej ośrodek APD powinien być zlokalizowany w osobnym budynku. Jeśli to nie jest możliwe, należy poświęcić najwięcej uwagi

ścianom ogniotrwałym (opóźniającym rozprzestrzenianie się ognia) wokół obszarów, wewnątrz których prawdopodobnie ogień nie będzie nigdy zaprószony. To powinno umożliwić oszczędności na kosztach instalacji, a także często może uchronić cenne urządzenia przed szkodami wodnymi, towarzyszącymi nieuchronnie gaszeniu pożaru. Inaczej mówiąc, przy wyborze systemu wykrywania i tłumienia ognia należy korzystać z usług specjalisty od tych spraw. W każdym razie pomieszczenia nad, pod i obok komputera powinny być używane do celów nie związanych z zagrożeniem ogniowym, a więc mogą tam być lokalizowane np. biura a nie stołówka (kuchnia!), magazyny papieru i materiałów biurowych czy ryzykowne procesy przemysłowe (wstrząsy, eksplozje).

Stłumienie w zarodku każdego zarzewia pożaru jest niesłychanie ważne. Zlokalizowanie pożaru ułatwi podział pomieszczeń ośrodka na strefy rozdzielone ścianami ogniotrwałymi (co najmniej o 2-godzinnej odporności, lepiej 4-godzinnej — klasa A lub B wg polskich oznaczeń) o drzwiach zamykających się samoczynnie. Praktyki podpierania takich drzwi, aby się nie zamykały, powinny być surowo tępione. Obok każdych takich drzwi (na zewnątrz pomieszczenia) należy umieścić odpowiednie gaśnice. Doboru gaśnic powinien dokonać specjalista ochrony przeciwpożarowej. Personel, od którego oczekuje się obsługi gaśnic w przypadku pożaru, powinien być odpowiednio poinstruowany i przeszkolony. Przeszkolenie powinno mieć charakter zarówno teoretyczny, jak i praktyczny. Na dziedzińcu lub na polu należy przeprowadzić praktyczne ćwiczenia w gaszeniu ognia za pomocą gaśnic śniegowych, pianowych, proszkowych oraz piasku i wody.

Systemy wykrywania ognia i tłumienia pożaru powinny być wybierane i instalowane na podstawie pełnej, realistycznej i opartej na dokładnych informacjach analizy ryzyka, kosztów i możliwych źródeł pożaru.

Jeśli w pomieszczeniach zainstalowane są wykrywacze ognia z automatycznym opóźnionym włączaniem urządzeń gaszących — personel powinien być przeszkolony w zakresie postępowania z takimi urządzeniami. Należy tu zwrócić uwagę, że bywają urządzenia, których próg czułości jest zbyt niski i które wywołują wiele fałszywych alarmów. Zachodzi więc potrzeba pouczenia personelu, aby machinalnie nie wyłączał on systemu gaśnic przed

upewnieniem się, że rzeczywiście niebezpieczeństwo pożaru nie istnieje.

Nie wolno zapominać, że istniejące wyposażenie przeciwpożarowe powinno być regularnie sprawdzane, a wyniki każdej takiej inspekcji — szczegółowo rejestrowane. Ważną sprawą jest także kontrola konstrukcji otaczających ośrodek pod względem ich palności i odporności na obciążenie ogniowe.

Pożar w otoczeniu ośrodka może przez promieniowanie cieplne spowodować unieruchomienie ośrodka, ponieważ taśmy magnetyczne i sprzęt elektroniczny ulegają uszkodzeniu w podwyższonych temperaturach.

Wszystkie pomieszczenia ośrodka powinny być wyposażone w kanały, służące do odprowadzania wody w razie jej przypadkowego napływu czy to z górnych kondygnacji, czy w wyniku akcji gaśniczej. Odnosi się to również do stropów nad tymi pomieszczeniami.

Łatwo palnych materiałów pomocniczych (papierów, taśm itp.), koniecznych w ośrodku, nie należy trzymać w ilościach większych niż potrzeba do jednodniowej pracy. Dzienne zapotrzebowanie należy trzymać w metalowych szafach lub pudłach, a uzupełnienia powinny być dostarczane z odseparowanego, ognioodpornego pomieszczenia.

Meble biurowe i całe wyposażenie ośrodka, łącznie z koszami na odpadki, powinny być metalowe; w pomieszczeniach nie powinno być dywanów ani łatwo palnych wykładzin.

Należy zapewnić łatwy i szybki dostęp do przestrzeni pod podniesioną podłogą w celu ułatwienia regularnego jej przeglądania i czyszczenia. Znane są wypadki eksplozji pyłów, które gromadziły się pod podniesioną podłogą. Szczególnie dużo pyłu powstaje w przypadku stosowania pewnych gatunków papieru w szybkich drukarkach wierszowych. Zaleca się sprawdzanie i czyszczenie przestrzeni pod podłogą co najmniej raz na kwartał. Uwagi te odnoszą się również do podwieszonych stropów nad salą komputera.

Przestrzenie pod podłogą i nad podwieszonym stropem stanowią zwykle plątaninę kabli. Należy unikać łączenia przewodów zasilających w wiązki. Jeśli biegną w rowkach, należy je umieścić raczej obok siebie, a nie jeden nad drugim. Wszystkie otwory w stropie

lub podłodze, przez które wyprowadzane są kable, powinny mieć gładkie, zaokrąglone krawędzie.

Klimatyzacja pomieszczeń APD powinna być — w miarę możliwości — niezależna i nie połączona z resztą budynku. Jeśli tak nie jest, w przewodach nawiewowych muszą znajdować się klapy, odcinające ewentualne płomienie lub dym. Wszelkie filtry powietrza muszą być wykonane z materiałów niepalnych. Wyłączniki wentylatorów i klap ogniowych powinny znajdować się na zewnątrz pomieszczeń komputera.

Główny wyłącznik zasilania (wyłączający zasilanie zarówno komputera, jak i instalacji klimatyzacyjnej) powinien znajdować się na zewnątrz pomieszczeń komputera i być łatwo dostępny, ale zarazem zabezpieczony przed dostępem osób nie upoważnionych.

Klasyfikacja zapisów [1])

Zapisy danych i programów, zgromadzone na terenie ośrodka APD, należy ocenić i zakwalifikować do jednej z czterech klas ważności.

Klasa I obejmuje zapisy, które są niezbędne do wykonania zadań ośrodka i nie dają się w ogóle odtworzyć lub też będą potrzebne natychmiast po pożarze, a nie mogą być dostatecznie szybko odtworzone.

Klasa II obejmuje ważne zapisy, których odtworzenie wiąże się wprawdzie z dużymi trudnościami lub znacznymi kosztami, lecz bez krytycznego opóźnienia jakiegokolwiek zasadniczego zadania systemu informatycznego.

Klasa III obejmuje zapisy, których utrata może sprawić wiele kłopotu, ale które można szybko odtworzyć i których zniszczenie nie stanowiłoby niepokonalnej przeszkody w szybkim przywróceniu sprawnej działalności ośrodka.

Klasa IV obejmuje zapisy, które są w danym okresie uznane za niepotrzebne.

W y m a g a n i a d o t y c z ą c e s k ł a d o w a n i a. Zapisy klasy I i II trzymane w hali komputera lub w archiwum nośników muszą być przechowywane w sprzęcie, zapewniającym dostateczną ochronę, tj. w sprzęcie o co najmniej 1-godzinnej odporności ognio-

[1]) Według norm NFPA (National Fire Protection Association, USA).

wej, zaopatrzonym w odpowiedni atest bezpieczeństwa pożarowego. Zapisy należące do klasy III należy trzymać w pudłach lub szafach metalowych, chyba że znajdują się one na nośnikach metalowych, które zgodnie z normami nie wymagają specjalnej ochrony. Zaleca się jednak trzymać w metalowych szafach także zapisy klasy II na nośnikach metalowych. Zapisy klasy IV nie wymagają oczywiście specjalnej ochrony, jako że nie są istotne.

Jeżeli zapisy klasy I i II są przechowywane poza halą komputera, to należy je trzymać w pomieszczeniach o odporności ogniowej współmiernej do stopnia zagrożenia pożarowego, ale nie mniejszej niż 2 godziny (z elementów konstrukcyjnych klasy B wg polskich oznaczeń). Zaleca się, by pomieszczenia magazynowe nie przekraczały kubatury 1400 m^3 dla materiałów papierowych, 280 m^3 dla zapisów na nośnikach z tworzyw sztucznych w pojemnikach niepalnych i 140 m^3 dla zapisów na nośnikach z tworzyw sztucznych w pojemnikach palnych. W odniesieniu do zapisów należących do klas III oraz IV i przechowywanych poza halą komputera nie jest wymagana żadna specjalna ochrona.

Pomieszczenia biblioteki i archiwum nośników magnetycznych powinny być użytkowane wyłącznie w charakterze zgodnym z przeznaczeniem. Wszelkie inne materiały — oprócz rezerwowych taśm i dysków, we właściwy sposób opakowanych — należy z tych pomieszczeń usunąć. Na zewnątrz drzwi do tych pomieszczeń powinny stać przenośne gaśnice (śniegowe, halonowe lub proszkowe).

Najlepszym zabezpieczeniem danych i programów jest oczywiście ich skopiowanie i przechowywanie wtórników w innej części budynku, a najlepiej w innym budynku, który nie powinien być objęty tym samym zagrożeniem pożarowym lub powodziowym. Szerzej będzie o tym mowa w rozdziale piątym.

Przestrzeganie norm zapobiegawczej ochrony przeciwpożarowej zmniejszy zagrożenie pożarowe. Pojemniki na odpady powinny być metalowe, z samozamykającymi się lub tłumiącymi płomień, otwartymi pokrywami. W każdym pomieszczeniu roboczym musi być odpowiednia ilość metalowych popielniczek z ciężką podstawą oraz ścisły harmonogram sprzątania podłóg w celu usunięcia materiałów palnych, gromadzących się wokół drutów i przewodów elektrycznych, szczególnie w izolacji z PCW.

Sprzęt komputerowy powinien być chroniony przez automatyczny system wykrywania i sygnalizacji pożaru, obejmujący przestrzenie nad sufitem i pod podłogą. Czujniki tego systemu powinny znajdować się również w kanałach nawiewowych, gdy instalacja klimatyzacyjna jest scentralizowana. System winien nie tylko dawać ostrzeżenie, ale także automatycznie wyłączać zasilanie komputera i instalacji klimatyzacyjnej energią elektryczną. Obecnie coraz szerzej wprowadzane są systemy o działaniu dwustopniowym. Po wstępnym zaalarmowaniu i krótkim czasie, w którym może nastąpić interwencja ręczna, następuje alarm właściwy i uruchomienie systemu automatycznego gaszenia.

W takich instalacjach ochrony pomieszczeń i sprzętu stosowane są automatyczne systemy detekcyjno-alarmowe, wyposażone w czujniki produktów spalania (czujniki jonizacyjne) lub czujniki dymowe. Zadaniem tych systemów jest wykrycie pożaru w jego początkowym stadium, zasygnalizowanie tego odpowiednim sygnałem dźwiękowym, uruchomienie instalacji gaśniczej w celu szybkiego ugaszenia oraz odcięcie dopływu prądu do sprzętu elektronicznego i do urządzeń klimatyzacyjnych.

W Stanach Zjednoczonych A.P. obowiązują systemy gaśnicze ze zraszaczami wodnymi. W Europie unika się ich ze względu na szkody wodne. Zarówno w Stanach Zjednoczonych, jak i w Europie szeroko stosowane są do dziś systemy gaszące dwutlenkiem węgla. Ich wielką wadą jest zagrożenie zatruciem personelu. Do stłumienia ognia potrzebne jest stężenie CO_2 w powietrzu 50÷60%. A już stężenie 5÷6% jest wystarczające dla uśmiercenia człowieka. Tak więc wszelkie systemy z CO_2 muszą być tak projektowane, aby niebezpieczeństwo pozostawania kogoś w strefie gaszenia było wykluczone.

Obecnie wprowadza się szeroko jako środek gaszący halogenowane węglowodory. Z kilku dostępnych typów najbardziej zalecany jest halon 1301 (bromotrójfluorometan), jako najmniej toksyczny dla ludzi oraz nie powodujący korozji urządzeń. Przy stężeniu gaśniczym tego halonu 3,7% pożary gaszono w ciągu 7—8 sekund. Zgodnie z danymi NFPA oddychanie powietrzem przy stężeniu halonu 1301 do 7% jest praktycznie nieszkodliwe, przy stężeniu 7÷10% wywołuje lekkie i szybko mijające objawy zatrucia, a dopiero przy stężeniach powyżej 10% efekt może być groźny dla istot

żywych. Przy wysokich temperaturach następuje rozkład halonu i w pewnych okolicznościach wolny fluorowodór i bromowodór — mogą być przyczyną lekkiej korozji urządzeń elektronicznych.

Najważniejsze wskazówki co do postępowania w przypadku alarmu pożarowego oraz najważniejsze numery telefonów powinny być wywieszone w widocznych miejscach. Personel należy przeszkolić w zakresie następujących procedur:

a) wyłączanie dopływu energii
b) wyłączanie wentylacji i klimatyzacji

(jeśli nie ma systemu automatycznego)

c) ewakuacja najważniejszych dokumentów,
d) zamykanie szaf ogniotrwałych,
e) posługiwanie się sprzętem przeciwpożarowym,
f) sztuczne oddychanie,
g) pierwsza pomoc.

Oprócz omówionych podstawowych zasad działania w celu zapewnienia ochrony przeciwpożarowej urządzeniom APD, należy dodatkowo uwzględnić lokalne kodeksy budowlane i przepisy ochrony przeciwpożarowej, tak aby warunki w każdym ośrodku obliczeniowym odpowiadały obowiązującym normom i przepisom prawnym.

Gospodarka makulaturą

Zabezpieczenie fizyczne obejmuje także problem niszczenia materiałów „wrażliwych", które przestają być potrzebne. Chodzi tu o kopie wszelkiego rodzaju dokumentów tajnych, poufnych i objętych tajemnicą służbową. Postępowanie z tymi dokumentami normują przepisy o tajemnicy służbowej i państwowej. Przepisy te na ogół nie uwzględniają jednak nośników informacji na wejściu i wyjściu komputera, czyli kart i taśm dziurkowanych, taśm i dysków magnetycznych oraz wydruków komputerowych.

Wszystkie te materiały — jeśli tylko nie podlegają archiwowaniu (kopie nadliczbowe, materiały robocze itp.) — bądź powinny zostać zniszczone, bądź też (jeśli nadają się, jak np. taśmy i dyski do ponownego wykorzystania) zapisane na nich dane należy skasować. Wiele komputerów dysponuje funkcją „zerowania" pamięci operacyjnej, taśm i dysków.

Należy pamiętać, że bieżącej pracy każdego komputera towarzyszy powstawanie ogromnych ilości zadrukowanego papieru, a treść na nim zawarta często ma krótkotrwałą użyteczność, choć niesie wiele interesujących informacji. Stąd też ogromne ilości makulatury, której niełatwo pozbyć się. Makulaturę tę należy gromadzić w strzeżonym i zamkniętym pomieszczeniu, a następnie w opłacalnych (z punktu widzenia transportu) partiach dostarczać bezpośrednio do fabryk papieru. Materiały bardziej wrażliwe należy uprzednio przepuścić przez tzw. „siekacze" lub „wilki" do papieru. Prawdziwy kłopot stwarzają kalki przy wydrukach wielokopiowych. Nie nadają się one na makulaturę, a ich niszczenie jest bardzo kłopotliwe. Stosunkowo najlepszym rozwiązaniem jest spalanie ich pod kotłami, jeśli powstające sadze nie grożą zanieczyszczeniem okolicy.

Jak wynika z dotychczasowych doświadczeń, najpewniejszą metodą wykradania informacji — a w każdym razie najtańszą i najłatwiejszą — jest grzebanie w koszach na śmieci. Znane są przypadki, że stare wydruki komputerowe używane były... do zawijania śledzi lub też robiono z nich bloki makulaturowe powszechnego użytku. Dopóki będzie się spotykać objawy takiego niedbalstwa, można sobie nie zaprzątać głowy podsłuchem na liniach transmisyjnych czy przechwytywaniem promieniowania elektromagnetycznego.

3. Zagadnienia kadrowe i organizacyjne

Ogromnie istotną sprawą z punktu widzenia bezpieczeństwa informacji jest morale personelu, który styka się z tą informacją. Morale to z kolei w danym ośrodku zależy od metody rekrutacji i doboru personelu, odpowiedniego przeszkolenia, motywacji (a więc bodźców psychologicznych i materialnych), wreszcie właściwego, ciągłego nadzoru.

W przypadkach gdy system APD wspiera tylko jedną określoną funkcję, jak np. kontrola zapasów magazynowych lub przyjmowanie zamówień, zatrudniony przy tej funkcji personel na ogół czuje konkretną odpowiedzialność i ma wystarczającą motywację, aby chronić dane i zapewnić pożądane wyniki końcowe. Gdy jed-

nak ośrodek APD realizuje szereg takich systemów, jego personel często nie zdaje sobie sprawy ze skutków ujawnienia, utraty lub zniszczenia danych w którejkolwiek z obsługiwanych dziedzin.

Ludzie na ogół reagują pozytywnie, gdy daje się im do zrozumienia, że wykonują pracę ważną i odpowiedzialną oraz że okazuje się im pełne zaufanie. Dlatego też, drogą odpowiedniego instruktażu i szkolenia, należy uświadomić personelowi ośrodka APD jego kluczową rolę, jeśli chodzi o pomyślną realizację funkcji wspieranych przez systemy APD oraz powagę problemów, jakie mogą zaistnieć, jeśli personel APD nie będzie świadomy potrzeby chronienia danych, powierzonych jego opiece.

Jeśli jednak nie są stosowane sankcje dyscyplinarne wobec tych, którzy lekceważą ustalone procedury zabezpieczenia, to reszta zatrudnionych ma prawo sądzić, że kierownictwo nie przywiązuje większej wagi do spraw bezpieczeństwa. Środki zabezpieczenia, które normalnie powinny być wystarczająco efektywne, staną się bez znaczenia, jeśli ludzie stwierdzą, że można je obejść lub ignorować bezkarnie. Jest to szczególnie groźne wówczas, gdy ci, którzy ignorują lub lekceważą otwarcie przepisy bezpieczeństwa należą do personelu kierowniczego.

Aspekty organizacyjne systemu zabezpieczenia informacji zasługują na więcej uwagi, niż im się jej dotychczas poświęca. Można tu wyodrębnić trzy podstawowe reguły:

— przydział odpowiedzialności,
— podział odpowiedzialności,
— rotacja odpowiedzialności.

Przydział odpowiedzialności

Jest sprawą podstawową, aby odpowiedzialność na każdym etapie cyklu przetwarzania była przydzielona w sposób jednoznaczny konkretnej osobie lub stanowisku. Zarówno dane, jak i programy stanowią pewien majątek, podobnie jak inne, bardziej uchwytne dobra. Jeśli pragnie się zapewnić im wystarczającą ochronę, musi być ściśle sprecyzowana odpowiedzialność w tym względzie.

Ogólnie biorąc, ktokolwiek ma styczność fizyczną z danym obiektem — powinien być bezpośrednio odpowiedzialny za ochronę tego obiektu. W przypadku danych znajdujących się na terenie ośrodka APD odpowiedzialność ta spoczywa na barkach kierow-

nictwa ośrodka. Zabezpieczenie danych i programów na innym terenie jest obowiązkiem osób, mających tam z nimi styczność. Kontrola wewnętrzna oraz SOI powinny kontrolować środki zabezpieczenia, jednakże ich odpowiedzialność jest z konieczności pośrednia.

Użytkownicy korzystający z usług APD mogą odpowiadać za dane jedynie do chwili, gdy znajdą się one na terenie ośrodka obliczeniowego, a następnie po jego opuszczeniu. Ponoszą oni także odpowiedzialność za użytkowanie znajdujących się na ich terenie terminali.

Z punktu widzenia użytkownika podstawą bezpieczeństwa eksploatacji jest wprowadzenie do systemu właściwych metod kontroli i weryfikacji, a następnie sprawdzenie po pewnym okresie eksploatacji, czy system nie został naruszony. W warunkach wielodostępności sprawa komplikuje się nieco, a zapewnienie poufności informacji w tak szerokim środowisku zależy od szeregu czynników, nad którymi przeciętny użytkownik nie ma żadnej kontroli.

Poufność informacji może zostać zagrożona w efekcie celowego działania lub też przypadkowo, w wyniku błędów w systemie albo błędów popełnianych przez użytkowników systemu. Kroki zapobiegające temu zagrożeniu mogą ograniczać się do uniemożliwienia dostępu osobom nieautoryzowanym, ale mogą także obejmować szyfrowanie danych przez substytucję i transpozycję znaków albo przez sumowanie algebraiczne znaków wiadomości ze znakami jakiegoś klucza.

Projektanci systemów odpowiadają za określenie wymagań pod względem bezpieczeństwa, za wprowadzenie odpowiednich zabezpieczeń do systemu i za poinstruowanie użytkownika w zagadnieniach ochrony informacji. Nie należy jednak zapominać, że odpowiedzialność projektanta za bezpieczną pracę systemu kończy się z chwilą ostatecznego przejęcia systemu do eksploatacji.

Do obowiązków inspektorów i audytorów[2] należy na ogół wy-

[2]) Augielskiemu słowu „Auditor" odpowiadać mogą w bezpośrednim tłumaczeniu — zależnie od kontekstu — terminy: rewident, inspektor, kontroler. Aby uniknąć wieloznaczności w dalszym toku operować się będzie terminem *audytor*, choć ściśle mówiąc ma ono nieco inne znaczenie w języku polskim; więcej na ten temat — w rozdziale szóstym.

jaśnienie przyczyn przypadków naruszenia bezpieczeństwa już po ich wystąpieniu. Inaczej mówiąc, główny nacisk kładziony jest na poszukiwanie słabych punktów systemu i wykrywanie przekroczeń w tym zakresie, a nie na projektowanie lub wdrażanie środków zabezpieczenia. Zazwyczaj audytorzy finansowi i księgowi nie posiadają dostatecznej wiedzy informatycznej, aby móc dokonywać inspekcji z punktu widzenia zabezpieczenia danych i urządzeń.

