OŚRODEK BADAWCZO-ROZWOJOWY INFORMATYKI

PRZEGLĄDY KONTROLNE SYSTEMÓW

EGZEMPLARZ OKRĘ

Europejski Program Badawczy Diebolda

40

Warszawa 1973

OŚRODEK BADAWCZO-ROZWOJOWY INFORMATYKI

PRZEGLĄDY KONTROLNE SYSTEMÓW

Europejski Program Badawczy Diebolda

Wyłącznie do użytku na terenie PRL

40

Warszawa 1973

Tytuł oryginału: Systems Auditing and Control

Document nr E86, March 1971

Tłumaczenie: Jędrzej Spychalski
Opiniodawca: Zbigniew Drabek
Redakcja: Andrzej Idźkiewicz

Komitet Redakcyjny

Mieczysław Gula, Franciszek Haratym, Andrzej Idźkiewicz, Janina Jerzykowska /sekretarz/, Jerzy Kisielnicki, Stanisław Nelken /zastępca przewodniczącego/, Krzysztof Skulski, Zdzisław Zapolski /przewodniczący/

Wydawca

Działowy Ośrodek Informacji, Warszawa, ul.Marszałkowska 104/122

OBRI Warszawa 1973 r. Nakład:850 +164 Objętość: ark.wyd. 6,5, ark.druk.12. Format A4. Papier offsetowy kl.III 80 g 61 x 86

Druk. DOI/P zam.nr206/73 R-13 Cena zł 92,-

SPIS TREŚCI

STRESZCZENIE 7

I. WPROWADZENIE 11

A. Tło badań 11
B. Wnioski 12
C. Zakres i metodologia 14

II. ADMINISTRACYJNE ŚRODKI KONTROLI 15

A. Organizacyjne środki kontroli 16
B. Inspekcja 17
C. Procedury wspierające 23
D. Zapobieganie katastrofie i wyprowadzanie systemu z katastrofy 27

III. ŚRODKI KONTROLI SYSTEMU 28

A. Środki kontroli wejścia 28
B. Zaprogramowane środki kontroli 33
C. Środki kontroli przetwarzania w systemach pracujących na bieżąco 34
D. Środki kontroli wyjścia 36
E. Dokumentacja 37

IV. ZABEZPIECZANIE 45

A. Projektowanie 45
B. Zabezpieczenie fizyczne 48
C. Eksploatacja 50
D. Personel 52

V. INSPEKTOR WEWNĘTRZNY W APD 53

A. Udział inspektora 54
B. Inspektor APD 56

ZAŁACZNIK A - Obowiązki inspektora wewnętrznego 59

ZAŁACZNIK B - Ochrona przeciwpożarowa systemów komputerowych 61

ZAŁACZNIK C - Lista kontrolna inspekcji systemu 70

BIBLIOGRAFIA 93

OD REDAKCJI

W niniejszym przekładzie pominięto rozdział VI oryginału /"Narada robocza na temat przeglądu kontrolnego systemów"/. Jest to dosłowny stenogram prowadzonej dość chaotycznie narady, pełen kolokwializmów i żargonu, bardzo trudny do przetłumaczenia, a niewiele wnoszący merytorycznie.

STRESZCZENIE

Wzmagający się wzrost liczby terminali zdalnego dostępu i systemów wielodostępnych, a także rosnąca zależność przedsiębiorstw od APD, stwarza popyt na nowy rodzaj przedstawiciela kierownictwa, który jednocześnie jest zaznajomiony z celami /zadaniami/ przedsiębiorstwa, jak i z funkcjami APD: inspektora APD.

Procedury inspekcji APD posiadają w swym założeniu te same postawione cele, co wewnętrzne procedury inspekcji opracowane w okresie, kiedy księgowość była w większości wykonywana ręcznie. Wnikanie komputera i sprzętu do przetwarzania danych w działalność przedsiębiorstwa i jego kierownictwa wzmogło zapotrzebowanie na odpowiednie środki zabezpieczające i środki kontroli, a to z tego powodu, że system może przeprowadzać manipulacje na znacznie większych ilościach i większej rozmaitości danych. Lecz zakres i złożoność systemu APD dość często wykracza poza doświadczenie, jakim dysponuje tradycyjny rewident wewnętrzny. Obecnie osoba taka powinna być specjalistą zarówno w zakresie procedur inspekcji, jak i procedur APD.

Doprowadziło to do powstania zasadniczych pytań na temat funkcji rewidenta APD: czy jest to tradycyjny rewident, który jest zaznajomiony z funkcją przetwarzania informacji, czy też jest to specjalista od systemów w stroju rewidenta, lecz bez zrozumienia tego, co w tym zakresie przedstawia sobą tradycyjny inspektor kontroli wewnętrznej? Także przedmiotem dyskusji jest istota i zakres wnikania nowego rewidenta APD w wydział przetwarzania danych