Można sobie wyobrazić powstanie specjalnych zespołów audytorskich, które mogłyby na zlecenie dokonywać analizy stanu zabezpieczenia określonych grup danych oraz całych ośrodków obliczeniowych, łącznie z bankami danych (por. rozdział szósty).

Personel archiwów, bibliotek i banków danych może wiele zdziałać w zakresie zabezpieczenia informacji i jej nośników. Ludzie ci są również odpowiedzialni za sprawny przebieg normalnej działalności instytucji (przedsiębiorstwa) w przypadku umyślnego lub przypadkowego zniszczenia ważnych danych. Komórki te współpracują z komórkami prawnymi w zakresie ustalania norm przechowywania oraz zabezpieczania dokumentów i materiałów informacyjnych (ważne, by było to w miarę możliwości w postaci czytelnej dla maszyny).

Podział odpowiedzialności

Znaną i stosowaną w dziedzinie kontroli księgowej i finansowej zasadą jest, aby odpowiedzialność kluczowa zawsze była ponoszona wspólnie przez więcej niż jeden wydział lub osobę. Tę samą zasadę należy bezwzględnie stosować w przetwarzaniu danych.

Po pierwsze żadnej osobie, bez względu na jej kwalifikacje i znaną uczciwość, nie wolno powierzać wyłącznej odpowiedzialności za opracowanie większego systemu. W szczególności nikt nie powinien odpowiadać łącznie za opracowanie systemu i za jego eksploatację oraz konserwację.

Po wtóre nie należy obarczać jednej osoby (bez nadzoru) odpowiedzialnością za wprowadzanie zmian lub aktualizację programów.

Po trzecie operator nie powinien sam brać programów lub zbiorów danych z biblioteki. Odpowiedzialność za nie musi spoczy-

wać na bibliotekarzu, któremu z kolei nie wolno uruchamiać ani obsługiwać komputera. Jeśli podczas nocnej zmiany nie ma bibliotekarza, wszystkie potrzebne zbiory muszą być wcześniej przygotowane i wyniesione na zewnątrz biblioteki.

Po czwarte w żadnych okolicznościach nie może przebywać w pomieszczeniu komputera tylko jedna osoba.

Po piąte — zanim jakiś system (lub pewna jego modyfikacja) wejdzie do eksploatacji, powinien zostać poddany badaniu przez osobę lub grupę osób, które nie były bezpośrednio zaangażowane w jego opracowanie.

Po szóste inspekcja (kontrola) wewnętrzna powinna dokonywać wyrywkowo sprawdzania wybranych przez siebie systemów.

Rotacja odpowiedzialności

Żaden programista ani projektant systemów nie powinien stale pracować nad tym samym typem prac. Trudniej w ten sposób ukryć swoje błędy; łatwiej dokończyć ewentualnie pracę za kogoś, kto odszedł (zachorował itp.); praca jest wykonywana staranniej, jeśli wiadomo, że w każdej chwili ktoś inny może ją przejąć i ocenić. Ponadto praca staje się bardziej urozmaicona.

Żaden operator nie powinien regularnie obsługiwać tych samych programów. Nie musi on w ogóle znać bliższych szczegółów obsługiwanego programu. Właśnie w przypadku operatorów należy zwracać szczególną uwagę na uczciwość i lojalność. Pożądane jest wprowadzenie dwuosobowej obsługi komputera, przy czym dobrze byłoby, gdyby skład takich „dwójek" ulegał ciągłej rotacji; utrudnia to zmowę. Wskazane jest, aby jeden operator podlegał kierownikowi eksploatacji, a drugi np. kierownikowi zespołu programistów. W ten sposób interesy nie dopuszczanych do pomieszczeń komputera programistów mogą być w pewnym sensie reprezentowane przez jednego z operatorów.

Urlopy powinny być obowiązkowo wykorzystywane w z góry ustalonych terminach.

Ład i porządek

Dobre gospodarowanie i ład są nieodzownymi warunkami dobrego zabezpieczenia. W dbałości o nie należy między innymi pamiętać o następujących zasadach postępowania:

— do minimum ograniczać ilość papieru w sali komputera,

— regularnie opróżniać kosze na śmieci,

— książka pracy maszyny powinna być prowadzona dokładnie i na bieżąco,

— jedzenie, picie i palenie powinny być zabronione w sali komputera, bibliotece oraz wszystkich pomieszczeniach pomocniczych.

Spożywanie posiłków w sali komputera grozi np. rozlaniem kawy, mleka czy słodkiej herbaty i uszkodzeniem sprzętu. Stosy taśm, dysków, kart dziurkowanych ułatwiają niepostrzeżone wyniesienie nośników danych z pomieszczenia. Dym z papierosów działa szkodliwie na urządzenia elektroniczne; może ponadto spowodować uruchomienie alarmu pożarowego.

Warto przy okazji zwrócić uwagę, że rampa służąca do odbioru dostaw papieru umożliwić może wejście intruzowi. Zwały zużytego papieru przygotowane na rampie do wywiezienia mogą ponadto stanowić bogate źródło ciekawych i jakże łatwych do zdobycia informacji. Dane poufne powinny zatem — zanim umieści się je na rampie — przejść przez specjalny siekacz. Karty dziurkowane należy przynajmniej rozsypać i pomieszać tak, aby ich zebranie i pogrupowanie w wymaganym porządku musiało kosztować wiele wysiłku.

Nadzór nad dokumentacją

Jednym z podstawowych warunków prawidłowej działalności ośrodka APD jest troskliwa opieka nad kontrolowanym obiegiem i właściwym przechowywaniem dokumentacji; wiąże się to z przestrzeganiem następujących zasad:

— wszystkie dokumenty muszą być numerowane i rejestrowane w chwili powstania,

— dokumenty dotyczące eksploatacji komputera powinny być pod opieką bibliotekarza i traktowane równie troskliwie, jak taśmy, dyski itp.,

— kopiowanie dokumentów powinno być dokonywane tylko przez specjalną komórkę i pod ścisłą kontrolą,

— dokumenty powinny być zamykane po godzinach pracy.

Biblioteka

Biblioteka zbiorów, programów i dokumentacji powinna być otwarta tylko w czasie obecności odpowiedniego pracownika. Wstęp do niej powinni mieć wyłącznie pracownicy specjalnie upoważnieni przez kierownictwo.

Bibliotekarz powinien stale, na bieżąco prowadzić zapisy dotyczące ruchu każdej szpuli, pakietu dysków, pliku kart itd.

Wszystkie pozycje biblioteczne powinny być chronione fizycznie: w szafach ogniotrwałych dobrze zamykanych. Wszystkie ważne zbiory i dokumenty powinny mieć kopie (wtórniki). Biblioteka powinna znajdować się w osobnym pomieszczeniu, zlokalizowanym blisko sali komputera.

Często zdarza się, że wiele osób ma praktycznie nieograniczony dostęp do biblioteki taśm i dysków. Niektóre biblioteki obudowane są wprawdzie grubymi ścianami, ale drzwi do nich są stale otwarte. A przecież gdyby ściany biblioteki były szklane lub gdyby okalały ją przepierzenia do wysokości piersi — byłby ułatwiony stały wgląd do wnętrza biblioteki i uniemożliwione lub przynajmniej utrudnione dokonywanie szkód w sposób niezauważalny. Biblioteka powinna być traktowana jako część pomieszczenia komputera i należy ją objąć tymi samymi ograniczeniami dostępu oraz zabezpieczeniami przed ogniem, dymem i wodą.

Programy, stanowiąc pewien majątek, powinny podlegać ochronie, podobnie jak dane. Oprócz tego należy także zapewnić ścisłą kontrolę i rejestrację ewentualnych modyfikacji programów, a także sprawdzanie czy w wyniku jakiejś zmiany nie nastąpiło uszkodzenie programu lub groźba ujawnienia zastrzeżonych danych.

Po zakończeniu pracy wszystkie pomieszczenia ośrodka powinny być dokładnie zamknięte i strzeżone przez wartowników. Praca w godzinach nadliczbowych może się odbywać tylko za specjalnym zezwoleniem i tylko pod warunkiem, że wykonywać ją będą co najmniej dwie osoby.

Oświetlenie ewakuacyjne

W pomieszczeniach ośrodka APD powinno być zainstalowane oświetlenie ewakuacyjne, zasilane z baterii akumulatorów. Oświe-

tlenie to powinno włączać się automatycznie po wyłączeniu zasilania komputera i klimatyzacji, a także w przypadku przerwy w dopływie energii z sieci elektroenergetycznej.

4. Zabezpieczenie logiczne

Zabezpieczenie logiczne systemu APD jest zagadnieniem złożonym. Podczas gdy zabezpieczenia fizyczne i organizacyjne ograniczają się w zasadzie do ochrony systemu przed zagrożeniami umyślnymi, zamierzonymi, na oprogramowaniu spoczywa ponadto — i to prawie w całości — zadanie ochrony przed błędami i zagrożeniami przypadkowymi. Funkcje ochronne podzielone są przy tym pomiędzy oprogramowanie podstawowe — a więc system operacyjny i całą bibliotekę programów usługowych (procesory pomocnicze, kompilatory, translatory itp.) — a oprogramowanie zastosowań. Oprogramowanie podstawowe użytkownik komputera nabywa na ogół wraz ze sprzętem i — jakkolwiek dokonując wyboru określonej maszyny wybiera jednocześnie system operacyjny o określonych cechach i funkcjach ochronnych — nie ma on zbyt wielkiego wpływu (oprócz pewnych opcji) na stopień zabezpieczenia logicznego systemu.

Natomiast podczas opracowywania programów określonych zastosowań użytkownik może i powinien przewidywać wprowadzanie dodatkowych funkcji wychwytywania i korekty błędów, zabezpieczenia obszarów pamięci i kontroli dostępu do zbiorów, zapisów, a nawet poszczególnych pozycji w zapisach. Zakres tych kroków zapobiegawczych będzie zależał przede wszystkim od sytuacji wyjściowej, a więc od zakresu zabezpieczeń już istniejących w oprogramowaniu systemowym, a następnie od wrażliwości i poufności określonych programów i danych przetwarzanych przez te programy.

System operacyjny (SO) sprawnie zarządza zasobami komputera, przyjmując na siebie przydział kanałów i urządzeń peryferyjnych i uwalniając programistę od wielokrotnego kodowania alokacji takich zasobów, jak jednostki taśmowe i dyskowe. Przydziela on również miejsce w pamięci operacyjnej i ma za zadanie zapewnić odseparowanie od siebie obszarów przydzielonych różnym pro-

gramom. Inaczej mówiąc SO kontroluje środowisko komputera w jego sprzężeniach (*interfaces*) z programami użytkowników, wykonującymi określone zadania; ułatwia także gospodarkę eksploatacyjną poprzez rejestrowanie wykorzystania urządzeń i programów, sporządzanie statystyki eksploatacyjnej i pilnowanie priorytetów.

System operacyjny steruje również transmisją danych oraz formuje kolejki nadchodzących komunikatów (zapytań, żądań), dopuszczając je pojedynczo do jednostki centralnej. W podobny sposób SO automatycznie rejestruje dane wyjściowe w buforze na taśmie lub dysku magnetycznym, gdzie przetrzymuje je do czasu, kiedy np. wolna będzie drukarka.

Wprowadzanie ewentualnych zmian do SO musi być znacznie surowiej nadzorowane, niż wprowadzanie zmian do programów użytkowników. Przede wszystkim wszelkie zmiany muszą być uzgodnione z dostawcą SO — w przeciwnym razie można utracić usługi gwarancyjne. Przetestowanie SO po wprowadzeniu zmian ma ogromne znaczenie, ponieważ SO oddziałuje wzajemnie ze sprzętem, obsługą i programami użytkowników. Może np. po jakiejś zmianie zajść konieczność ponownej kompilacji wszystkich programów aplikacyjnych. Wszelkie zmiany w SO są więc również bardzo kosztowne.

Funkcje ochronne SO

System operacyjny jest takim samym programem, jak wszystkie inne. Dlatego też we wszystkich współczesnych komputerach musi istnieć strukturalna ochrona pamięci operacyjnej, polegająca na podzieleniu jej na różne sektory, osobne dla SO i dla programów aplikacyjnych. W konstrukcji sprzętu został uwzględniony mechanizm, zapobiegający uzyskaniu za pośrednictwem programu użytkownika dostępu do sektorów innych niż przydzielone danemu programowi. Mechanizm ten powinien chronić osobno przed pisaniem, czytaniem i wykonywaniem operacji na danych. Program, któremu udałoby się dostać do systemu operacyjnego, mógłby uzyskać również dostęp do wszelkich innych informacji zawartych w komputerze.

Często zachodzi potrzeba, aby dwa programy miały dostęp do

tej samej informacji. Najpospolitszym przykładem może tu być sytuacja, gdy program użytkownika musi komunikować się z systemem operacyjnym. To komunikowanie się jest zazwyczaj umożliwione w taki sposób, że SO jest zawsze „panem" a program użytkowy — „niewolnikiem". Program użytkownika może żądać od SO wykonania określonych funkcji lub dostarczenia pewnych danych. Jednak SO powinien zawsze dokonywać pełnej kontroli poprawności i prawomocności żądania programu, zanim żądanie to zostanie zaspokojone.

W większości komputerów jednostka centralna rządzi wszystkim, co dzieje się wewnątrz komputera. A zatem bezpieczny system nie umożliwia programiście bezpośredniego dostępu do wszystkich funkcji (zasobów) jednostki centralnej. Zazwyczaj zasoby jednostki centralnej są podzielone na dwie grupy: zasoby wspólne i uprzywilejowane. Zasoby wspólne są dostępne dla wszystkich programów; zasoby uprzywilejowane są dostępne tylko dla SO. Bywa to również tak rozwiązywane, że dla zasobów uprzywilejowanych jest przeznaczona osobna jednostka centralna. Jeśli program użytkownika przewiduje dokonanie uprzywilejowanej operacji, musi to odbywać się drogą pośrednią. Program użytkownika przesyła komunikat do SO, który najpierw sprawdza uprawnienia komunikatu, a następnie odpowiednio reaguje. Wszelkie przerzuty danych pomiędzy różnymi sektorami pamięci oraz do i z jednostek peryferyjnych są operacjami uprzywilejowanymi. Równiez uprzywilejowane są wszelkie zmiany w systemie zabezpieczeń komputera, jak np. zmiany w ochronie obszarów pamięci.

System operacyjny jest więc zazwyczaj zabezpieczony przed dostępem ze strony programów użytkowników i wiele szczególnie ryzykownych operacji może być dokonywanych tylko przez SO.

Mimo że SO jest jednym z najlepiej sprawdzonych i chronionych programów w komputerze, nie można i tu wykluczyć pewnych pomyłek. Niektóre z nich mogą zostać wykorzystane przez zręcznego manipulatora. Każdy z takich błędów jest unikalny i trudny do sklasyfikowania, ale można wymienić kilka przykładów częściej występujących słabych punktów systemów operacyjnych:

1. Kiedy program użytkownika żąda od SO wykonania pewnej operacji, nie zawsze następuje dokładne sprawdzenie prawomocności żądania.

2. Program użytkownika ma możliwość zmiany treści komunikatu do SO już po sprawdzeniu przez SO jego prawomocności, ale zanim nastąpiło wykonanie żądanej operacji.

3. Po umieszczeniu przez SO sprawdzonej już informacji w obszarze pamięci użytkownika (np. zawartość buforów wejścia/wyjścia z towarzyszącą informacją), program użytkownika może zmienić tę informację tak, że zostanie ona później mylnie zinterpretowana przez SO.

4. Istnieje w SO pewna „furtka" celowo umieszczona dla ułatwienia pracy programistów systemowych lub dla przewidywanych w przyszłości, ulepszonych programów usługowych. Furtka taka może jednak zostać nadużyta przez inne programy. Może ona również powstać w wyniku dywersyjnej działalności (z myślą o przyszłym wykorzystaniu) nieuczciwego członka grupy, opracowującej system operacyjny. Przyczynami takich słabych punktów SO mogą być: zbyt wysoki koszt wyrafinowanych metod zapewniających pełne bezpieczeństwo, a także — najczęściej — fakt, że współczesne SO są tak rozbudowane i skomplikowane, że nikt nie jest w stanie objąć wszelkich rodzajów interakcji, jakie mogą wystąpić wewnątrz SO.

System operacyjny może być opracowany tak, żeby ryzyko wystąpienia tych słabych punktów było mniejsze. Może on zostać podzielony na wiele podprogramów, które są wzajemnie chronione przed sobą tak, jakby były programami użytkowymi. Kiedy jeden z takich podprogramów żąda od innego wykonania jakiejś operacji, żądanie to zostaje zweryfikowane, podobnie jak żądania użytkowników. Tego rodzaju struktura SO ma wiele zalet z punktu widzenia ochrony: intruz, któremu uda się wtargnąć do jednej „komory" nie uzyskuje natychmiastowego dostępu do innych „komór"; najbardziej ryzykowne operacje mogą zostać umieszczone w podprogramie, który licznymi „drzwiami" jest odseparowany od podprogramów stykających się bezpośrednio z programami użytkowników; sumienne sprawdzenie każdego podprogramu jest łatwiejsze niż całego SO.

Rozważania te, skądinąd interesujące, niewiele dają komuś, kto otrzymał gotowy SO wraz z zakupionym komputerem. Może on jednak, jeśli przywiązuje dużą wagę do zabezpieczeń, korzystać ze starszych, z reguły lepiej sprawdzonych, wersji systemu. Czę-

sto wiąże się to, niestety, z rezygnacją z pewnych udoskonaleń lub nowych funkcji wprowadzanych do kolejnych wersji. Można również „zaminować" system. Polega to na wprowadzeniu do SO specjalnych funkcji sprawdzających i na zamianie niektórych pól danych. Zaminowanie ma na celu ochronę przed zręcznym intruzem, który miał okazję zapoznać się szczegółowo z danym SO w innym ośrodku obliczeniowym. Infiltrację systemu można tylko wtedy uznać za udaną, jeśli nie została ona wykryta. Tymczasem SO jest zazwyczaj tak wrażliwy, że intruz łatwo może spowodować „upadek" systemu, zwłaszcza jeśli w pewnych miejscach obraz SO będzie inny, niż ów intruz mógł się spodziewać. Analiza przyczyn upadku systemu może wykazać, co się wydarzyło.

Jest rzeczą bardzo ważną, aby SO zawsze zerował wszystkie zbiory, gdy tylko zostaną one zwolnione przez użytkownika. Odnosi się to do zbiorów roboczych oraz do pamięci operacyjnej lub wirtualnej (zerowanie nie daje pełnego zabezpieczenia, jeśli chodzi o taśmy i wymienne dyski magnetyczne; specjalne postępowanie może ujawnić informację nawet po kilkakrotnym zapisaniu jej nieregularnymi szumami).

Dotychczas nie jest znany system operacyjny bezpieczny w stu procentach. Niektóre opublikowane prace teoretyczne dowodzą, że nie istnieje praktyczna procedura, prowadząca do możliwości stwierdzenia z całą pewnością, że dany sytem jest całkowicie bezpieczny (*secure computer system certification*). Żadna z firm produkujących oprogramowanie nie może się pochwalić, że któryś z jej systemów nie został nigdy „złamany".

Dlatego też jedynym sposobem wyeliminowania problemu zabezpieczenia jest posiadanie komputerów całkowicie i wyłącznie przeznaczonych (*dedicated*) do prac tajnych (przynajmniej na pewnych zmianach roboczych) tak, że całe wejście i wyjście dostępne jest tylko osobom upoważnionym. W większości krajów jest to jedyna dopuszczalna metoda przetwarzania ściśle tajnych danych wojskowych. Metoda ta jest bardzo kosztowna w przypadku dużych, rozbudowanych zestawów komputerowych.

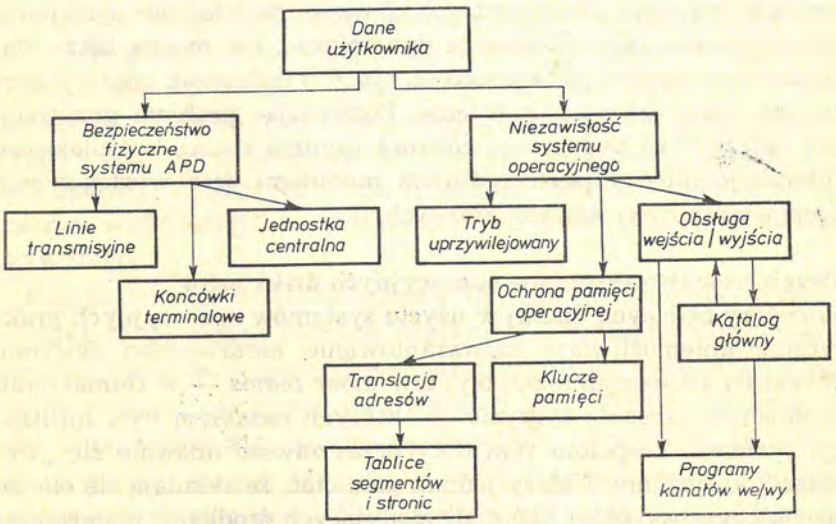
Niezawisłość systemu (*system integrity*)

W anglosaskiej literaturze informatycznej często spotyka się termin *system integrity*. Najczęściej bywa on tłumaczony na polski

jako „integralność systemu". W gruncie rzeczy słowo *integrity* nie jest jednoznacznie przetłumaczalne. Oznacza ono, zależnie od kontekstu: całkowitość, głębię, czerstwotę, nienaruszalność; w stosunku do osób: prawość, uczciwość, niezawisłość [3]). W zestawieniu „system integrity" należy go — moim zdaniem — tłumaczyć jako „niezawisłość systemu". Odpowiednik ten wystarczająco, z punktu widzenia przedmiotowej tematyki, odzwierciedla sens wyrażenia angielskiego.

Przez *niezawisłość systemu* należy tu rozumieć możność przewidywania, że dany system wykonuje to, co do niego należy, to co nam się wydaje, że powinien wykonywać i — miejmy nadzieję — nic innego.

Z pojęciem tym wiąże się właściwe funkcjonowanie sprzętu i oprogramowania, odpowiednie bezpieczeństwo fizyczne i konieczny stopień zabezpieczenia przed podsłuchem i przechwytywaniem promieniowania. Na rysunku 6 został przedstawiony schemat zależności, jakie występują między nienaruszalnością danych przetwarzanych przez system APD *trzeciej generacji plus* (trzecia i na-



Rys 6. Nienaruszalność danych użytkownika systemu APD jako funkcja zabezpieczenia fizycznego i niezawisłości systemu operacyjnego

[3]) Por.: *The Kościuszko Foundation Dictionary*, New York 1959; *The Concise Oxford Dictionary of Current English*, Oxford University Press 1964.

stępne), a bezpieczeństwem fizycznym systemu oraz niezawisłością SO.

Jak wynika ze schematu, bezpieczeństwo fizyczne zależy od skuteczności zabezpieczenia jednostki centralnej, linii transmisyjnych oraz końcówek (terminali).

Niezawisłość systemu operacyjnego zagwarantowana jest tylko wtedy, gdy realizowane są prawidłowo (i kontrolowane): praca SO w trybie uprzywilejowanym, ochrona pamięci operacyjnej oraz obsługa kanałów wejścia i wyjścia. Pamięć operacyjna z kolei jest skutecznie chroniona tylko pod warunkiem, że jednocześnie spełniane są dwa wymagania: prawidłowo zestawione i chronione tablice adresowania oraz właściwie wykorzystane klucze ochrony pamięci. Podobna zależność występuje dla odgałęzienia „obsługa wejścia i wyjścia", z tym że dochodzi tu wzajemna zależność z katalogiem głównym (*directory*). Ta wzajemna zależność oznacza, że penetracja katalogu zagraża obsłudze wejścia/wyjścia i vice versa. Oznacza to również, że zależności występujących w związku z ochroną nienaruszalności danych nie można przedstawić za pomocą prostego wykresu „drzewiastego". Z uwagi na właściwe systemowi operacyjnemu skomplikowanie dynamiczne, nie można także statycznego schematu pokazanego na rys. 6 [4]) traktować jako wyczerpująco ilustrującego zagadnienie. Rozważając problem penetracji SO należy brać pod uwagę również czynnik czasu, kompleksowe interakcje między poszczególnymi modułami oraz występowanie niepowtarzalnych zdarzeń losowych.

Bezpieczeństwo systemów operacyjnych dziś i jutro

Rozmiary będących dzisiaj w użyciu systemów operacyjnych praktycznie uniemożliwiają zagwarantowanie niezawisłości systemu. Wykazały to specjalne zespoły, tzw. *tiger teams* — w tłumaczeniu dosłownym „zespoły tygrysie" — których zadaniem była infiltracja systemu. Zespołom tym dotychczas zawsze udawało się „wedrzeć" do systemu. Należy jednak pamiętać, że składają się one ze specjalistów wysokiej klasy, dysponujących środkami materialnymi, znających w szczegółach system komputerowy i mających nieograniczony czas na wykonanie tego zadania.

[4]) Schemat przedstawiony na rys. 6 odnosi się, ściśle biorąc, do systemów wirtualnych. Przytoczone tutaj rozważania mają jednak sens ogólny.

Dzisiejsze systemy operacyjne zostały zaprojektowane w warunkach, gdy — w dążeniu do maksymalnego wykorzystania sprzętu i wspólnego użytkowania banków danych — projektanci byli zainteresowani w głównej mierze tym, aby uniknąć potencjalnego chaosu, jaki mógłby powstać przy jednoczesnym korzystaniu z systemu przez wielu użytkowników; czyli właściwie za najważniejszą sprawę uznawano niezawisłość systemu. Między niezawisłością systemu i bezpieczeństwem danych istnieją ścisłe związki, jednak nawet doskonała niezawisłość systemu nie gwarantuje absolutnego bezpieczeństwa danych. Jest tak dlatego, że sam mechanizm — system operacyjny — jest subtelny i wrażliwy.

Zagadnienie jest o tyle złożone, że nie można ograniczyć się do rozważania samego tylko SO i oddzielić jego funkcji od struktury („architektury") sprzętu komputerowego.

Zabezpieczenie przed interferencją wzajemną użytkowników zostało rozwiązane niemal idealnie przez zastosowanie koncepcji tzw. *maszyny wirtualnej*. Oparte na niej systemy stwarzają dla użytkownika sztuczne, pozorne (wirtualne), zamknięte środowisko, tak że każdy z wielu współużytkowników odnosi wrażenie wyłącznego użytkowania komputera i SO. Osiąga się to przez przydzielanie pełnej kopii SO każdemu programowi użytkownika. Cały zespół (maszyna wirtualna) jest traktowany przez monitor (program sterujący) jako jeden program. Monitor ten zachowuje się jak system operacyjny, którego jedną z funkcji jest izolowanie od siebie maszyn wirtualnych, zaprogramowanych wewnątrz systemu rzeczywistego.

Podejście takie załatwia sprawę fizycznego dzielenia zasobów komputera pomiędzy różnych użytkowników, ponieważ prowadzi do wyizolowania poszczególnych użytkowników i stworzenia pozornie sytuacji, jak gdyby każdy z nich był jedynym w systemie. Ale jednocześnie podejście to uniemożliwia wspólne użytkowanie lub wymianę danych (zbiorów danych lub programów) między różnymi użytkownikami. Nie załatwia to praktycznego aspektu bezpieczeństwa danych, które nie ma polegać na całkowitym wzbronieniu dostępu, lecz na określeniu modularnych uprawnień dostępu zgodnie z potrzebami, bez ponoszenia przy tym nadmiernego ryzyka.

Wrażliwość systemu w znacznym stopniu zależy w praktyce od rodzaju programów, do jakich mają dostęp użytkownicy systemu.

W najprostszym przypadku użytkownik może tylko wprowadzać dane do istniejącego i ściśle określonego programu (np. systemu gospodarki materiałowej). Użytkownik nie posiada umiejętności programowania i nie ma kontroli nad przebiegiem przetwarzania a wyłącznie nad rodzajem i wartością dostarczanych danych. W takiej sytuacji zagrożenie jest niewielkie.

W drugim przypadku użytkownik może wpływać na przebieg przetwarzania poprzez instrukcje pisane w języku, będącym pewnego rodzaju językiem wyższego rzędu. Jeśli program interpretujący jest starannie zaprojektowany i sprawdzony, zagrożenie jest niemal równie małe, jak w pierwszym przypadku.

Jeśli jednak użytkownik ma dostęp do bardziej ogólnych języków wyższego rzędu, jak COBOL czy FORTRAN, rosną możliwości jego niepożądanej ingerencji w system; jest bowiem znacznie trudniej napisać i sprawdzić kompilatory tych języków gwarantujące niezawisłość i bezpieczeństwo systemu.

Wreszcie, jeśli użytkownik umie posługiwać się assemblerem, tzn. ma dostęp do niemal wszystkich funkcji systemu, zagrożenie jest oczywiście znacznie większe.

Jak wynika z dotychczasowych rozważań, modyfikacja istniejącego SO w kierunku zwiększenia zabezpieczeń jest bardzo trudna, jeśli nie wręcz niemożliwa. Można jednak przewidzieć pewne kierunki, w jakich będą musieli pójść projektanci nowych SO. Jednym z głównych trendów jest rozwijanie *koncepcji jądra* (*kernel*). Chodzi tu o wyizolowanie tych części SO, które sterują dostępem. Utworzone w ten sposób „jądro" będzie na tyle małe, aby można je było szczegółowo zbadać dla realistycznej oceny jego wrażliwości i zmniejszyć szanse wystąpienia błędów.

Drugą obiecującą koncepcją jest architektura systemu oparta na *deskryptorach*, zastosowana już w niektórych systemach (np. MULTICS, opracowany przez „Massachusetts Institute of Technology" wraz z „Honeywell Information Systems"). W systemach tego typu dostęp do zasobów jest realizowany nie poprzez ich adresy fizyczne lub logiczne, lecz za pośrednictwem specjalnych deskryp-

torów. W ten sposób użytkownicy zostają wyizolowani w całkiem niezależnych strefach adresów wirtualnych, zachowując jednak możność wspólnego użytkowania programów i danych, również za pomocą deskryptorów. Na podstawie tej architektury uda się, być może, opracować znacznie bardziej bezpieczny system operacyjny.

Te i podobne koncepcje będą wykorzystywane w przyszłych systemach, w których bezpieczeństwo danych będzie jednym z podstawowych założeń projektowych. Specjaliści przyznają jednak, że i one nie zapewnią absolutnego bezpieczeństwa, i nie należy liczyć na to, że pewnego dnia jakiś producent oprogramowania będzie mógł w kontrakcie zagwarantować klientowi pełne bezpieczeństwo systemu. Można co najwyżej spodziewać się stwierdzenia, że dany system spełnia pewne ściśle określone kryteria.

Funkcje ochronne programów użytkowych

Zanim będzie można mówić o tym, jakie funkcje ochronne spełniać mogą programy użytkowe, należy zastanowić się, jak ustrzec się przed tym, aby programy te same nie stanowiły (celowo lub przypadkowo) zagrożenia dla bezpieczeństwa informacji. W głównej mierze do zmniejszenia częstotliwości występowania błędów programowych przyczyniają się: staranne testowanie programów i wnikliwa kontrola jakości. Wnikliwa kontrola jakości z kolei zależy od ustalenia ściśle egzekwowanych norm („standardów") opracowywania, dokumentowania, modyfikacji i eksploatacji programów. Normy takie ułatwiają również korekcję błędów.

Testowanie i konserwacja (aktualizacja) programów są znacznie ułatwione, jeśli programy zbudowane są modularnie. Obniża to również koszty programowania.

Ważne jest, aby wynikowe kody programów (wersje eksploatacyjne) traktowane były jak wszystkie dane — a więc również z zastosowaniem tych samych środków i metod ochrony. Kod wynikowy przechowywany na taśmie magnetycznej lub wymiennym pakiecie dysków powinien być opatrzony sumami kontrolnymi, bitami parzystości i kontrolą sekwencji bloków w celu uniknięcia utraty kodu lub błędów transferu, które mogą spowodować błędne wykonywanie programu.

Zawarte w programach użytkowych funkcje ochronne, jakie mają one spełniać, będą zależały od stopnia ochrony wymaganego dla przetwarzanych informacji i od stopnia ochrony, jaki już zapewnia sam system operacyjny. Inaczej mówiąc, funkcje ochronne programu użytkowego stanowią uzupełnienie i wzmocnienie tych samych funkcji, realizowanych przez SO.

V. Ochrona informacji w poszczególnych fazach APD

1. Ochrona w fazie projektowania systemu

Przystępując do projektowania nowego systemu (podsystemu) przetwarzania dla określonego zastosowania należy brać pod uwagę następujące cztery główne obszary działania, które mogą wzajemnie na siebie oddziaływać (dodatnio lub ujemnie):

— zespół projektujący,
— opracowywany system użytkowy,
— istniejące i eksploatowane systemy (operacyjne, użytkowe),
— instytucja (przedsiębiorstwo) jako całość.

Wzajemne oddziaływania wymienionych czynników występują przez cały okres projektowania, wdrażania i eksploatacji systemu. W celu śledzenia ich i zapobiegania ujemnym skutkom, wynikającym z niedbalstwa lub złej woli, konieczny jest stały nadzór nad procesem projektowania. Firma IBM w swoich publikacjach zaleca przeprowadzanie ponadto w cyklu projektowania dwóch tzw. *przeglądów bezpieczeństwa (security review)*, a mianowicie: na początku projektu (po analizach wstępnych i opracowaniu założeń) oraz przed rozpoczęciem testowania całości systemu (podsystemu). Do celów tych przeglądów służą specjalne listy kontrolne.

Dokumentacja projektowa

Zespoły projektujące systemy (podsystemy) i pojedyncze programy użytkowe powinny kierować się pewnymi ogólnymi wytycznymi sporządzania dokumentacji.

Ze względu na znaczenie wyraźnego podziału obowiązków i odpowiedzialności, oraz przez wzgląd na zasadę „każdy wie tyle, ile mu potrzeba do wykonywania pracy — ani więcej, ani mniej",

cała dokumentacja systemowa powinna być sporządzana w postaci odrębnych zeszytów problemowych. Szczególnie odnosi się to do dokumentacji eksploatacyjnej. Użytkownik systemu nie musi znać wewnętrznej logiki programów, a operator nie powinien zaglądać do podręcznika programisty.

Część ogólnoopisowa dokumentacji systemowej powinna zawierać pełną listę przewidzianych w poszczególnych programach środków kontroli danych na wejściu i wyjściu (procedur weryfikujących i redagujących).

W dokumentacji każdego podsystemu i programu powinien znajdować się załącznik poufny, zawierający listę procedur zabezpieczających zbiory i dostęp do nich oraz ideowy schemat blokowy, wskazujący gdzie i jak omawiane procedury są stosowane. W szczególności dotyczy to podsystemów i programów eksploatowanych ze zdalnych końcówek (zarówno w trybie dialogowym, jak i wsadowym). Bezpieczeństwo całego systemu zależy od nieujawnienia zawartej tutaj informacji. Załącznik ten jest niezbędny dla celów kontroli wewnętrznej.

Dokumentacja powinna także zawierać zasady działania sprzężeń zwrotnych, występujących w trakcie wdrażania i eksploatacji systemu, a przede wszystkim tryb modyfikacji problemowych (logicznych) oraz tryb wprowadzania zmian w programach. Wszelkie modyfikacje i zmiany muszą być w pełni uzasadnione, udokumentowane, zatwierdzone i zarejestrowane. Wzór przykładowego formularza rejestracji zmian podano w tablicy IV.

Pożądane jest również, aby dokumentacja zawierała wskazówki co do postępowania w przypadku awarii uniemożliwiającej dokonywanie normalnego przetwarzania.

Dokumentacja powinna dawać odpowiedź na pytanie, czy zastosowano takie środki kontroli i weryfikacji danych, jak:

— sumy kontrolne *(hash totals)*,
— sprawdzanie kompletności,
— sprawdzanie formatu,
— sprawdzanie zakresu,
— sprawdzanie sensowności,
— sprawdzanie uporządkowania (sekwencji),
— zliczanie zapisów, znaków i bloków,
— kontrola arytmetyczna sum w wierszach i kolumnach,

TABLICA IV

Wzór formularza rejestracji zmian w programie
(wg *Computer Security Handbook* — praca zbiorowa — Macmillan, N. Jork, Londyn)

Nazwa, opis., ew. numer programu	Numer kolejny zmiany .....
	Zmiana wprowadzana od dnia.....

Zmianę zainicjował ..... dnia .....

Propozycja zmiany zatwierdzona przez ..... dnia .....

Opis celu zmiany lub jej przyczyny

Ocena wartości (efektu) zmiany

Opis dokonanych uprzednio zmian (i ich wpływu na ten i inne programy)

Ocena kosztu przeprowadzenia zmiany

Zatwierdził ..... dnia:

Zmiany dokonał ....

Zmianę sprawdził ....

Wprowadzono informację do dokumentacji ....

Wprowadzono zmianę do instrukcji eksploatacyjnej ....

Inspekcja zmian przez ....

— informacje o wyjątkach (*exception reporting*),
— punkty kontrolne w programach (*check-point/restart*),
— sprawdzanie etykiet zbiorów.

Dokumentacja powinna także informować, w jaki sposób przeprowadza się kontrolę jakości wyjścia z drukarki, czy wszystkie

strony są numerowane, czy przewidziano wskaźnik ostatniej strony, jaka jest liczba kopii i kto je otrzymuje. Jeśli stosuje się formularze z nadrukiem, należy załączyć wzory tych formularzy.

W załączniku poufnym należy również podać, które zbiory oraz w jaki sposób są chronione, gdzie użyto kluczy odczytu i zapisu itp. Należy podać opis procedur sprawdzania uprawnień użytkowników korzystających z końcówek zdalnego dostępu, jeśli takie zostały przewidziane dodatkowo (oprócz istniejących w SO).

Należy także podać czy i w jaki sposób rejestrowane są każdorazowe seanse współpracy końcówek dialogowych z systemem.

Zasady przechowywania i aktualizacji dokumentacji

Przystępując do omówienia tego tematu, należy zdefiniować ściśle kilka pojęć.

Dokumentacja systemu są to dokumenty — w zasadzie w formie konwencjonalnej, ale ewentualnie również w postaci np. plików kart dziurkowanych lub szpul taśmy magnetycznej — które opisują konkretny system informatyczny. Treść i formę dokumentacji systemu definiują ustalone normy i wzorce.

Biblioteka dokumentacji jest to komórka organizacyjna, której zadaniem jest opieka nad dokumentami oraz rejestrowanie ich ruchu, a także ewentualne pomieszczenie, w którym przechowywane są te dokumenty.

Archiwum rezerwowe jest to pomieszczenie, w którym przechowuje się awaryjne wtórniki dokumentacji techniczno-eksploatacyjnej po przyjęciu jej przez komisję odbioru dokumentacji i zatwierdzeniu przez kierownictwo ośrodka APD.

Egzemplarz „żelazny" jest to egzemplarz, który nigdy nie opuszcza biblioteki (najczęściej oryginał dokumentacji).

Kopia archiwalna jest to awaryjna kopia dokumentacji, która przechowywana jest w archiwum rezerwowym.

Kopia robocza jest to kopia wydawana na zewnątrz biblioteki dla celów eksploatacji systemu lub też do prac nad modyfikacją i konserwacją systemu.

Zadaniem biblioteki dokumentacji jest przechowywanie i udostępnianie „żelaznego" egzemplarza dokumentacji.

Po dokonaniu przez komisję odbioru przyjęcia określonego kom-

pletu dokumentacji systemu i przekazaniu go do eksploatacji, żelazny egzemplarz składany jest w bibliotece. Dokumenty otrzymują specjalną sygnaturę, po czym wykonuje się kopię archiwalną, która zostaje złożona w archiwum rezerwowym poza terenem ośrodka APD.

Kopie archiwalne podlegają co najmniej raz na kwartał aktualizacji do stanu identycznego z egzemplarzem żelaznym.

Dla każdego dokumentu w bibliotece zostaje sporządzona metryczka, w której odnotowywane jest kto i kiedy otrzymał kopię roboczą dokumentu. W przypadku aktualizacji dokumentu wszyscy wymienieni w metryczce otrzymują nowe strony do wymiany.

Rzeczą niesłychanie ważną jest ścisła rejestracja każdej kopii sporządzonej z dokumentu lub nośnika magnetycznego: dla kogo sporządzono, na czyje polecenie, kiedy — oraz pokwitowanie (czytelne!). Dokumentacja programu stanowi własność intelektualną, choć dotychczas nie objętą ochroną prawną. Poza tym — sporządzenie kopii może być pierwszym krokiem na drodze do uzyskania nielegalnego dostępu do systemu.

Kopie archiwalne dokumentacji techniczno-eksploatacyjnej systemu operacyjnego i biblioteki programów SO są traktowane analogicznie, jak kopie dokumentacji systemów użytkowych. W szczególności odnosi się to do dokumentów powstałych w wyniku modyfikacji tych programów, dokonywanej przez programistów SO.

Gospodarka dokumentami składającymi się na dokumentację systemów i nośnikami danych powinna być tak zorganizowana, aby dla każdego z nich istniała pełna historia od chwili powstania, uwzględniająca wszystkie zmiany, aktualizacje i statystykę eksploatacyjną.

Zasady organizacji dostępu do systemu

Projektując system należy ustalić równowagę między potrzebą informacji a stopniem dostępu do systemu, jaki będą miały osoby mające zapotrzebowanie na informacje. Idealna byłaby oczywiście sytuacja, kiedy niemal każdy, kto tego potrzebuje, otrzymuje zezwolenie na dostęp do systemu. Lecz środowisko bez ograniczeń nie jest oczywiście środowiskiem zabezpieczonym.

Biorąc pod uwagę drugą skrajność — maksymalne ograniczanie dostępu — nietrudno wyobrazić sobie efekty zbyt ścisłego kontrolowania środowiska, operowania procedurami zabezpieczenia tak surowymi, że tylko wąska grupa operacyjna ma dostęp do systemu, a strumień informacji wejściowej do środowiska APD jest znacznie uszczuplony.

Projekt systemu powinien szczególnie uwzględniać cztery podstawowe czynniki, które wpływają na bezpieczeństwo operacji APD: rozpoznanie użytkownika, sprawdzenie upoważnienia użytkownika, natychmiastowe wykrycie nie upoważnionego dostępu oraz środki nadzoru i kontroli.

System po zweryfikowaniu zapytującego musi sprawdzić, czy ma on prawo otrzymać określoną informację. Wejście do systemu nigdy nie powinno umożliwiać swobodnego dostępu, jaki pozwalałby każdemu użytkownikowi na myszkowanie i losowy dostęp do zbiorów. Każdy zbiór cechuje się odmienną, wyróżnialną wśród innych wrażliwością i powinno to być uwidocznione w tablicy upoważnień, która wskazuje, kto posiada upoważnienie dostępu do określonej części określonego zbioru oraz kto może dokonywać zmian w tych zbiorach.

Natychmiastowe wykrycie intruza powinno wiązać się z zapewnieniem, że zostanie on odrzucony zanim wykorzysta dostęp do zbioru, a nie post factum. Należy również prowadzić rejestr wszystkich usiłowań uzyskania dostępu do zbioru bez upoważnienia, a każde takie usiłowanie powinno automatycznie powodować odpowiednią reakcję. Pierwsze takie zdarzenie może wynikać z przypadkowego błędu, lecz następne usiłowania powinny być dokładnie zbadane, ponieważ według wszelkiego prawdopodobieństwa zostały one podjęte w złych zamiarach.

Drugie lub najdalej trzecie usiłowanie uzyskania dostępu bez zezwolenia powinno spowodować automatyczne wyłączenie terminala danego użytkownika z systemu, z zastrzeżeniem, że tylko SOI może go ponownie włączyć.

Inspekcja systemu powinna być przeprowadzana w taki sposób, aby ujawniała charakterystyczne szczegóły każdego dostępu do systemu. Rejestry, w których zbiera się takie informacje powinny być tworzone przez sam system i powinny być przedmiotem częstej kontroli ze strony SOI. W akcji tej może pomagać sama maszy-

na i właściwie powinna ona okresowo dokonywać kontroli częstotliwości dostępu oraz tak zmieniać rozmieszczenie zbiorów — stosownie do częstotliwości korzystania z nich — aby zapewnić optymalne czasy dostępu.

Kontrolujący powinien zdawać sobie sprawę, że bardzo rzadkie próby uzyskania dostępu do zbioru mogą faktycznie świadczyć o utworzeniu — przez obejście systemu — nowej drogi dostępu do zbioru, nie pozostawiającej śladów.

Nawet najbardziej wrażliwe dane muszą być gdzieś przechowywane i jakoś przetwarzane — a nie można rezygnować z możliwości, jakie daje APD, tylko ze względu na bezpieczeństwo. W komputerach wieloprogramowych z dołączonymi bezpośrednio zdalnymi terminalami podstawową zasadą pracy jest nieprzetwarzanie tajnych informacji jednocześnie z innymi, o bardziej ogólnym charakterze. Innym z podstawowych prawideł, obowiązujących w tym środowisku, jest nieistnienie zdalnych wyjść z tajnych zbiorów. Natomiast odpowiedzialnością za z d a l n e wprowadzanie jako takie — jeśli chodzi o nienaruszalność danych — obarczony jest użytkownik i trudno wymagać, aby ponosił ją odbierający te dane.

2. Ochrona w fazie eksploatacji

Przygotowanie i kontrola danych wejściowych

Przygotowanie i kontrola danych wejściowych zapobiegają przedostawaniu się i przetwarzaniu danych „niedopuszczalnych". Istnieją dwie drogi zabezpieczenia systemu przed niewłaściwymi danymi: uchwycenie ich zanim zostaną przetworzone — czy to ręcznie podczas przygotowywania danych, czy też poddając je sprawdzaniu programowanemu — albo wykrycie na tyle szybko po przetwarzaniu, aby można było jeszcze naprawić powstały błąd.

Występuje tu również istotny element analizy: jak i dlaczego błędne dane przedostały się, i jak tego uniknąć na przyszłość.

1. Kontrola wsadu (partii). Przy eksploatacji systemu komputerowego jednym z podstawowych warunków prawidłowego przetwarzania jest, aby zostały wprowadzone w s z y s t k i e potrzebne

dane. Wyniki przetwarzania — mimo prawidłowego przebiegu tego procesu — nie spełnią założeń systemu, jeśli nie wszystkie istotne dane zostały przetworzone i włączone do sprawozdań wynikowych. Istnieje kilka metod kontroli kompletności wprowadzanych do systemu danych.

Najczęściej stosowaną metodą jest porównywanie dwóch otrzymanych niezależnie sum wsadowych (*batch totals*). Jedna suma wsadowa obliczana jest przez komputer, drugą zaś oblicza się ręcznie (ewentualnie za pomocą sumatorów), nim wsad zostanie wprowadzony do komputera. Sumę tę dołącza się do formularzy z danymi, zanim przekaże się je do zakodowania (perforacji).

Niezależnie od tego można dla każdego cyklu przetwarzania rozpoczynać nową sekwencję numerowania wsadu. Numery wsadów mogą mieć kolejność wzrastającą. Brak kolejnego numeru wsadu będzie oznaczał przeoczenie.

W odniesieniu do systemów, które nie pracują w trybie przetwarzania wsadowego konieczne jest opracowanie innych metod. Może być np. potrzebne otrzymywanie w punkcie kontrolnym (lub u źródła danych) potwierdzenia każdej otrzymanej na wejściu transakcji. Zachodzi wówczas potrzeba dysponowania metodą sprawdzania, czy takie potwierdzenie nastąpiło w każdym bez wyjątku przypadku. Jest to oczywiście pracochłonne, a poza tym zwiększa możliwość błędów (sprawdzania dokonuje człowiek, nie komputer).

2. Wykrywanie błędów i przekłamań. Wśród najważniejszych metod wykrywania błędu należy wymienić tzw. *techniki nadmiarowe*. Wymagają one użycia dodatkowego wyposażenia lub dodatkowych danych. Bez względu na sposób realizacji, zadaniem technik nadmiarowych jest wykrywanie błędów w pracy systemu i stworzenie warunków do korekty możliwie największej liczby tych błędów.

Metodom tym poświęcona jest obszerna literatura. Interesujący przegląd tych zagadnień można znaleźć w publikacji Europejskiego Programu Badawczego Diebolda E-76 (sierpień 1970), pt. *Error Control Coding in Communications and Hardware* [5]).

[5]) Wyd. w przekładzie polskim: *Zastosowanie kodowania do kontroli błędów w transmisji danych oraz sprzęcie*. OBRI, EPBD, Zeszyt 42, Warszawa 1973.

3. Sprawdzanie kolejności. Jeśli dokumenty z danymi wejściowymi są opatrywane kolejnymi numerami, można dokonywać sprawdzania kolejności numeracji dla upewnienia się, że dane wejściowe są kompletne. Niewielka modyfikacja formularzy wejściowych — wprowadzenie kolejnej numeracji — warta jest zachodu. Metoda ta wymaga, aby stanowisko kontroli wejścia podawało komputerowi dwa numery:

a) numer ostatniego dokumentu, przetwarzanego w ostatnim cyklu przetwarzania,

b) numer ostatniego zweryfikowanego dokumentu źródłowego.

System powinien zawierać standardowe programy, sprawdzające czy wczytano wszystkie zweryfikowane dokumenty, wygenerowane od czasu ostatniego cyklu przetwarzania. Dokumenty brakujące (ich numery) powinny znaleźć się na liście kontrolnej. Jeśli nie brak żadnego dokumentu, fakt ten również winien być odnotowany na liście kontrolnej.

4. Kontrola formatu (redakcji). Kontrola formatu (*edit controls*) ma na celu sprawdzenie, czy dane wchodzące do systemu mają postać zrozumiałą dla komputera. Kontroli tej może dokonywać specjalny program redakcji wejścia albo też może ona być dokonywana w czasie przenoszenia danych z kart na taśmę lub dysk, z taśmy na dysk itp. Program ten powinien generować sumy kontrolne, które można będzie porównywać po ukończeniu procesu redagowania.

Sposób przeprowadzania kontroli formatu, jaki powinien być stosowany przez system, zależy od trzech czynników: rodzaju błędów, jakie mogą występować, przydatności określonych metod kontroli oraz kosztu w stosunku do ewentualnych konsekwencji wystąpienia błędów. Po wczytaniu danych do komputera mogą być zastosowane następujące metody kontroli formatu.

Sprawdzenie poprawności znaku. Jeśli pewnemu polu danych podporządkowane są niektóre znaki (np. zero lub spacja), można zaprogramować sprawdzanie, czy nie występują inne znaki.

Sprawdzenie zawartości pola. Jeśli pole może zawierać tylko znaki alfabetyczne lub tylko numeryczne — stosuje się kontrolę zgodności.

Sprawdzenie rozmiarów pola. Jeśli pole danych wejściowych może zawierać tylko określoną liczbę znaków — sprawdzić, czy nie jest ona przekroczona.

Sprawdzenie znaku pola. Jeśli dane pole powinno zawierać zawsze dodatnie (lub ujemne) wartości — sprawdzić znak.

Sprawdzenie cyfry kontrolnej. Cyfra kontrolna ma za zadanie wykrycie, czy nie wystąpiło przestawienie lub podstawienie cyfr w danych liczbowych. Stosowane najczęściej przy identyfikatorach liczbowych.

Kontrola kompletności danych. Sprawdzenie, czy wszystkie pola zapisu, potrzebne do przetworzenia transakcji, są istotnie wypełnione.

Kontrola upoważnienia. Może być pożądane sprawdzenie, czy wydział inicjujący transakcję ma do tego upoważnienie.

Kontrola zgodności. Pola danych mogą być sprawdzane nie tylko pojedynczo, ale i w zestawieniach. Wartości dopuszczalne dla danego pola mogą zależeć od wartości jednego (lub więcej) z innych pól. Może więc być potrzebna seria badań dla różnych kombinacji warunków.

Kontrola sensowności. W odniesieniu do pewnych pól mogą istnieć rozsądne granice maksymalnych lub minimalnych wartości. Kontrola może wykazać, czy wartość pola mieści się w tych rozsądnych granicach.

Kontrola sekwencji zapisów. Jeśli zapisy numerowane są kolejno, kontrola ta wykaże czy nie brak zapisów, lub czy nie występują one dwukrotnie. Lista takich zapisów umożliwi wyjaśnienie przyczyn występowania błędu.

5. Listy odrzuconych pozycji. Jeśli w danych wejściowych występują błędy, powinien zostać wygenerowany raport, podający listę błędnych pozycji z wyjaśnieniem, dlaczego zostały one odrzucone. Pozycje te mogą być listowane w porządku, w jakim wystąpiły lub pogrupowane według rodzajów błędów.

Ważne jest, aby lista błędów dostarczała użytkownikowi informacji wystarczających do przeprowadzenia niezbędnej korekty, bez potrzeby uciekania się do pomocy ośrodka APD.

Lista błędów oraz odrzucone dane powinny być zwrócone komórce inicjującej w celu skorygowania i ponownego przedłożenia. Można również użyć tzw. *zbioru zawieszeń (suspense file).*

6. Zbiory zawieszeń. Kiedy następuje odrzucenie błędnego zapisu, pożądana jest kontrola jego ruchu. Można wykorzystywać w tym celu zbiór zapisów, których przetwarzanie zawieszono. Jest to po prostu zbiór wszystkich odrzuconych, błędnych zapisów. Gdy zapisy te zostaną po skorygowaniu ponownie przedłożone i przyjęte, usuwa się je ze zbioru zawieszeń. Metoda ta umożliwia śledzenie na bieżąco aktualnego stanu pozycji jeszcze nie poprawionych.

Kontrola eksploatacji systemu

W trakcie przetwarzania istnieje możliwość wystąpienia błędów, wynikających z założenia niewłaściwych taśm magnetycznych lub umieszczenia zbiorów lub transakcji na niewłaściwej taśmie lub dysku. Aby zmniejszyć ryzyko wystąpienia tego typu błędów stosuje się specjalne metody, z których najważniejsze zostaną dalej omówione.

1. Etykiety zewnętrzne. Zbiory na kartach, dyskach lub taśmach powinny być wyraźnie oznakowane, tak aby operator mógł zorientować się w ich zawartości. Na etykietach zewnętrznych taśm powinna znajdować się data zapisania, numer zbioru, nazwa zbioru i termin ważności. W dużych ośrodkach taśmy powinny być identyfikowane numerem szpuli.

2. Etykiety wewnętrzne. W celu upewnienia się, że użyty jest właściwy zbiór, że zbiór z aktualnymi danymi nie zostanie przedwcześnie zniszczony oraz że poddano przetwarzaniu kompletny zbiór — na początku i na końcu zbioru powinny być umieszczane etykiety. Etykieta szpuli powinna stanowić część etykiety zbioru, aby zapobiec pomyłkom w razie korzystania ze zbiorów wieloszpulowych.

3. Odtworzenie i wznowienie przebiegu technologicznego. Jeśli następuje odrzucenie programu *(abort)* lub nie zgadzają się sumy kontrolne, potrzebne są procedury wznowienia przebiegu technologicznego *(recovery and restart)*. Jeśli tylko jest to możliwe, programy o stosunkowo długim czasie trwania powinny być pisane w taki sposób, aby skorygowanie błędu występującego pod koniec przebiegu nie wymagało wznawiania całości przebiegu. W niektórych przypadkach najbardziej wskazane jest dzielenie dużych pro-

gramów, realizujących więcej niż jeden proces przetwarzania, na dwa lub trzy odrębne programy; jeśli wystąpi wówczas przerwa w trakcie danego programu, tylko ten program musi być wznowiony po korekcie błędu. Proces ten bywa określany nazwą *check-point* (dosłownie: *punkt kontrolny*). Należy stosować tę metodę, jeśli przewidywany czas wykonywania programu przekracza 30 minut.

Kontrola przetwarzania

Środki kontroli przetwarzania stosowane są w programach systemowych w celu wykrywania błędów spowodowanych przeoczeniem lub niedokładnością programisty, zaniedbaniem obowiązków przez operatora lub będących wynikiem błędów w działaniu sprzętu. Jakkolwiek testowanie programów (i całego systemu) ma na celu prześledzenie wszystkich ścieżek logicznych procesu przetwarzania, jest rzeczą mało prawdopodobną, aby udało się wytestować wszystkie możliwe zbiegi warunków w odniesieniu do dużego programu, zanim zostanie on przekazany do eksploatacji. Dlatego potrzebne są środki kontroli przetwarzania zawarte zarówno w poszczególnych programach, jak i w całym systemie, mające za zadanie wychwytywanie błędów przetwarzania w chwili ich wystąpienia.

Istnieją trzy rodzaje środków kontroli stosowanych dla sprawdzenia poprawności przetwarzania, mianowicie: sprawdzanie zakresu, sumowanie krzyżowe i bilansowanie sum kontrolnych.

1. Sprawdzanie zakresu *(limit test)*. Podobnie jak w przypadku redagowania danych wejściowych, można sprawdzić przebieg przetwarzania za pomocą zaprogramowanych instrukcji, które badają sensowność wyników przez porównanie ich z pewnym zakresem możliwych wartości. Na przykład: płaca netto na liście płacy może być przyrównywana do pewnej górnej granicy. Jeśli wartość na jakimś odcinku wypłaty przekracza tę granicę, jest to prawdopodobnie błąd i należy tę pozycję sprawdzić. Można również w razie wystąpienia pozycji wątpliwych generować komunikaty dla użytkownika systemu o potrzebie sprawdzenia danej pozycji.

2. Sumowanie krzyżowe *(crossfooting test)*. Przebieg sumowania krzyżowego jest podobny do metody ręcznej kontroli, stosowanej w rachunkowości. Poszczególne pozycje sumowane są w ko-

lumnach i wierszach niezależnie od siebie, a następnie uzyskuje się sumę „krzyżową" przez zsumowanie kolumny sum cząstkowych, po czym porównuje się ją z takąż sumą dla wiersza sum cząstkowych. Albo na przykład na liście płac podsumowuje się zarobek brutto, zarobek netto i wszystkie potrącenia. Następnie oblicza się niezależnie sumę zarobków netto przez odjęcie od sumy zarobków brutto wszystkich sum dla poszczególnych pozycji potrąceń. Niezgodności oznaczają wystąpienie błędów w procesie przetwarzania.

3. Bilansowanie sum kontrolnych *(control total balancing)*. Sumy kontrolne mogą być stosowane w celu sprawdzenia przetwarzania danych wewnątrz systemu. Na przykład sumy kontrolne na wyjściu programu redagującego powinny być użyte jako sumy kontrolne wejścia dla programu aktualizacji i powinny bilansować się z sumami kontrolnymi na wyjściu programu aktualizacji.

Sumy kontrolne uzyskiwane w trakcie przetwarzania powinny mieć taką postać, aby — jeśli to tylko możliwe w danym zastosowaniu — mogły być porównywane z sumami kontrolnymi otrzymanymi w procesie kodowania (perforowania) danych lub wprowadzania ich po raz pierwszy do systemu.

Kontrola wyjścia

Kontrola ta zapewnia poprawność i dokładność wyników przetwarzania oraz terminowe dostarczanie dokumentów wynikowych w ręce osób upoważnionych — i nikogo innego.

Podstawowe zasady kontroli wyjścia można by ująć następująco:

1. Wszystkie dane wyjściowe powinny być poddane weryfikacji. Polega ona w zasadzie na sprawdzeniu, czy sumy kontrolne zbiorów wejściowych plus sumy kontrolne danych aktualizujących równają się sumom kontrolnym zbiorów wynikowych.

2. Weryfikacja wyjścia powinna należeć do obowiązków odrębnego zespołu kontroli jakości, który nadzoruje również korektę błędów, sprawdza sensowność danych wynikowych i czuwa nad prawidłową dystrybucją dokumentów wyjścia.

3. Wszystkie wydruki powinny mieć co najmniej dwie daty: datę sporządzenia oraz datę końca okresu sprawozdawczego (np. dane na dzień 30 czerwca 1977 r.).

4. Jeśli w chwili sporządzania wydruku brakowało pewnych danych — powinno to być wyraźnie stwierdzone.

5. Na każdej stronicy wydruku powinien znajdować się pełny nagłówek.

6. Na każdej stronicy powinien być umieszczony jej numer. Ponadto na ostatniej stronicy powinna znaleźć się informacja: „ostatnia stronica".

7. W wydruku nie powinno być stronic pustych.

8. W nagłówku wydruku powinna być podana liczba sporządzonych kopii.

Oczywiście, ta sama informacja powinna znajdować się w instrukcji operatorskiej eksploatowanego systemu.

Testowanie i wdrażanie systemów aplikacyjnych

Końcowa faza procesu projektowania systemu — zaczynająca się od testowania systemu jako całości i konwersji zbiorów, a kończąca się pierwszymi cyklami przetwarzania eksploatacyjnego — należy do szczególnie krytycznych. Była o tym mowa w rozdziale trzecim. Tu nieco szerzej zostanie potraktowane zagadnienie tworzenia zbiorów.

Tworzenie zbiorów powinno być dokonywane z dostatecznym wyprzedzeniem w czasie, tak aby można je było bardzo dokładnie sprawdzić. Z chwilą umieszczenia zbioru po raz pierwszy na nośniku magnetycznym jest absolutnie niezbędne sporządzenie pełnego wydruku tego zbioru i sprawdzenie go pozycja po pozycji. Jest to praca bardzo uciążliwa i czasochłonna, nie wolno jednak z niej zrezygnować. Należy dokładnie przeanalizować wszystkie niezgodności między dotychczasowymi dokumentami prowadzonymi ręcznie, a zbiorami komputera. Czasem okazuje się, że błąd powstał w starych zbiorach i trzeba go prześledzić aż do źródła. Wszelkie poprawki w zbiorach danych powinny być dokonywane za pomocą normalnego programu aktualizacji, przewidzianego w systemie, a nie przez użycie specjalnie opracowanych procedur. W ten sposób kontroluje się zarazem prawidłowość działania programów aktualizujących.

Upewnienie się, że nowo tworzone zbiory są bezbłędne — jest niesłychanie ważne. Dawne, prowadzone ręcznie kartoteki nie

mogły być bezbłędne, choćby były prowadzone nadzwyczaj skrupulatnie. Czasem liczba błędnych pozycji dochodzi do 10%. Zdarza się, że fakt ten jest podawany jako argument przemawiający za celowością komputeryzacji. Naturalnie proces przenoszenia danych na nowe formularze, a następnie np. na karty dziurkowane, przyczynia się do dalszego wzrostu liczby błędów.

Rozpoczynanie rutynowego przetwarzania na niezbyt dokładnie sprawdzonych danych wejściowych jest bardzo ryzykowne i nie wolno do tego dopuszczać. Sporządzanie wydruków i kontrola wyjścia powinny być szczególnie staranne w ciągu kilku pierwszych cykli pracy systemu. Istnienie nie wykrytych błędów w programach i w danych wejściowych jest nie tylko prawdopodobne. Jest praktycznie pewne.

Kopie awaryjne

Była już uprzednio mowa o archiwalnych kopiach dokumentacji systemu, przechowywanych jako kopie awaryjne na innym terenie, nie podlegającym tym samym zagrożeniom co teren ośrodka APD. Kopie awaryjne powinny być sporządzone zarówno dla programów (kody źródłowe i kody wynikowe), jak i dla danych (zbiory podstawowe — *master files* i zbiory aktualizujące *transaction files*), umieszczonych na nośnikach w postaci taśm i dysków magnetycznych lub taśm i kart perforowanych. W przypadku jakiejkolwiek awarii systemu umożliwi to odtworzenie lub korektę danych i powrót do punktu, w którym przetwarzanie zostało przerwane. W odniesieniu do zbiorów na taśmach stosuje się zazwyczaj zasadę zachowywania starego zbioru podstawowego po każdej dokonanej aktualizacji. Najświeższa kopia zbioru podstawowego — to syn, starsza — ojciec, poprzednia — dziad; tworzy się w ten sposób tyle generacji, ile wymaga tego natura systemu i polityka przedsiębiorstwa. W przypadku dysków — zazwyczaj zapisy zbioru aktualnego zastępują stare zapisy, a więc po zakończeniu przetwarzania stary zbiór nie istnieje.

Stosowana jest więc procedura wykonywania kopii na taśmie *(dump)* albo po zakończeniu przetwarzania, albo pod koniec dnia (zmiany) oraz — niekiedy — dodatkowo dla wszystkich aktualizowanych zbiorów przy końcu tygodnia. W każdym przypadku od-

tworzenie zbiorów oznacza powtórne wykonanie programów, przy czym początek cyklu sięga tak daleko wstecz, jak jest to konieczne.

Oczywistą konsekwencją utrzymywania kopii awaryjnych są dodatkowe koszty (czas pracy maszyny, koszt nośników, koszt składowania i ewidencji), które muszą być bilansowane przez ewentualne straty do poniesienia w przypadku zniszczenia lub uszkodzenia zbiorów. Ponieważ nawet w najlepiej prowadzonym ośrodku zdarzają się mniejsze lub większe awarie, tworzenie i przechowywanie kopii awaryjnych uznawane jest powszechnie za nieodzowny akt przezorności. Sposób przechowywania kopii dyktowany jest przez dwa podstawowe czynniki:

1. Ważne zbiory muszą być tak magazynowane, aby co najmniej jedna kopia przetrwała wszelkie możliwe katastrofy.

2. Jeśli zbiory te zawierają wrażliwe informacje, muszą być także chronione przed kradzieżą (należy pamiętać, że na ogół szafy ogniotrwałe nie stanowią wystarczającego zabezpieczenia przed włamaniem).

Ponadto archiwum musi zapewniać warunki przechowywania zalecane przez producenta nośników (klimatyzacja, czystość). Procedury gospodarki kopiami awaryjnymi powinny być ściśle kontrolowane, a ich ewidencja zawsze prowadzona na bieżąco.

Zbiory zawierające bibliotekę kodów źródłowych oraz kodów wynikowych muszą być uważane za równie ważne, jeśli nie ważniejsze niż zbiory danych, nie tylko ze względu na koszty ich uzyskania. Kopie awaryjne kodu wynikowego są szczególnie potrzebne, ponieważ zbiór ten jest na ogół użytkowany przez komputer przez więcej godzin w każdym tygodniu, niż jakiekolwiek inne zbiory, a tylko wówczas, kiedy komputer jest wyłączony (jeśli bywa wyłączany) zbiory te będą zabezpieczone w szafie ogniotrwałej lub sejfie. Z tego samego powodu zbiory te są bardziej narażone na błędy zapisu/odczytu i na uszkodzenia. Dlatego też kopie muszą być regularnie sporządzane — i to najlepiej dwie: jedna będąca zawsze pod ręką, do natychmiastowego użytku w razie uszkodzenia roboczej, a druga w oddalonym archiwum.

Zasady bezpiecznej gospodarki nośnikami

1. Gospodarka kartami perforowanymi. Karty powinny być składowane w oryginalnych kartonach. Zużywać je należy na zasadzie

„pierwsze przyszły — pierwsze wychodzą". Karty, które jakiś czas znajdowały się w skrajnych dopuszczalnych warunkach klimatycznych (temperatura, wilgotność) powinny być przed użyciem przetrzymane przez kilka godzin w klimacie pomieszczeń komputera.

Po wyperforowaniu karty powinny leżeć w tacach, przyciśnięte sprężynującym uchwytem. Karty, w których stwierdzono uszkodzenie lub błąd perforacji powinny być bezzwłocznie wymienione. Kierownik zmiany powinien na karcie odnotować powód jej wycofania i zwrócić ją do sekcji kontroli wejścia, gdzie powinna być zachowana aż do czasu, kiedy dany przebieg przetwarzania *(job, run)* zostanie uznany za pomyślnie zakończony.

Jeśli karta nie wejdzie do czytnika przy pierwszej próbie, zarówno tę, jak i następną kartę należy zreprodukować przed następnym wprowadzaniem do czytnika. Karty reprodukowane powinny różnić się kolorem.

Po użyciu karty powinny być przechowywane przez minimum czasu, koniecznego dla zabezpieczenia. Karty zużyte należy wyrzucać do specjalnie na ten cel przeznaczonego pojemnika.

Jeśli karty przeznaczone są dla innego ośrodka, powinny być ciasno zapakowane w sztywne pudła kartonowe. Wolną przestrzeń należy wypełnić plikiem kart zużytych, ściągniętych taśmą i oznaczonych jako makulatura. Pliki kart powinny być opatrzone wyraźnym symbolem identyfikacyjnym na grzbiecie oraz na pierwszej i ostatniej karcie — najlepiej flamastrem.

Podobne zasady obowiązują przy gospodarce taśmą papierową.

2. Gospodarka papierem do drukarek. Zapas roboczy papieru do drukarek przed użyciem powinien przez co najmniej 48 godzin znajdować się w tych samych warunkach klimatycznych, co komputer. Nie należy przechowywać papieru blisko grzejników ani w pomieszczeniach wilgotnych, ani też w bezpośrednim blasku słońca.

3. Gospodarka taśmami magnetycznymi. Taśmy powinny stale znajdować się w specjalnych pojemnikach i być wyjmowane tylko na czas załadowania. Pierścień zapisu należy zdejmować ze szpuli wyjściowej natychmiast po rozładowaniu — chyba że taśma użytkowana była wyłącznie jako tymczasowa (robocza).

Nie można dopuszczać do tego, aby luźne końce taśmy leżały na podłodze lub innych powierzchniach, z których mogą zebrać

kurz. W razie upuszczenia szpuli, powinna ona zostać przekazana obsłudze konserwatorskiej do sprawdzenia, zanim zostanie dopuszczona do dalszego użytku.

Transport taśmy powinien odbywać się w specjalnie do tego przeznaczonych pudłach (walizeczkach), a po transporcie powinna ona leżeć w środowisku komputera przez co najmniej 24 godziny przed użyciem.

4. Gospodarka dyskami magnetycznymi. Wymienne pakiety dysków nie założone na trzpień muszą być stale przechowywane w swoich szczelnie zamkniętych pojemnikach. Dolna część pojemnika powinna być przytwierdzona natychmiast po zdjęciu pakietu. Pojemniki należy utrzymywać w doskonałej czystości. Jeśli pakiet zostanie upuszczony lub uderzony, nie wolno w żadnych okolicznościach zakładać go na trzpień przed dokładnym zbadaniem przez konserwatora komputera. Podczas transportu należy pojemnik z dyskami umieścić w worku foliowym, a następnie w kartonie (najlepiej oryginalnym, fabrycznym). Po przewiezieniu pakiet powinien znajdować się przez co najmniej dwie godziny przed użyciem w klimacie sali komputera.

3. Szczególne problemy ochrony w systemach o zdalnym dostępie

Wzrastający zakres zastosowań systemów APD, do których możliwy jest dostęp ze zdalnych terminali, przyczynia się do zwiększenia wrażliwości systemu w porównaniu z wyodrębnionymi, zamkniętymi ośrodkami, jakie przeważały dotychczas.

Systemy, o których mowa, można podzielić na trzy obszerne klasy:

1. Systemy obsługujące terminale i umożliwiające pracę dialogową (wyłącznie lub obok przetwarzania wsadowego).

2. Systemy pracujące na bieżąco *(real-time)*. Typowym przykładem jest tu system rezerwacji miejsc lotniczych.

3. Systemy wchodzące w skład sieci przetwarzania rozproszonego *(distributed processing networks)*.

Wszystkie dotychczas omawiane środki zabezpieczające odnoszą się w głównej mierze do centralnych instalacji komputerowych

oraz w znacznym stopniu do końcówek używanych do przetwarzania wsadowego. Inaczej jednak sprawa wygląda, jeśli chodzi o terminale do pracy interaktywnej. Potrzebne tu są dodatkowe środki zabezpieczenia, ponieważ:

— terminal jest zazwyczaj zlokalizowany poza terenem, objętym władzą kierownictwa ośrodka APD,

— nadzór nad pracą komputera obsługującego terminale jest znacznie trudniejszy,

— w grę wchodzi zazwyczaj korzystanie z tych samych zbiorów przez różnych użytkowników,

— ośrodek komputerowy często ma za zadanie świadczenie usług na rzecz szeregu różnych odbiorców, czasem reprezentujących sprzeczne interesy.

W odniesieniu do systemów o zdalnym dostępie można wyróżnić następujące podstawowe grupy zagrożeń:

1. Przypadkowe błędy użytkownika. Użytkownik może mimo woli uzyskać dostęp do informacji, do której nie jest uprawniony, przez podanie ważnego hasła, nazwy zbioru, instrukcji, nie będąc świadomym ich znaczenia. Może również uzyskać fragmentaryczną informację z pamięci operacyjnej, jeśli zażąda np. wydruku zawartości jej komórek.

2. Wady i błędy systemu. System może omyłkowo dostarczyć informacji, której użytkownik nie żądał. Może również umożliwić użytkownikowi zmianę informacji, której nienaruszalność powinna być zachowana.

3. Rozmyślne „podsłuchiwanie" ruchu danych za pomocą urządzeń technicznych (szczególnie przy transmisji danych).

4. Rozmyślne pogwałcenie niedostępności systemu za pośrednictwem normalnego terminala, np. przez podszywanie się pod upoważnionego użytkownika.

Terminale zdalnego dostępu, które nie są strzeżone, mogą zostać wykorzystane przez osoby nie upoważnione do celów prywatnych lub przestępczych. Szczególnie terminale umożliwiające dostęp do danych, którymi gospodaruje system, powinny znajdować się w zamykanym i strzeżonym pomieszczeniu lub być zaopatrzone w wyłączniki zasilania uruchamiane za pomocą klucza, tak aby ktoś nie posiadający klucza nie mógł uruchomić terminala. Powinna również istnieć metoda identyfikacji przez system osoby

obsługującej terminal. Fakt, że w pamięci systemu jest zarejestrowane, kto konkretnie wykonywał jakie operacje, odczytywał jakie dane lub jakie modyfikował zbiory, jest na ogół skutecznym odstraszeniem od użycia terminala w sposób niedozwolony.

Kontrola wejścia

Szczególnie w systemach należących do pierwszych dwóch klas wymienionych uprzednio, ale także w przetwarzaniu rozproszonym, zasadniczą rolę odgrywa interaktywna współpraca z komputerem. Nie mają tu więc zastosowania omawiane już metody kontroli wejścia dla przetwarzania wsadowego. Dane do systemu są wprowadzane ze zdalnych terminali przez operatorów o różnym poziomie wiedzy fachowej. W tych warunkach programy redakcji wejścia mają decydujące znaczenie. Ogólnie biorąc, wymaga się aby każdy dialog między maszyną (systemem) a terminalem był inicjowany przez komunikaty zawierające takie informacje, jak identyfikacja terminala i użytkownika, hasła, rodzaj transakcji itp. Z chwilą gdy system potwierdzi uprawnienia zgłaszającego się, użytkownik ten rozpoczyna transmisję danych, a następnie podprogramy redagujące wejście powinny przeprowadzić weryfikację wprowadzanych danych.

Podprogramy redagujące są różne, zależnie od systemu, w którym mają być użyte. W systemach pracujących na bieżąco najbardziej pożądaną cechą jest szybka odpowiedź, a redagowanie zabiera czas. Z drugiej jednak strony nieścisłe dane, jeśli zostaną dopuszczone do systemu, mogą spowodować zniekształcenie zbiorów. Wielu projektantów systemów pracujących na bieżąco będzie wolało poświęcić czas uzyskiwania odpowiedzi na rzecz zapewnienia ścisłości danych. Podprogramy redagujące w systemach zdalnego dostępu kontrolują upoważnienie użytkownika, sprawdzają poprawność danych wejściowych, zapisują komunikaty w rejestrze oraz wprowadzają pozycje do rejestru badań kontrolnych.

Niezależnie od możliwości wystąpienia błędów z winy operatora terminala, następna przyczyna ich pojawiania się może wynikać z faktu przesyłania danych do komputera poprzez łącza telekomunikacyjne. W celu zapewnienia wiernego (nie zniekształconego) odbioru komunikatu konieczna jest dokładna kontrola bitów parzystości oraz sum kontrolnych.

Kiedy użytkownik zgłasza się do systemu zdalnego dostępu, zasadnicze znaczenie ma zakres jego upoważnień. Będzie on zależeć od takich względów, jak przeszkolenie, stanowisko w przedsiębiorstwie oraz rodzaj potrzebnych w związku z wykonywaną pracą informacji. Upoważnienie może zezwalać na dostęp do zbioru w celu jego aktualizacji albo tylko w celu odczytu danych. Dostęp może być ograniczony tylko do pewnych zapisów w zbiorze lub nawet do pewnych pól w zapisie. Na przykład użytkownik może mieć zezwolenie na dostęp do zbioru zawierającego dane personalne, lecz nie na dokonywanie w nim zmian, albo też wolno mu żądać nazwisk i adresów niektórych pracowników, lecz może nie mieć prawa przeglądania ich zarobków ani oceny wydajności, nawet jeśli zapisy zawierające nazwiska i adresy zawierają także te dane.

Fakt udzielenia dostępu do zbioru jest odnotowywany w rejestrze dostępów lub transakcji wraz z symbolem upoważnienia oraz informacją o tym, jakie operacje były na zbiorze wykonywane. Tego rodzaju rejestr może być nieocenioną pomocą w czasie dokonywania inspekcji przez audytora oraz w przypadku konieczności rekonstrukcji zbioru z powodu zaistniałych i stwierdzonych zniekształceń.

Użytkownicy wywołujący programy w systemie zdalnego dostępu prezentują różny stopień przygotowania technicznego oraz zróżnicowane potrzeby w odniesieniu do danych i zbiorów. Niektórym z użytkowników można dać sporą dozę swobody manipulacji na zbiorach, podczas gdy inni muszą być w tym zakresie ograniczeni. Środki zabezpieczenia stosowane w systemach przetwarzających zdalnie mają przede wszystkim na celu strzeżenie nienaruszalności zbiorów.

Kiedy użytkownik korzysta z dostępu do zbioru, mając do tego upoważnienie, powinien być włączany specjalny przełącznik „blokady", który zapewni nieosiągalność danego zbioru dla innych użytkowników aż do chwili, gdy zbiór zostanie zwolniony.

Kontrola wyjścia

W systemie pracującym ze zdalnym dostępem kontrola nad wyjściem jest sprawowana przez system, tj. upoważnienie użytkowni-

ka wskazuje również, jakie materiały wyjścia może, a jakich nie może on otrzymać.

Jak widać z przeprowadzonych rozważań, systemy zdalnego dostępu znacznie trudniej jest kontrolować i zabezpieczać. Jest jednak pewien aspekt, który silnie przemawia na korzyść systemów pracujących interaktywnie. Chodzi o to, że przy właściwie zaprojektowanym i prawidłowo prowadzonym dialogu większość błędów można uchwycić na bieżąco, w chwili kiedy operator je popełnia. Wówczas błąd lub niezgodność można skorygować od razu. Jeśli kwestionowana jest poprawność jakiejś pozycji — np. abonent kwestionuje wysokość otrzymanego rachunku telefonicznego — sprawdzenie tej pozycji może zostać dokonane od ręki. Zbędne tu jest prowadzenie „zbiorów zawieszeń", o których była mowa przy przetwarzaniu wsadowym.

Bazy danych

Większość systemów o bezpośrednio dołączonych zdalnych terminalach dysponuje również bezpośrednimi zbiorami danych, często nazywanymi, nieco dowolnie, *bazami danych*.

Zintegrowana baza danych różni się nieco od biblioteki zbiorów. Wobec tego właśnie, że jest ona zintegrowana, system operacyjny „traktuje" ją jako pojedynczy zbiór, mimo że może ona zawierać pozycje bardzo różnorakiej natury i wrażliwości (poufności), powiązane w logiczne łańcuchy. W tym przypadku pojęcie „użytkownik" (twórca zbioru) zostaje zastąpione pojęciem „administrator bazy danych"; jednym z głównych obowiązków administratora bazy danych jest sterowanie dostępem i uprawnieniami wszystkich korzystających z tej bazy.

Przy takich założeniach strukturalnych opisywane dotychczas zasady gospodarki zbiorami nie są wystarczające do zdefiniowania różnych uprawnień do dostępu. Rozwiązanie tego problemu zaproponowała w 1969 r. specjalna grupa robocza utworzona w USA do spraw systematyzacji baz danych („Data Base Task Group" — DBTG/CODASYL). Polega ono na zastosowaniu koncepcji „podschematów" *(sub-schemas)*. Nazwa „schemat" obejmuje całą bazę danych. Dostęp do niej ma jedynie system operacyjny. Koncepcja schematu i podschematów umożliwia „założenie zamka" na wszy-

stkie dane znajdujące się w bazie, czyli na każdy element *(item)*, każdą strefę *(item zone)*, każde połączenie logiczne *(chaining between items)*.

Administrator bazy danych przydziela każdemu użytkownikowi (lub programowi użytkownika) odpowiedni podschemat. Podschemat ten odzwierciedla obraz części bazy danych, dostępnej dla tego użytkownika (tak użytkownik ma „widzieć" bazę danych), a jednocześnie stanowi definicję uprawnień dostępu do danych, zawartych w bazie. Należy zauważyć, że stosowalność metody podschematów nie ogranicza się tylko do zintegrowanej bazy danych — można ją zastosować do każdego innego rodzaju zbiorów, np. do zbiorów sekwencyjnych.

Na rynku można znaleźć wiele rozwiązań pakietów zarządzania bazami danych (DBMS — DATA BASE MANAGEMENT SYSTEMS); wiele z nich — jak np. IDS firmy Honeywell, DMS firmy UNIVAC — oparto na koncepcji DBTG/CODASYL. Przy wyborze rodzaju DBMS z punktu widzenia ochrony informacji należy kierować się przede wszystkim dwoma kryteriami:

a) jak rozwiązany jest problem hierarchizacji dostępu do grup zapisów, zapisów, poszczególnych pól w zapisach oraz połączeń między nimi,

b) jakie możliwości wznawiania przetwarzania i odtwarzania zbiorów *(restart and recovery)* zapewnia dany DBMS w przypadku uszkodzenia zbiorów i wystąpienia błędów.

Błędy transmisji

Komputery uczestniczące w zdalnym przetwarzaniu muszą być wyposażone w specjalne pakiety oprogramowania, obsługujące transmisję danych. Bez względu na zakres i stopień kompleksowości, każdy z takich pakietów musi spełniać pewne minimum wymagań z punktu widzenia ochrony informacji. Często pakiety tej kategorii tworzą podzespół uzupełniający systemu operacyjnego. Bywają one nazywane „metodą dostępu" *(access method)* systemu operacyjnego. Najbardziej znanymi przykładami takich pakietów są BTAM, QTAM i TCAM firmy IBM. Niektóre z dostępnych na rynku pakietów zaprojektowano pod kątem obsługi zarazem bazy danych i procesów transmisji danych (pakiety typu DBDC — Data Base/Data Communications).

Elementarny system pracujący w trybie *on-line* musi realizować następujące podstawowe funkcje z zakresu ochrony danych:

1. Sprawdzanie czy nie występują błędy, zarówno w znakach za pomocą kontroli parzystości, jak i w komunikatach za pomocą kontroli redundancji wzdłużnej (np. analiza kontrolnych znaków wielomianowych).

2. Redagowanie komunikatów — w miarę potrzeby. Na przykład operator może popełniać błędy podczas uderzania w klawisze albo cofania karetki lub błędy polegające na wymazaniu znaków. Komunikat musi zostać tak przeredagowany, aby uzyskał formę odpowiednią do przetwarzania. Znaki kontrolne muszą zostać rozpoznane i usunięte.

Funkcje te mogą być realizowane przez główny komputer, powoduje to jednak obniżenie jego sprawności. Dlatego też zazwyczaj część tych funkcji realizuje „inteligentny" terminal. Większość pakietów transmisji danych ma jednak znacznie bardziej rozbudowane funkcje ochronne; niektóre z nich zostaną pokrótce omówione.

Wznowienie pracy po uszkodzeniach

1. Uszkodzenie linii. W przypadku uszkodzenia łączy transmisji danych lub końcówek, program może zapisać odpowiednią informację, ułatwiającą wznowienie pracy po naprawie.

2. Kolejna numeracja komunikatów. Komunikaty mogą być opatrywane kolejnymi numerami u źródła *(front-end)*, aby ułatwić wznowienie pracy po uszkodzeniu. Kolejne numery mogą być podawane operatorom terminali.

3. Pomoc w przypadku uszkodzenia centralnego komputera. Oprogramowanie komputera sterującego linią transmisyjną może zarejestrować dane, potrzebne do wznowienia pracy przez centralny komputer po jego naprawieniu. Może również automatycznie przesyłać odpowiednie informacje dla operatorów.

4. Procedury wznowienia. Powinny być napisane specjalne programy, ułatwiające wznawianie pracy po awariach. Mogą one korzystać z rejestru komunikatów oraz z systemu kolejnej numeracji.

5. Diagnostyka. Prawidłowość funkcjonowania różnych części

systemu może być sprawdzana za pomocą programów diagnostycznych, zawartych w centralnym komputerze. Prawidłowe działanie końcówki i jej połączenia z komputerem może być sprawdzane przez wywołanie z terminala programu diagnostycznego, który sprawdzi wszelkie możliwe okoliczności.

6. Sprawdzanie w pętli *(cross-patching)* polega na tym, że sygnały z wyjścia komputera nie są kierowane bezpośrednio do wejścia terminala, lecz najpierw przebiegają w pętli wyjście/wejście komputera. Rozwiązanie to (wysłanie danych i natychmiastowe ich przejęcie) ma na celu sprawdzenie, czy funkcje nadawania i odbioru komputera działają prawidłowo. Zastosowanie takiej metody umożliwia stwierdzenie przyczyny złego funkcjonowania sprzętu, w związku z czym program automatycznej realizacji tej funkcji oddaje niezwykle cenne usługi.

Kontrola dostępu

Dwa aspekty oprogramowania procesu transmisji danych, których uwzględnienie jest pożądane z punktu widzenia bezpieczeństwa, to:

1. Możliwość jednoznacznego zidentyfikowania terminala, nawiązującego z danym komputerem łączność.
2. Możliwość zidentyfikowania osoby obsługującej ten terminal.

Terminale zbudowane z uwzględnieniem wymogów bezpieczeństwa mają możliwość przesłania swojego numeru identyfikacyjnego do komputera. Komputer może sprawdzić ten numer w chwili otrzymania zapytania. W oprogramowaniu komputera może być uwzględnione sprawdzanie — przed wysłaniem odpowiedzi do terminala — tożsamości urządzenia, do którego odpowiedź ta będzie transmitowana.

Użytkownik terminala może być rozpoznawany na różne sposoby; najczęściej identyfikacja polega na sprawdzeniu przez komputer zastrzeżonego klucza lub hasła, podanego przez użytkownika. Hasło zmieniane jest w nieregularnych odstępach czasu. Użytkownik może też włożyć do czytnika terminala swoją kartę identyfikacyjną, co spowoduje, że przesłany zostanie numer użytkownika. Program sprawdza, czy dany użytkownik uprawniony jest do wykonywania operacji, które go interesują.

Szyfrowanie i rozszyfrowywanie. W celu uchronienia „wrażliwych" danych przed podsłuchem lub przypadkowym niewłaściwym skierowaniem może być stosowana kryptografia. Oprogramowanie transmisyjne może dokonywać zaszyfrowywania i rozszyfrowywania komunikatów.

Nadzór nad bezpieczeństwem. W razie wystąpienia objawów naruszenia bezpieczeństwa oprogramowanie może automatycznie wyłączyć daną końcówkę i powiadomić SOI o zaistniałej sytuacji zagrożenia. Wszystkie przypadki potencjalnego zagrożenia powinny być przez program rejestrowane dla potrzeb przyszłej analizy lub kontroli.

W wielu programach transmisji danych nie są jeszcze uwzględnione funkcje zabezpieczające. W przyszłości jednak będą one coraz powszechniej stosowane.

Dialog człowiek-maszyna

Niektóre funkcje związane z dialogiem człowiek—maszyna mogą być wbudowane w pakiety oprogramowania. Te funkcje jednakże — bardziej niż inne, dotychczas omówione — mogą być uzależnione od konkretnego zastosowania.

1. Kontrola sensowności. W odniesieniu do pewnych pól mogą zostać ustalone dopuszczalne granice wartości, w celu ułatwienia wychwytywania błędów operatorskich.
2. Kontrola kompletności. Zapis może być składany pozycja po pozycji, a następnie sprawdzany, czy jakiejś pozycji nie pominięto.

Ochrona linii transmisyjnych

Ochrona fizyczna w systemach o zdalnym dostępie jest naturalnie znacznie trudniejsza niż w zamkniętych systemach, zlokalizowanych na jednym terenie. Dane przesyłane są do i z komputera za pomocą linii transmisyjnych, biegnących najczęściej przez tereny nie podlegające „władzy" ośrodka APD i korzystających z jego usług użytkowników. Oprócz zwiększonego tym sposobem zagrożenia fizycznego linii przesyłowych (przez uszkodzenia mechaniczne, ogień, wodę itp.) występuje dodatkowo zwiększenie zagrożenia podsłuchem takiej linii. Podsłuch może być pasywny

bądź aktywny. Podsłuch *pasywny* polega na włączeniu się w sposób dowolny (ale niezauważalny) do linii transmisji danych i przechwytywaniu przekazywanych tą linią sygnałów. Przejmowanie w ten sposób danych nie wiąże się z dużymi kosztami (można np. użyć do rejestracji sygnałów taniego magnetofonu) i jest stosunkowo proste. Jego największą niedogodnością jest jednakże — zazwyczaj nieunikniona — konieczność wyczekiwania godzinami na informację, która może okazać się użyteczna. Ale jest to jednocześnie sposób na zdobycie identyfikatorów i haseł, które umożliwią następnie dostęp do systemu z legalnego terminala.

Inaczej przedstawia się sprawa podsłuchu *aktywnego*. Wymaga on dysponowania terminalem i modemem kompatybilnymi z terminalami i modemami podsłuchiwanego systemu. Wymaga również dobrej znajomości tego systemu i zaawansowanych umiejętności technicznych i programistycznych. Źródła zachodnie wymieniają szereg szczególnie pomysłowych sposobów aktywnego podsłuchu, jak np. metoda *piggyback* (w dosłownym tłumaczeniu „na barana"), polegającą na przechwytywaniu transmisji dzięki temu, że terminal podsłuchujący generuje komunikaty analogiczne do tych, jakie występują normalnie w seansie dialogowym podsłuchiwanego systemu. Wykorzystywane w tym przypadku może być to, że często użytkownik przez dłuższe okresy „milczy" między otwarciem seansu a wyłączeniem się. W tych okresach podsłuchujący może z powodzeniem wchodzić w rolę legalnego użytkownika, a nawet może przechwycić oraz wygasić sygnały zakończenia dialogu i kontynuować pracę, kiedy prawdziwy użytkownik wyłączy się. Metody te należy uznać za teoretycznie możliwe oraz technicznie wykonalne, jednak bardzo kosztowne i trudne w realizacji, szczególnie jeśli identyfikatory, hasła i klucze dostępu do zbiorów są konsekwentnie stosowane, a także często zmieniane.

Linie transmisyjne bywają: prywatne, dzierżawione i publiczne.

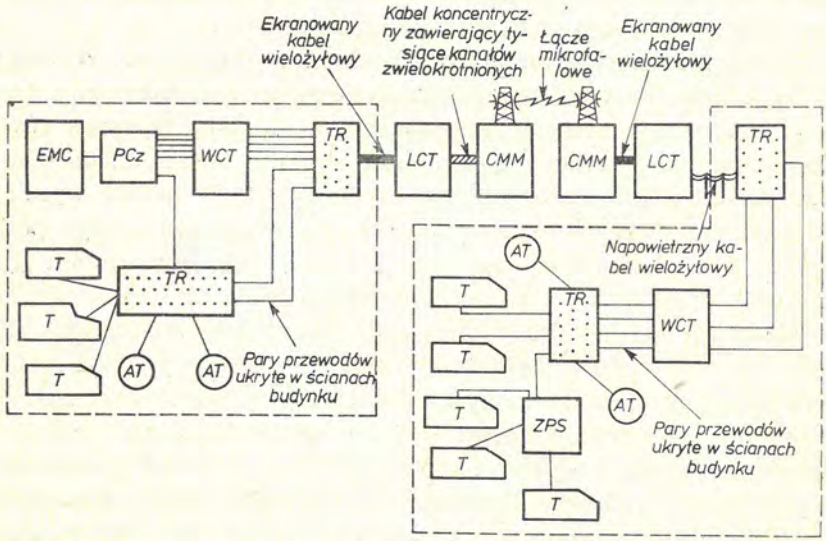
Linie prywatne są dla osób postronnych o przestępczych zamiarach trudne do zlokalizowania; w razie potrzeby można je specjalnie chronić, ekranować itp.

Linie dzierżawione bywają bardziej dostępne, ale z kolei są zazwyczaj pilniej kontrolowane i strzeżone przez właściciela.

Do linii publicznych jest wprawdzie stosunkowo najłatwiejszy (co nie znaczy jeszcze łatwy) dostęp, są to jednak na ogół linie

wieloprzewodowe o dużym natężeniu ruchu i dobranie się do tej pożądanej pary przewodów — która niesie interesujące informacje — jest bardzo utrudnione.

Na rysunku 7 pokazano poglądowo przykład linii transmisyjnej stosowanej przy zdalnym przetwarzaniu. Komputer zlokalizowany w budynku (po lewej stronie rysunku) połączony jest z terminalami w tym samym (lub sąsiednim) budynku oraz, poprzez linię transmisyjną międzymiastową, z terminalami oddalonymi (w budynku po prawej stronie rysunku). Przewody z budynku komputera wyprowadzone są w postaci kabla, zawierającego wiele par przewodów. Dostanie się do tego kabla pod powierzchnią ulicy byłoby niesłychanie utrudnione. Intruz nie może otworzyć sobie po prostu włazu i przystąpić do pracy. Nawet gdyby mu się to udało, musiałby posiadać dokumentację, z której mógłby odczytać wzajemne przyporządkowanie przewodów i abonentów. Konieczna byłaby więc zmowa z właściwym pracownikiem sieci telefonicznej.



Rys. 7. Przykładowy przebieg drogi transmisji danych przy zdalnym przetwarzaniu

EMC — komputer główny, *PCz* — procesor czołowy *(front-end)*, *WCT* — wewnętrzna centrala telefoniczna, *TR* — tablica rozdzielcza, *LCT* — lokalna centrala telefoniczna, *CMM* — centrala międzymiastowa, *ZPS* — zdalny procesor sieci, *T* — terminal, *AT* — aparat telefoniczny

Kabel wiedzie do lokalnej centrali telefonicznej — na ogół zachowywany jest tutaj wysoki stopień zabezpieczenia. Trudno więc wyobrazić sobie samodzielne osiągnięcie dostępu do centrali, bez współudziału odpowiedniego personelu.

Z centrali lokalnej biegnie do centrali międzymiastowej kabel koncentryczny, przenoszący kilka tysięcy zwielokrotnionych torów akustycznych. Teoretycznie można przechwycić tę wiązkę, zarejestrować i poddać takim zabiegom, aby wydzielić sygnały biegnące przez jeden z wielu kanałów i zintepretować je. Wymagałoby to jednak specjalistycznego przygotowania i wyposażenia w niezmiernie kosztowne urządzenia.

Między centralami międzymiastowymi sygnały mogą być przesyłane przez łącze mikrofalowe, również zawierające wiele tysięcy kanałów. Dalej sygnały biegną znów ekranowanymi kablami wielożyłowymi do centrali lokalnej.

Ostatnie połączenie — od lokalnej centrali do tablicy rozdzielczej w budynku — może biec, powiedzmy, linią napowietrzną. Tu przechwycenie informacji może być nieco łatwiejsze, ale nadal zbyt trudne, aby mogło być praktykowane przez każdego, kto chciałby wedrzeć się do systemu APD.

Analiza przedstawionych warunków prowadzi do wniosku, że stosunkowo najłatwiej jest włączyć się do linii transmisyjnej wewnątrz budynku. Kable są tu rozdzielone na poszczególne pary i przyłączone do zacisków tablic rozdzielczych. Zazwyczaj każda para przewodów jest wyraźnie oznakowana. Pary te, po drodze do wewnętrznej centralki telefonicznej przechodzą następnie przez dalsze tablice rozdzielcze. Wreszcie w samej centralce są na ogół proste do zidentyfikowania i łatwo dostępne.

Reasumując, najbardziej skuteczne udaremnienie podsłuchu uzyskuje się przez odpowiednią ochronę tablic rozdzielczych i central telefonicznych. Urządzenia te powinny znajdować się w zamkniętych i strzeżonych pomieszczeniach. Tablice rozdzielcze powinny być umieszczone w zamykanych szafach. Wskazane jest także zainstalowanie w tych szafach alarmu przeciwwłamaniowego. System komputerowy może być tak zaprojektowany, aby każde usiłowanie włamania zostało wykryte i zasygnalizowane. W szczególnie ważnych sytuacjach można stosować skuteczne, choć kosztowne zabezpieczenie, polegające na umieszczeniu tablic rozdziel-

czych i łączy w kanałach z nadciśnieniem. Spadek ciśnienia występujący w efekcie próby dostania się do łączy transmisyjnych może być natychmiast zasygnalizowany.

Jest sprawą oczywistą, że osoby zgłaszające się jako pracownicy sieci telefonicznej do montażu lub konserwacji linii należy poddać skrupulatnemu badaniu tożsamości.

Kryptografia

Jeśli zachodzi obawa, że mimo wszystkich zabezpieczeń nie można jednak całkowicie wykluczyć podsłuchu należy zastosować — jeżeli jest to uzasadnione wrażliwością przesyłanych informacji — metody kryptograficzne, czyli szyfrowanie i deszyfrowanie danych.

Istnieje obszerna literatura o teoretycznych i praktycznych aspektach kryptografii. Większość tych publikacji ukazała się przed nadejściem „ery komputerów" — jest to więc obecnie literatura przestarzała. Komputer stwarza nieosiągalne przedtem możliwości zarówno jeśli chodzi o szyfrowanie informacji, jak i łamanie szyfrów. Jednak ostatecznie, jeśli posługiwać się komputerem rozsądnie, szyfrujący osiąga pewną przewagę nad tym, kto usiłuje znaleźć klucz odczytu, pod warunkiem, że ten ostatni nie dysponuje nieograniczonymi środkami i dowolnie długim czasem.

Przesyłanie zaszyfrowanej informacji między dwoma komputerami jest stosunkowo mało kosztowne i istnieje wiele metod, które są praktycznie wystarczająco niezawodne. Jeśli chodzi o wymianę informacji między komputerem i oddalonymi terminalami, sytuacja jest bardziej skomplikowana. Albo terminal musi być zaprojektowany jako urządzenie „inteligentne" w stopniu wystarczającym do prac kryptograficznych, albo też musi on być zaopatrzony w przystawkę kryptograficzną — co wiąże się z dodatkowymi kosztami, ogranicza możliwości wyboru rodzaju kodów i zmniejsza bezpieczeństwo transmisji.

Ogólnie mówiąc, kryptografia w transmisji danych musi być realizowana sumiennie i fachowo albo... wcale. Informacja niedbale szyfrowana jest bardziej zagrożona niż nie szyfrowana wcale, ponieważ powstaje złudne poczucie bezpieczeństwa tam, gdzie go wcale nie ma.

VI. Utrzymanie systemu zabezpieczeń

1. Podstawowe środki prewencyjne

Szkolenie

Szkolenie personelu jest zasadniczym elementem każdego programu ochrony informacji. Proces szkolenia powinien mieć charakter ciągły i powinien obejmować pracowników wszystkich szczebli. Ideałem byłaby sytuacja, gdyby każdy pracownik był przekonany o tym, że podejmowane środki ochrony informacji stoją nie tylko na straży interesów i szeroko pojętego majątku przedsiębiorstwa (instytucji, urzędu), ale bronią również jego interesów; zawężają bowiem w krytycznej sytuacji krąg osób podejrzanych, chroniąc przed odpowiedzialnością tych, którzy spełniają sumiennie swoje obowiązki. Podstawowym warunkiem jest jednakże, aby każdy pracownik czuł, że sprawy te traktowane są poważnie przez kierownictwo oraz aby znał swoje miejsce i rolę w ogólnym systemie zabezpieczeń.

Zadaniem szkolenia jest zatem uświadomienie pracownikom potrzeby i ważności programu ochrony oraz motywacja w kierunku czynnego uczestniczenia w tym programie i przyczyniania się do jego skuteczności.

Szkolenie może mieć mniej lub bardziej formalny charakter, zależnie od wielkości organizacji i liczby pracowników. Szkolenie formalne powinno dzielić się na dwa etapy:

1. Wiadomości ogólne o ochronie informacji i środowiska jej przetwarzania — zajęcia wspólne dla wszystkich pracowników.

2. Zajęcia w grupach dla projektantów systemów, programistów, operatorów itd.

Szkolenie nieformalne powinno polegać na przygotowaniu i rozprowadzeniu zwięzłych i jasnych — ale wyczerpujących zagadnienie — instrukcji, obejmujących różne dające się przewidzieć okoliczności i różne stanowiska. Znajomość tych instrukcji powinna być stale sprawdzana, a ich przestrzeganie — kontrolowane i konsekwentnie egzekwowane. Żaden pracownik nie może mieć podstawy do twierdzenia, że nie rozumie na czym ochrona informacji polega lub że nie wie, jaka jest jego rola i odpowiedzialność w systemie ochrony.

Reasumując, bez względu na to jak przeprowadzany jest proces szkolenia, powinien on być nastawiony na osiągnięcie trzech celów:

a) wyjaśnienie każdemu pracownikowi dlaczego potrzebny jest system ochrony informacji wraz z objaśnieniem zagrożeń, jakie mogą występować w konkretnej sytuacji pracownika i zakładu,

b) wyjaśnienie szczegółów działania systemu ochrony,

c) wyjaśnienie każdemu pracownikowi, na czym polega jego odpowiedzialność w zakresie ochrony wrażliwej informacji przedsiębiorstwa (instytucji, urzędu).

Sposoby zapewnienia rezerwowej mocy obliczeniowej

Całkowite zdublowanie sprzętu. Jest to oczywiście rozwiązanie najkosztowniejsze i stosowane tylko w sytuacjach, kiedy nie może być tolerowana przerwa w przetwarzaniu — np. w niektórych zastosowaniach w czasie rzeczywistym lub w kontroli procesów ciągłych. Naturalnie koszty zapasowego sprzętu muszą być uzasadnione wynikami analizy ekonomicznej.

Częściowe zdublowanie sprzętu. Zapewnienie dodatkowych jednostek taśmowych, dyskowych itp. ponad niezbędnie konieczne należy do szeroko stosowanych praktyk, zabezpieczających przed unieruchomieniem całego systemu w razie uszkodzenia jednego urządzenia peryferyjnego. Oczywiście takie zapasowe jednostki zainstalowane obok normalnej instalacji, stanowią zabezpieczenie tylko na wypadek awarii maszyny. W przypadku pożaru itp. są w tym samym stopniu zagrożone, co reszta zainstalowanego sprzętu.

Zdublowanie podstawowych instalacji doprowadzających. Zasilanie energią elektryczną, doprowadzenie światła i wody, klimaty-

zację itp. należy traktować tak samo, jak inne zasoby systemu. Istnieje bogaty wybór sprzętu zapewniającego ochronę przed zakłóceniami w sieci i dłuższymi okresami spadku napięcia. Właściwe eksploatacyjnie i zadowalające ekonomicznie rozwiązanie problemów zabezpieczenia przed skutkami przerw w dopływie prądu i spadku napięcia w sieci możliwe jest jedynie po przeprowadzeniu głębokiej analizy konkretnych potrzeb danej instalacji APD, łącznie z przewidywanym wzrostem poboru energii elektrycznej.

Umowy o wzajemnym wsparciu. Do rozpowszechnionych praktyk należą umowy o „ubezpieczeniu wzajemnym" między sąsiadującymi użytkownikami podobnych zestawów sprzętu. Takie zabezpieczenie dobrze służy w razie pożaru czy innych okoliczności narażenia całego zainstalowanego sprzętu, jak również w przypadku dłuższej awarii maszyny. Należy jednak pamiętać, że rozwiązanie to ma dwie zasadnicze wady: po pierwsze, czas korzystania z instalacji może być bardzo ograniczony, ponieważ właściciel musi kontynuować swoje przetwarzanie; po drugie, różnice w konfiguracji, systemach operacyjnych itp., które mogą zostać wprowadzone już po zawarciu umowy, mogą utrudnić lub wręcz uniemożliwić awaryjne wykorzystanie instalacji. Tak więc warunki wszelkich takich umów należy często sprawdzać i aktualizować, jeśli mają one być realne w sytuacji krytycznej. Warto tu podać przykładowo kilka punktów, które powinny znaleźć się w typowej umowie o wzajemnym wsparciu:

1. Każda ze stron zobowiązuje się, że w przypadku awarii udostępni drugiej stronie określoną ilość czasu maszyny (np. w każdej dobie jedną zmianę 8-godzinną, przez 7 dni w tygodniu). Ilość ta z reguły nie będzie wystarczająca, należy więc pomyśleć o dodatkowej, podobnej umowie z innym „sąsiadem".

2. Każda ze stron powinna być przygotowana na to, że będzie musiała zawiesić część mniej pilnych prac na okres udzielania pomocy drugiej stronie. Trzeba patrzeć realnie i pogodzić się z faktem, że warunkiem przyjścia komuś z istotną pomocą jest poniesienie samemu pewnych ofiar; można np. proste prace — takie jak wydruk tabel lub sprawozdań — zlecić tymczasowo innemu ośrodkowi. Będzie to niewielką ceną, jaką zapłaci się za gwarancję uzyskania szybkiej i sprawnej pomocy w sytuacji katastrofalnej.

3. Należy przewidzieć w umowie wzajemne ułatwienia w prze-

testowywaniu swoich programów na obcym urządzeniu. Dobrze byłoby, aby obie strony miały przygotowane uproszczone programy awaryjne, w których być może trzeba zrezygnować z pewnych mniej ważnych funkcji na rzecz sprawnego wykonania funkcji podstawowych. Ideałem byłoby, gdyby z normalnie eksploatowanych programów łatwo było usunąć pewne mniej istotne moduły.

4. Przy ustalaniu szczegółów umowy może okazać się, że jedna (lub obie) ze stron musi uzupełnić swoją konfigurację drobnymi dodatkowymi urządzeniami, aby zaspokoić ewentualne potrzeby partnera. Trzeba naturalnie ustalić, kto za jakie urządzenia dodatkowe płaci.

5. Umowa powinna jasno precyzować ewentualne wzajemne zobowiązania finansowe i zasady rozliczania. Ma to również znaczenie przy zawieraniu umowy na polisę ubezpieczeniową (o czym będzie dalej mowa).

Przetwarzanie „na piechotę". W przypadku niektórych systemów może być do przyjęcia awaryjne przejście na krótki czas na przetwarzanie ręczne. Jeśli to rozwiązanie ma być stosowane, konieczne są ścisłe, jasno napisane instrukcje dla personelu wykonawczego. W wielu przypadkach brak odpowiedniego personelu stanowi główną przeszkodę w przyjęciu takiego wariantu.

Częściowe przetwarzanie awaryjne. W niektórych sytuacjach może być realne stosowanie częściowego przetwarzania. Na przykład, jeśli normalne przetwarzanie listy płac jest chwilowo niemożliwe, może okazać się praktyczne wypłacanie okrągłych sum, bliskich zarobkom, w charakterze zaliczki, a następnie dokładne rozliczenie wtedy, gdy wznowiona zostanie normalna działalność APD. Może to być łatwiejsze i tańsze niż procedury konwencjonalne.

Duplikaty zbiorów, programów i dokumentacji. Podstawą każdego systemu zabezpieczeń jest, jak podkreślano, przechowywanie duplikatów zbiorów, programów (nie wyłączając oprogramowania systemu) i dokumentacji. Duplikaty te powinny być przechowywane w pomieszczeniu odległym od ośrodka obliczeniowego, aby wyeliminować ryzyko tego samego zagrożenia oryginału i kopii. Należy zapewnić systematyczną aktualizację takich kopii bezpieczeństwa.

Polisy ubezpieczeniowe

Kompleksowy program ochrony powinien obejmować także polisę ubezpieczeniową, co ma na celu przede wszystkim:

a) zapewnienie funduszów na naprawę lub odkupienie urządzeń oraz odtworzenie zbiorów a także pokrycie zwiększonych kosztów, związanych z przetwarzaniem awaryjnym,

b) zwrot ewentualnych należności klientom, nie obsłużonym w konsekwencji awaryjnego zawieszenia usług przetwarzania (np. kary umowne),

c) pokrycie innych strat wynikłych w konsekwencji przerwy w przetwarzaniu.

Ustalenie sum ujętych punktem a) jest stosunkowo łatwe. Szczególną uwagę należy zwrócić na koszty wymiany (niekoniecznie takie same, jak nabycia) urządzeń łącznie z urządzeniami towarzyszącymi — takimi jak np. instalacja klimatyzacyjna — oraz przewidzieć koszty ewentualnych napraw budynku itp.

Ocena kosztów wtórnych ujętych w punktach b) oraz c) często bywa trudna, a jednak zaniedbanie ich może mieć bardzo nieprzyjemne skutki.

Państwowy Zakład Ubezpieczeń w Polsce dotychczas nie zawiera umów na ubezpieczenie ośrodków obliczeniowych, oprócz normalnego ubezpieczenia majątkowego od pożaru, powodzi i innych katastrof żywiołowych, od szkód w transporcie oraz kradzieży z włamaniem i rabunku (stan z lipca 1978 r.).

2. „Futurologia" ochrony informacji

Scenariusz katastrofy

Przewidywanie przebiegu mogącej ewentualnie nastąpić katastrofy przypomina nieco... planowanie własnego pogrzebu. Jest pewne, że niewiele osób o tym pomyśli, a jeśli nawet — to załatwienie tej sprawy zostanie odłożone na później. A jednak proces układania scenariusza postępowania w przypadku katastrofy może dać wiele pozytywnych skutków, nawet jeśli do danej katastrofy (miejmy nadzieję) nie dojdzie. Samo przemyślenie planu postępowania

i analiza możliwych skutków zwróci uwagę planującego na możliwe do zastosowania środki zapobiegające przykrym wydarzeniom, a co najmniej osłabiające ich skutki.

Z punktu widzenia ochrony informacji w ośrodku APD można przyjąć następującą definicję:

Katastrofa jest to częściowa lub całkowita utrata jednego lub więcej zasobów systemu APD na nieprzewidziany i długi okres, pociągająca za sobą skutki o poważnym wpływie na działalność organizacji obsługiwanej przez ten system.

Jeśli przystąpi się do realistycznego analizowania możliwych katastrof w celu zaplanowania postępowania w obliczu takich sytuacji, okaże się po chwili zastanowienia, że właściwie musi istnieć szereg takich planów — scenariuszy. Uwzględniania wymagają następujące zasoby ośrodka APD:

— programy,
— dane próbne,
— dokumentacja,
— dane właściwe (zbiory główne, zbiory transakcji, zbiory taśmowe),
— materiały pomocnicze i zasilanie,
— powierzchnia,
— środowisko,
— terminale,
— linie transmisyjne,
— personel,
— komputer i urządzenia peryferyjne.

Każdy z tych zasobów jest niezbędny i wymaga ochrony. Każdy też z tych zasobów może ulec częściowemu lub całkowitemu uszkodzeniu lub zniszczeniu niezależnie od innych, choć w większości przypadków zaistniała katastrofa stanowić będzie kombinację szeregu wydarzeń, o różnych skutkach dla różnych zasobów.

Wynika stąd, że należy przeanalizować i przygotować co najmniej tyle scenariuszy, ile jest tych zasobów. Im bardziej modularny będzie plan postępowania na wypadek nieszczęścia, tym większa jest szansa, że w konkretnej sytuacji będzie można go skutecznie zrealizować. Jeśli natomiast w chwili katastrofy będzie do dyspozycji tylko jeden piękny, kompleksowy, wyczerpujący plan, najprawdopodobniej w krytycznym momencie trzeba będzie za-

rzucić go i zdać się na intuicję, co może oczywiście skończyć się następnym nieszczęściem.

Przygotowanie dobrego, modularnego, realistycznego scenariusza katastrofy wymaga sporo pieniędzy, czasu i wiedzy. Pożądane jest wciągnięcie do tej pracy również dobrych fachowców spoza ośrodka APD, co ułatwi rzeczową ocenę zagrożeń i kosztów, choćby nawet przybliżoną.

Niektórzy specjaliści zalecają rozpocząć pracę od przeprowadzenia symulacji poszczególnych katastrof. Organizacje, które dokonywały takich symulacji były często — niemal zawsze — przerażone wynikami. W typowych sytuacjach dane nie dawały się odtworzyć, rezerwa awaryjna była niedostępna lub niewystarczająca, koszty przekraczały kwoty ubezpieczenia itd.

Zalecane są dwie metody symulacji: albo seria różnych pozorowanych katastrof, o rosnących stopniowo rozmiarach, albo jedna wielka, rozległa katastrofa (pożar, powódź, trzęsienie ziemi) — symulacja połączona z usuwaniem lub korektą ujawnionych braków i kontynuowaniem ćwiczenia aż do pomyślnego (mniej więcej) zakończenia. Zgodnie z doświadczeniami nagromadzonymi przez organizacje, które dokonały takich „prób generalnych" według opracowanych scenariuszy, czas i pieniądze wydatkowane na te próby opłaciły się sowicie.

Należy jednak pamiętać, że wypróbowane i akceptowane scenariusze sprawdzają się w konkretnych warunkach. Ponieważ warunki te nieustannie zmieniają się w czasie, scenariusze ulegają dezaktualizacji. Jest zatem rzeczą konieczną przeprowadzanie okresowych ćwiczeń według scenariuszy i dostosowywanie ich każdorazowo do zmienionych warunków. Daje to tę korzyść dodatkową, że ćwiczy się jednocześnie personel — który też przecież nie jest stały.

3. Nadzór nad systemem zabezpieczeń

Wykrywanie i rejestrowanie usiłowań uzyskania nielegalnego dostępu do systemu APD oraz reakcja na te usiłowania, stanowią integralną część każdego kompleksowego systemu zabezpieczeń. Nadzór (*monitoring*) powinien być czynny i bierny. Nadzór bierny po-

lega na analizowaniu „po fakcie" kto i w jaki sposób usiłował dobrać się do systemu oraz czy mu się to udało. Nadzór czynny polega na bieżącym śledzeniu i wykrywaniu niedozwolonych czynności wówczas, kiedy są wykonywane. Nadzór bierny wchodzi w zasadzie w skład funkcji audytora wewnętrznego i zostanie szerzej omówiony w dalszej części tego rozdziału. Tu uwaga zostanie skoncentrowana na nadzorze czynnym, który należy przede wszystkim do obowiązków stanowiska do spraw ochrony informacji (SOI). W sprawowaniu tego nadzoru powinien pomagać SOI aktywny monitor systemowy.

Monitor ten wykorzystuje zasoby systemu APD do sprawowania ciągłej kontroli nad stanem bezpieczeństwa systemu. Wymaga to trzech różnych działań:

— wykrywania,
— alarmowania lub ostrzegania,
— automatycznej akcji zapobiegawczej.

Wykrywanie

Wykrywanie wydarzeń zagrażających bezpieczeństwu jest zadaniem złożonym. Monitor aktywny musi ustalić, jakie reakcje systemu lub jakie wydarzenia stanowią pogwałcenie bezpieczeństwa. Musi stale sterować właściwym funkcjonowaniem mechanizmów ochronnych systemu, a także musi umieć rozpoznać naturę zagrożenia, aby podjąć akcję zapobiegawczą i zaalarmować SOI. Dobry monitor wykryje takie pogwałcenie zasad zabezpieczenia, jak:

— usiłowanie odczytania i modyfikowania danych przez jakiś program (użytkownika), któremu prawo do tego nie przysługuje,

— żądanie podprogramu bibliotecznego przez nie upoważniony do tego program (użytkownika),

— zgłoszenie się do systemu terminala nie mającego upoważnienia,

— wprowadzenie z terminalą nieważnego identyfikatora lub hasła,

— inicjowanie jakiejś akcji przez użytkownika w godzinach, w których nie ma on do tego prawa,

— przekraczanie przez użytkownika pewnych ograniczeń nało-

żonych na tryb jego pracy, jak przydzielony czas pracy, liczba stron wydruku lub dopuszczalna liczba błędnych działań,

— usiłowanie uzyskania dostępu do urządzenia peryferyjnego lub próba przesłania transakcji przez nie upoważnionego do tego użytkownika,

— próba dostania się bez upoważnienia do obszarów uprzywilejowanych w pamięci, takich jak tabele upoważnień lub listy haseł.

Ponadto aktywny monitor powinien mieć możność kontrolowania sposobu wykorzystywania określonych zasobów przez poszczególnych, uprawnionych użytkowników.

Alarmowanie i ostrzeganie

Z chwilą gdy nastąpi wykrycie istotnego wydarzenia, system powinien dysponować mechanizmem umożliwiającym zaalarmowanie operatora i SOI, aby podjęli oni odpowiednie kroki w kierunku bądź oceny i udzielenia zezwoleń, bądź uniemożliwienia czy przerwania pewnych działań. Zaalarmowanie może nastąpić poprzez sygnały świetlne albo dźwiękowe lub przez nadanie odpowiedniego komunikatu na pulpit operatorski lub monitor ekranowy.

W określonych okolicznościach, przed przesłaniem alarmu może zostać nadany komunikat ostrzegawczy do terminala, z którego korzysta „delikwent". Alarm zostaje włączony dopiero wówczas, gdy komunikat ostrzegawczy nie odnosi skutku.

Automatyczna akcja zapobiegawcza

Samo alarmowanie zagrożenia nie wystarcza. Powinna po nim automatycznie nastąpić akcja uniemożliwiająca intruzowi uzyskanie dalszych informacji. Mogą tu być potrzebne tablice decyzyjne; jeśli wykroczenie jest drobne i może być spowodowane błędem użytkownika, należy poprzestać na wspomnianym ostrzeżeniu użytkownika. Jeśli wykroczenie jest poważne lub ten sam błąd powtarza się mimo ostrzeżenia, monitor może podjąć jedną z następujących akcji:

— zawiesić wykonanie „obwinionego" programu,

— wyłączyć terminal lub zablokować jego klawiaturę,

— odmówić na określony czas przyjmowania informacji wejściowych,
— wpędzić delikwenta w pułapkę.

Natychmiastowe zawieszenie programu powinno mieć miejsce wówczas, gdy następuje bez upoważnienia odwołanie do określonych urządzeń peryferyjnych, gdy użytkownik pogwałci obszary ochronne pamięci lub gdy w programie zawarto wykonywanie instrukcji uprzywilejowanych. Zawieszenie to musi być całkowite. Powinny zostać przerwane wszelkie działania programu i usunięte z kolejek wszelkie jego zapotrzebowania (życzenia).

Aby uniemożliwić użytkownikowi ponawianie wykroczeń można zablokować klawiaturę terminala w taki sposób, aby odblokować go mogła tylko osoba upoważniona. Można także przerwać seans łączności z „podejrzanym" terminalem. Ponowne usiłowania nawiązania łączności zajmą użytkownikowi dość czasu, aby umożliwić SOI ustalenie, kto jest intruzem, i uniemożliwić jednocześnie użytkownikowi odkrycie np. metodą szybkich prób — i błędów — ważnego hasła.

Wreszcie monitor może wprowadzić użytkownika w pułapkę w taki sposób, że zamiast oczekiwanych prawdziwych i cennych informacji będzie on otrzymywał dane fikcyjne — zupełnie nie domyślając się tego. Usypia to czujność intruza, dając SOI czas na ustalenie jego tożsamości i lokalizacji.

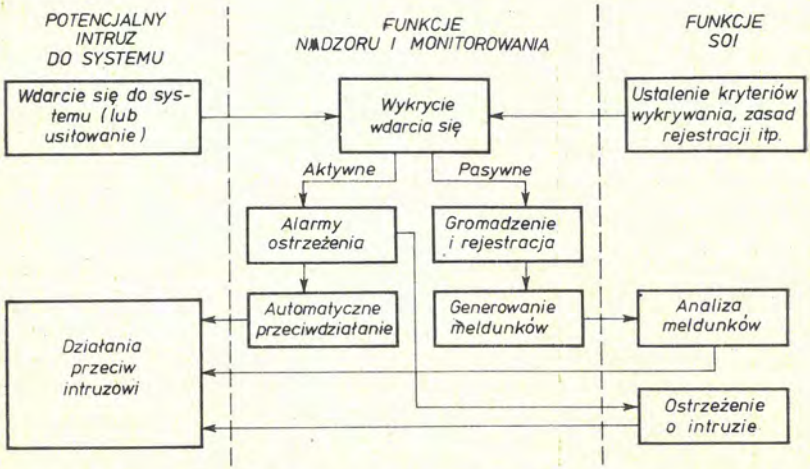
Nadzór realizowany przez monitor pasywny polega na rejestrowaniu przebiegu działań użytkowników w kierunku ustalenia i sprawdzenia stanu zabezpieczenia systemu w niedalekiej przeszłości. Jest to, inaczej mówiąc, nadzór ochronny nad systemem „po fakcie", nie w czasie rzeczywistym. Jakkolwiek przy tak sprawowanym nadzorze intruz może być pewien, że nie grozi mu bezpośrednie przyłapanie na gorącym uczynku, sama świadomość, że prędzej czy później jego działania wyjdą na jaw — stanowi jednak poważny element odstraszający.

Na nadzór bierny składają się trzy elementy:
— gromadzenie i rejestrowanie danych o pracy systemu,
— rozpoznawanie działań nielegalnych,
— generowanie meldunków.

Na ogół tego typu monitory gromadzą wszelkie informacje o ruchu wrażliwych danych — legalnym i nielegalnym. Podobnie, jak

monitory aktywne, również pasywne powinny umieć zadecydować, jakie zachowanie systemu lub jakie zdarzenia stanowią pogwałcenie bezpieczeństwa. Na podstawie takiej analizy generowane są meldunki o wydarzeniach i akcjach „podejrzanych".

Zestawienie funkcji nadzoru ochronnego oraz wzajemne zależności między SOI, funkcjami monitorów i potencjalnymi intruzami pokazano na rys. 8.



Rys. 8. Schematyczne ujęcie mechanizmu nadzoru i monitorowania

Szereg istniejących systemów operacyjnych dysponuje monitorami, realizującymi niektóre lub wszystkie omówione funkcje.

4. Kontrola i inspekcja systemów APD

W większości krajów istnieją niezależne firmy biegłych księgowych, które dokonują co najmniej raz w roku przeglądu ksiąg i działalności przedsiębiorstw w celu znalezienia potwierdzenia, że bilanse i sprawozdania budżetowe w sposób właściwy prezentują sytuację finansową firmy (w PRL funkcje te sprawują Najwyższa Izba Kontroli i banki; w organizacjach społecznych podobną rolę spełniają komisje rewizyjne).

Ludzi sprawujących te funkcje nazywa się różnie: audytorami, rewidentami, inspektorami zewnętrznymi.

Nieco inną rolę spełniają audytorzy wewnętrzni. Są oni orga-

nem dyrekcji lub rady nadzorczej, wykonującym zadanie wewnętrznej kontroli prawidłowości gospodarki finansowej, materiałowej itp.

Wraz ze wzrostem znaczenia komputerów w życiu gospodarczym zmieniają się zadania i metody pracy audytorów zarówno zewnętrznych, jak i wewnętrznych. Z jednej strony muszą oni być przygotowani do fachowej kontroli skomputeryzowanych systemów finansowych, gospodarczych i zarządzania. Z drugiej zaś strony komputer jako taki staje się coraz bardziej nieodzownym narzędziem pracy audytora.

Ze względu na tematykę tego opracowania należy poświęcić nieco uwagi zadaniom i metodom pracy audytora wewnętrznego z punktu widzenia zapewnienia właściwej ochrony informacji i środowiska jej przetwarzania.

Cele inspekcji APD

Audytor APD zajmuje się inspekcją ośrodka obliczeniowego (łącznie z systemami i oprogramowaniem) oraz inspekcją systemów użytkowych. Sprawdza on czy środki i zasoby są właściwie strzeżone oraz użytkowane zgodnie z przeznaczeniem; kontroluje niezawisłość i niezawodność systemu rachunkowości a także opracowywanych w tym systemie sprawozdań finansowych.

W zasadzie działalność audytora APD ma charakter prewencyjny — wykrycie zaniedbań lub machinacji, zanim powstaną problemy. Ponadto jednak audytor APD musi pełnić częściowo funkcje dochodzeniowe w sytuacji, gdy już zostały stwierdzone nieprawidłowości.

Kwalifikacje audytora APD

Zawód audytora APD dopiero zaczyna kształtować się. Skąd należy rekrutować kandydatów?

1. Uczyć audytorów informatyki. Może to być najlepszym rozwiązaniem, jeśli audytor jest na tyle zainteresowany komputerami, że poświęci swój czas na dodatkowe studia. Takich znajdzie się niewielu. Na ogół audytor może zdobyć bez większego trudu elementarne wiadomości o komputerze, ale jest wątpliwe czy uda

mu się wystarczająco poznać technologię APD, aby nie dać się wodzić za nos.

2. Uczyć projektantów (programistów) umiejętności audytorskich. Te same trudności. Niektórzy sądzą jednak, że łatwiejsze to niż nauczenie audytora informatyki.

3. Tworzyć zespoły mieszane. Jest to chyba najlepsze rozwiązanie. W dodatku wspólnie pracując, ludzie wiele wzajem od siebie nauczą się i z czasem mogą zacząć pracować samodzielnie.

4. Przydzielić audytorom programistów, których zadaniem będzie pisanie programów rewidenckich. Rozwiązanie niekosztowne, ale ryzykowne. Programiści będą pisać programy sprawdzające ich własną pracę. Stwarza to pole do nadużyć.

5. Zlecić programowanie na zewnątrz. Jeśli brak audytorów o umiejętności programowania, może to być lepsze rozwiązanie niż zatrudnianie własnych programistów, będzie jednak więcej kosztować.

Pozycja audytora APD w strukturze organizacyjnej

Wydział inspekcji APD winien być niezależny od innych komórek operacyjnych i podlegać bezpośrednio dyrekcji. Audytorzy APD powinni stale śledzić pracę ośrodka obliczeniowego, by być w kursie wydarzeń; powinni być zorientowani, jakie nowe projekty są w opracowaniu, jakie większe zmiany wprowadza się do systemów w eksploatacji, jakie zmiany w systemach rzutują na bezpieczeństwo informacji.

Wydział inspekcji APD powinien dysponować dobrymi pakietami oprogramowania rewidenckiego, dostosowanymi do konkretnych potrzeb. Personel powinien nie tylko być dobrze przeszkolony w posługiwaniu się tym oprogramowaniem, ale również podlegać ciągłemu szkoleniu, aby nadążać za szybkim rozwojem technologii APD.

Audytor APD musi polegać na wewnętrznych procedurach kontrolnych organizacji, musi wiedzieć z całą pewnością, że przyczyniają się one do minimalizacji szans oszustwa i machinacji. Jego zadaniem jest upewnienie się, że te środki kontroli wewnętrznej są wystarczające oraz zgodne z wymaganiami i przepisami.

W dotychczasowych „ręcznych" systemach rachunkowości wewnętrzne środki kontroli były dobrze udokumentowane i łatwe do prześledzenia. Księgi są zawsze dostępne i na ogół każdą transakcję można prześledzić wizualnie poprzez procedury księgowości. Inaczej sprawa wygląda w rachunkowości skomputeryzowanej. Zapisy znajdują się na nośnikach magnetycznych, przebieg transakcji nie jest łatwo dostrzegalny ani w każdej chwili dostępny do zbadania.

Rodzaje inspekcji APD

Do inspekcji zapisów komputerowych można dwojako podchodzić; możliwa jest więc:

— inspekcja „wokół" komputera,

— inspekcja przy użyciu komputera.

To pierwsze podejście nie wymaga specjalnych kwalifikacji technicznych i opiera się na metodach dobrze audytorowi znanych. Bada on transakcje wchodzące do komputera i porównuje z wynikami opuszczającymi komputer po przetwarzaniu, upewniając się, czy cały proces przebiega prawidłowo. Może on nawet przygotować zestaw próbnych transakcji i poddawać je przetwarzaniu, pod warunkiem, że potrafi następnie zlikwidować ich efekt, tak aby wartości próbne nie pozostały na zawsze w księgach przedsiębiorstwa.

W drugim przypadku audytor wykorzystuje programy komputera do wykonania niektórych czynności inspekcyjnych. Na przykład może użyć programu wybierającego losowo pewne zapisy ze zbioru w celu wydrukowania ich i przeanalizowania. Inspekcja przy użyciu komputera wiąże się zazwyczaj z wykorzystaniem specjalnych programów, umożliwiających badanie stanu różnych rodzajów zbiorów.

Niezależnie od sposobu podejścia do inspekcji audytor może posługiwać się różnymi metodami i narzędziami analitycznymi (patrz tablica V). Niektóre z nich automatyzują proces inspekcji. Nie mogą one jednak nigdy zastąpić intuicji, uwagi i oceny doświadczonego audytora. Jego doświadczenie pozwala mu właściwie ocenić skuteczność środków kontroli wewnętrznej. Rozmowa z ludźmi mo-

TABLICA V

Zestawienie metod i narzędzi inspekcji APD

Sprawdzanie ręcznych i skomputeryzowanych etapów przetwarzania	Metody ręczne	Inspekcja „wokół" komputera
		Weryfikacja list kodów źródłowych
	Metody ręczne oraz programy generowania schematów blokowych	Weryfikacja logiki schematów blokowych programów
	Metody ręczne oraz programy generowania danych próbnych	Metoda danych próbnych
		Metoda ITF (Integrated Test Facility) lub metoda modelu przedsiębiorstwa — jako rozwinięcie metody danych próbnych
	Własne programy audytorskie	Równoległa symulacja całości lub części systemu użytkowego w celu wygenerowania systemu audytorskiego, odpowiadającego eksploatowanemu i niezależnie przetwarzającego dane przedsiębiorstwa
	Uogólnione, parametryzowane pakiety audytorskie	
Sprawdzanie wyników przetwarzania	Metody ręczne, własne programy audytorskie oraz uogólnione pakiety audytorskie	Weryfikacja pozycji zbioru z osobą spoza APD
		Testy zredagowania i sensowności pozycji w zbiorze

że go szybciej naprowadzić na słabe punkty systemu niż jakiekolwiek zautomatyzowane procedury.

Zadania audytora APD

Aby być pewnym, że interesy przedsiębiorstwa są właściwie zabezpieczone, audytor powinien uczestniczyć już w procesie projektowania systemów informacyjnych, szczególnie systemów dotyczących gospodarki finansowej i materiałowej. Już bowiem w procesie projektowania powinny zostać włączone do systemu skuteczne

środki kontroli. Im bardziej zautomatyzowany jest system, tym większa potrzeba współdziałania audytora przy jego projektowaniu. Współdziałanie to ma większe znaczenie przy systemach pracujących na bieżąco lub korzystających z silnie zintegrowanej bazy danych, niż przy systemach pracujących metodą wsadową. System zautomatyzowany może wykonać wiele pracy za audytora, kontrolując dokładność, bezbłędność, kompleksowość i bezpieczeństwo przetwarzania. Audytor musi jednak zapewnić, aby w systemie przewidziano środki umożliwiające sprawdzenie, czy programy rzeczywiście wykonują to, do czego zostały przeznaczone, oraz sposoby odtworzenia historii tego, co działo się z każdą z poszczególnych transakcji.

Jest jednak rzeczą ważną, aby audytor nie brał na siebie obowiązków projektanta. Jego zadaniem jest ustalenie założeń do projektu w części dotyczącej ochrony i kontroli danych, a następnie ocena, jak dalece założenia te zostały zrealizowane. Gdyby audytor sam projektował środki kontroli, dokonywałby następnie inspekcji własnej pracy, co nie gwarantowałoby obiektywnego, bezstronnego podejścia. Podobnie, nie do audytora należy egzekwowanie przepisów i procedur — jego zadaniem jest ocena i skuteczność egzekwowania ich przez innych.

Przed zatwierdzeniem nowego systemu do eksploatacji — obojętne, czy jest to system opracowany na miejscu, czy zakupiony na zewnątrz — audytor powinien spełnić rolę koreferenta systemu z punktu widzenia środków ochrony i kontroli. Czasem stanowiska projektantów i audytora mogą różnić się. Rzeczą kierownictwa będzie ocena potencjalnych zagrożeń i kosztów związanych z ich zmniejszeniem, a następnie decyzja, jaką należy obrać drogę.

Inspekcja systemów w eksploatacji

Inspekcja systemów będących w eksploatacji służy dwóm celom. Pierwszym jej zadaniem jest wykrywanie problemów, zagrożeń, złych nawyków, głupich posunięć i błędów. Drugim zaś jej zadaniem jest uświadomienie tym, którzy chcieliby skorumpować lub uszkodzić system, że mogą przecież zostać przyłapani. Dla osiągnięcia tych celów powinny być przeprowadzane dwa rodzaje inspekcji:

1. Dorywcze, niespodziewane kontrole w nieregularnych odstępach czasu.

2. Kompleksowe, wnikliwe inspekcje, dokonywane w z góry zaplanowanych terminach.

Istnieje cały szereg metod, które może stosować audytor dokonując inspekcji eksploatowanych systemów. Niektóre z nich zostaną bliżej omówione.

1. Wywiad bezpośredni. Audytor często rozpoczyna od zadawania pytań w celu zorientowania się w ogólnym poziomie ochrony i podejściu personelu do problemów zabezpieczenia. Może próbować wejść na salę komputera lub do archiwum zbiorów, aby przekonać się, czy wywoła to jakąś reakcję. Może zapytać użytkownika co stanie się, jeśli określony zbiór na taśmie magnetycznej zostanie zniszczony; może zapytać operatora, co by zrobił, gdyby z komputera zaczął wydobywać się dym; może spytać użytkownika terminala, czy widzi możliwość odczytania zbiorów, których odczytać nie powinien. Wiele pytań typu „co by było, gdyby..." wskaże na dziedziny, które mogą wymagać bliższego zainteresowania.

2. Listy kontrolne. Audytor może posłużyć się listami kontrolnymi, w rodzaju listy przedstawionej w załączniku A, w celu uzyskania możliwie dokładnego obrazu sytuacji w zakresie ochrony informacji. Audytor, korzystając z dostępnych wzorów, powinien sam sporządzić taką listę odpowiadającą konkretnej sytuacji i potrzebom jego organizacji. Lista taka jest pomocna w dokonywaniu wnikliwego przeglądu, nie można jednak traktować jej jako czegoś, co zastąpi trzeźwy osąd doświadczonego specjalisty APD w dokonywaniu inspekcji środowiska przetwarzania danych.

3. Kontrola bieżąca. Audytorzy dokonują systematycznych, choć nieregularnych w czasie kontroli wszelkiego rodzaju dokumentów rejestrujących, jak log operatorski, ewidencja ruchu nośników (taśm, dysków), wydruk z konsoli operatorskiej itp. Kontrola bieżąca ma wykazać, czy dokumenty są starannie i na bieżąco prowadzone oraz czy nie są omijane procedury ochronne. Do tego celu audytor powinien posiadać dokładną listę wszelkich wprowadzonych środków kontroli i materiałów ewidencyjnych.

4. Próby wyrywkowe. Porównywanie dokumentów wejścia i wyjścia komputera — a nawet zapoznanie się z kodami źródłowymi programów — nie umożliwia jeszcze audytorowi autorytа-

tywnego stwierdzenia, czy to co dzieje się wewnątrz komputera ściśle odpowiada oficjalnym procedurom przedsiębiorstwa. Jedyną drogą prowadzącą do odpowiedzi na to pytanie jest zaprojektowanie i przeprowadzenie prób na wyrywkowo dobieranych transakcjach za pomocą tzw. „tropu audytorskiego" (*audit trail*).

Trop audytorski polega na przygotowaniu i zarejestrowaniu:

a) na wystarczająco długi — stosownie do potrzeb — czas,

b) we względnie dostępnej formie,

c) z dokładnością wystarczającą do celów inspekcji

zapisów, które umożliwią prześledzenie każdego z poszczególnych elementów danej transakcji od źródła, poprzez stadia pośrednie aż do końcowego wyniku i vice versa; to znaczy z możliwością wykorzystania tych zapisów do śledzenia wstecz — od końcowych wyników poprzez pośrednie stadia do początkowego źródła transakcji.

5. Fałszywe transakcje. Skutecznym sposobem sprawdzenia działania logicznych środków zabezpieczenia jest wprowadzenie transakcji z celowo wprowadzonymi błędami, aby przekonać się czy system je wykryje. Zależnie od rodzaju pozycji, występujących w danej transakcji, wprowadzane błędy mogą testować niektóre lub wszystkie środki kontroli logicznej, omówione w rozdziale piątym.

6. Próby przełamania ochrony. Podobnie jak wprowadzanie fałszywych i błędnych transakcji stanowi najlepszy sprawdzian skuteczności procedur weryfikujących, tak przemyślane i inteligentne próby pogwałcenia ochrony są najlepszym sprawdzeniem skuteczności systemu zabezpieczeń (por. „zespoły tygrysie"). Niestety, przeciętny audytor rzadko jest typem nadającym się na włamywacza. Z drugiej strony istnieją osoby, które potrafią bez trudności wejść do zamkniętej sali komputera za kimś upoważnionym i wyjść niezauważone np. z kilkoma szpulami taśmy magnetycznej. Podobnie spotyka się osobowości, które charakteryzuje specjalny rodzaj pomysłowości technicznej i które bez pudła znajdą sposób na ominięcie zaprogramowanych barier ochronnych. Pomoc takich osób może być dla audytora bardzo cenna. Inna sprawa, że w wielu istniejących systemach nie potrzeba ani wielkiego tupetu, ani sprytu, aby dostać się wszędzie...

7. Próbne dane (zapisy, pseudotransakcje) i model przedsiębior-

stwa. Audytor powinien mieć w zbiorach systemu pewne zapisy wyłącznie do celów inspekcji. Zapisy te są aktualizowane przez pseudotransakcje, wprowadzane przez audytora do systemu. Podlegają one temu samemu przetwarzaniu co autentyczne zapisy i transakcje. Umożliwia to sprawdzanie, czy programy działają poprawnie i czy nikt przy nich nie majstrował. Niektórzy audytorzy dysponują kompletem zapisów przedstawiających pełny system lub też mały model firmy (*mini company*). Wykorzystanie takich modeli jest szczególnie przydatne w sytuacji, gdy przechodzi się na nowy system.

8. Programy specjalne. Rozwinięciem metody próbnych danych jest system programów ITF (*Integrated Test Facility*); umożliwia on wprowadzenie dobranych próbnych transakcji na danych umieszczonych w zbiorze podstawowym (*master file*), zawierającym również dane rzeczywiste, prześledzenie drogi tych transakcji próbnych przez różne funkcje systemu i sprawdzenie poprawności wyników na wyjściu systemu. Wymaga to utworzenia fikcyjnej jednostki, której będą dotyczyć próbne dane (wydziału, pracownika, klienta itp.); ITF jest tak zaprogramowany, że wyklucza próbne zapisy i transakcje z sum, które są rejestrowane w odpowiednich pozycjach księgowości przedsiębiorstwa.

Audytor powinien dysponować własnymi programami — szczególnie niezbędnymi do przeprowadzania inspekcji systemów dialogowych i pracujących na bieżąco — dokonującymi określonych prób kontrolnych. Programy te, jeśli to tylko możliwe, powinny być pisane poza ośrodkiem APD.

Istnieją również na rynku gotowe „pakiety audytorskie" (*computer audit programs, computer audit packages*). Są to zwykle pakiety ogólnego przeznaczenia do stosowania w różnych komputerach; audytor adaptuje je do swoich konkretnych potrzeb przez ustawienie określonych parametrów. Pakiety te są na ogół dość kosztowne i oprócz licznych zalet, wykazują także wiele wad. Oznacza to, że zakup ich wymaga dojrzałej analizy, opartej na dostępnych w literaturze fachowej opisach i doświadczeniach ich użytkowników. Istnieją także gotowe kwestionariusze, które po wypełnieniu przez dostawcę pakietu umożliwiają wnikliwą ocenę zalet i wad pakietu z punktu widzenia ściśle określonego zastosowania.

Rola wewnętrznego audytora w przedsiębiorstwie (urzędzie, instytucji)

Z uwagi na funkcje kontrolne sprawowane przez audytora oraz na to, że dokonuje on oceny efektywności pracy ośrodka APD i opracowuje zalecenia w kierunku poprawienia jakości tej pracy, niektórzy kierownicy ośrodków APD uważają niesłusznie, że dokonywanie inspekcji terenu ich działania przez audytora świadczy o negatywnej ocenie ich umiejętności i stanowi podważenie ich autorytetu.

Nawet najbardziej fachowy i sumienny personel APD podlega ocenie kierownictwa zwierzchniego. Ocena ta dokonywana jest z ramienia dyrekcji przez audytora, ponieważ członkowie dyrekcji w dużej organizacji nie są w stanie osobiście wszystkiego skontrolować. Zadaniem wydziału inspekcji APD jest ocena efektywności środków kontroli w całości organizacji, tym samym jest on jednym z najważniejszych narzędzi kontroli. Współpraca z tym wydziałem i okazywana mu pomoc jest świadectwem dojrzałości kierownictwa APD. Audytorzy wewnętrzni pomagają zmniejszyć ryzyko nierozerwalnie związane z pracą ośrodka APD, pomagają rozwiązywać trudne problemy oraz korzystnie wpływać na ochronę informacji i środowiska jej przetwarzania.

Zakończenie

W zakończeniu tego zwięzłego przeglądu zagadnień związanych z ochroną informacji i środowiska jej przetwarzania autor chciałby szczególnie podkreślić dwa ważne aspekty problemu ochrony.

Po pierwsze: uzyskanie istotnie skutecznej i pełnej w określonych realnych warunkach ochrony jest możliwe jedynie wtedy, gdy podchodzi się do tego problemu w sposób systematyczny, kompleksowy i uporządkowany. Inaczej mówiąc, pierwszym i podstawowym krokiem jest opracowanie planu systemu zabezpieczeń. Podejście „akcyjne", polegające na doraźnym reagowaniu na zagrożenia w chwili, kiedy zostaną one dostrzeżone lub tylko na sygnały zaniepokojonego kierownictwa przedsiębiorstwa (urzędu, instytucji) nie prowadzi do uzyskania rozsądnego poziomu zabezpieczenia przy realistycznym poziomie kosztów.

Po drugie: w praktyce można kwestionować twierdzenie, że system zabezpieczeń rzeczywiście przyczynia się do zwiększenia kosztów operacji APD. Prawidłowe zabezpieczenie systemu przynosi korzyści, które mogą w pełni rekompensować poniesione koszty. Wykluczenie zbędnych osób z pomieszczenia komputera przyczynia się do sprawniejszej i wydajniejszej pracy; użytkowanie bezpiecznego wariantu systemu operacyjnego zmniejsza straty czasu związane z przestojami maszyny z przyczyn związanych z oprogramowaniem oraz zwiększa niezawodność pracy systemu; ścisła kontrola i rejestracja modyfikacji (aktualizacji) zbiorów, uruchamiania programów i dokonywania w nich zmian prowadzi do wykrycia nie tylko osób mających złowrogie zamiary, ale również tych osób spośród personelu, które wymagają większego nadzoru i doszkalania; uniknie się w ten sposób wielu strat finansowych, powodowanych zaniedbaniami oraz błędami popełnionymi

przez osoby uczciwe i chętne, lecz nie mające wystarczającego doświadczenia lub niedoszkolone.

Dobrze funkcjonujący system zabezpieczeń przyczynia się do lepszej dyscypliny i organizacji pracy, ułatwia więc w konsekwencji zarządzanie.

Załącznik A

Lista kontrolna

Pomocą w sprawdzaniu, czy przedsięwzięte środki zabezpieczenia są kompletne i odpowiadające ogólnym zasadom może być lista kontrolna, przedstawiona dalej. Należy podkreślić, że odpowiedź „tak" na konkretne pytanie nie świadczy jeszcze, że istnieje pełne zabezpieczenie informacji lub zainstalowanych urządzeń — brak bowiem miary ilościowej stopnia zabezpieczenia. Natomiast odpowiedź „nie" z pewnością świadczy o potrzebie zwrócenia baczniejszej uwagi na dany obszar działania.

1. Czy podjęto decyzję, co ma być chronione?
2. Czy staramy się — w granicach możliwości — zachować anonimowość pomieszczeń i czy ograniczono ruch obcych?
3. Czy dostęp do wszystkich pomieszczeń ograniczono do kręgu osób bezpośrednio w nich zatrudnionych?
4. Czy podczas pracy w ośrodku APD przestrzegana jest surowa dyscyplina porządkowa?
5. Czy podjęto wystarczające kroki zabezpieczające fizycznie wszystkie urządzenia, łącznie z ochroną przed środowiskiem?
6. Czy morale pracowników — widzianych jako zespół i indywidualnie — jest dobre?
7. Czy wszyscy pracownicy są wystarczająco przeszkoleni? Czy są pod stałym nadzorem?
8. Czy istnieje jasna, sprecyzowana polityka przydzielania, dzielenia i rotacji odpowiedzialności?
9. Czy wszystkie zbiory i dokumentacje, bez wyjątku, podlegają wystarczającej kontroli?
10. Czy istnieje wystarczające zabezpieczenie awaryjne (zastępcze zbiory, programy, urządzenia)? Czy istnieją i czy są stale utrzymywane w stanie aktualności plany działania w przypadku awarii?
11. Czy są opracowane (i znane wszystkim pracownikom) instrukcje alarmowe (p.pożarowe, ewakuacyjne itp.)? Czy są one wypróbowane (np. próbne alarmy)?

12. Czy istnieje ustalona procedura spodziewanych i niespodziewanych inspekcji urządzeń, pracy i oprogramowania?
13. Czy udało się uniknąć podejścia do spraw bezpieczeństwa informacji opartego na wymyślnych urządzeniach, które często zawodzą?
14. Czy usiłowano porównać koszt zabezpieczeń ze stopniem oczekiwanego ryzyka, wyrażonym w jednostkach kosztu?
15. Czy jest zapewnione, aby każdy system, program, procedura oraz wszelkie ich zmiany były zatwierdzone przez właściwą instancję?

Bibliografia

1. Attanasio C. R., Markstein P. W., Phillips R. J.: *Penetrating an Operating System: a Study of VM/370 Integrity.* IBM Systems Journal 1976, Nr 1, s. 104
2. *Computer Security Handbook,* praca zbiorowa. Macmillan Information, New York 1973
3. Davis G. B.: *Auditing and EDP.* American Institute of Certified Public Accountants 1968
4. Diebold Research Program — Europe, Doc. Nr EC-24, Conference Proceedings. Meeting XXIV, 1972
5. Diebold Research Program — Europe, Doc. Nr E-92, Ensuring the Security of the Information Resource, 1972
6. Europejski Program Badawczy Diebolda Nr 40: *Przeglądy kontrolne systemów.* OBRI, Warszawa 1973
7. Europejski Program Badawczy Diebolda Nr 54: *Oprogramowanie dla transmisji danych.* OBRI, Warszawa 1974
8. Flory W.: *Berücksichtigung des Factors Sicherheit beim Site Planning* Seminarium nt. „Sicherheit von EDV — Anlagen". Sperry — UNIVAC, Schweiz, 1973
9. IBM Corporation: *The Considerations of Data Security in a Computer Environment,* White Plains. N.Y. Form G 520-2169
10. Kulikowski J. L.: *Organizacyjne i techniczne aspekty ochrony danych w systemach informatycznych.* Materiały z konferencji nt. „Prawne problemy systemów informatycznych". Wrocław, maj 1976
11. Martin J.: *Security, Accuracy and Privacy in Computer Systems.* Prentice — Hall Inc. Englewood Cliffs, N.Y. 1973
12. Wasserman J.: *Plugging the leaks in computer security.* „Harvard Business Review". September—October 1969
13. Wooldridge S., Corder C., Johnson C.: *Security Standards for Data Processing.* Macmillan Press Ltd. London 1973

Redaktor techniczny
Władysława Nasternak
Korektor
Mieczysław Szostakowski
Printed in Poland
Państwowe Wydawnictwo Ekonomiczne, Warszawa 1979
Zlec. 87/76. Wyd. I. Nakład 5000 + 240 egz.
Ark. wyd. 8,5. Ark. druk. 9,25
Papier druk. sat. kl. IV, 70 g. Format 61×86/16
Oddano do składania 30.XI.1978 r. Podpisano do druku 5.IV.1979 r.
Druk ukończono w kwietniu 1979 r.
Cena zł 26,—
Zakłady Graficzne w Katowicach, ul. Armii Czerwonej 138
Zam. 1089/4/78, G-5

W serii
„INFORMATYKA W PRAKTYCE"
ukazały się dotychczas następujące pozycje:

MARTIN ZSCHOCKE

Elektroniczne przetwarzanie danych w gospodarce materiałowej
s. 118, cena zł 14,—

*

AGATA ROJEK-GROSZEWSKA
ANDRZEJ ZALESKI

Gromadzenie danych do elektronicznego przetwarzania na przykładzie obrotu towarowego
s. 350, cena zł 40,—

*

KIT GRINDLEY, JOHN HUMBLE

Skuteczność wykorzystania komputera
s. 245, cena zł 45,—

*

STANISŁAW ZADROŻNY

Organizacja zbiorów w małej informatyce
s. 200, cena zł 40,—

*

EDWARD KOLBUSZ, EDWARD KRAM

Wdrażanie systemów informatycznych w przedsiębiorstwie przemysłowym
s. 268, cena zł 36,—

*

ANDRZEJ JORDAN

Organizacja zbiorów w pamięciach dyskowych
s. 130, cena zł 19,—

PRACA ZBIOROWA

Przechowywanie danych (tłum. z jęz. niem.)
s. 154, cena zł 23,—

ZYGMUNT RYZNAR

Bank danych w przedsiębiorstwach przemysłowych
s. 172, cena zł 26

IGNACY DZIEDZICZAK

Model księgowości informatycznej w przedsiębiorstwie
s. 212, cena zł 38,—

BRONISŁAW OBIREK

Przygotowanie przedsiębiorstwa do zastosowania informatyki w zarządzaniu
s. 152, cena zł 23,—

JANUSZ ILCZUK
MARIA JERCZYŃSKA

Efektywność systemów informatycznych zarządzania
s. 208, cena ok. zł 38,—

W przygotowaniu:

ROMUALD JAGIELSKI

Komputery Jednolitego Systemu
s. ok. 450, cena ok. zł 40,—

Cena zł 26,–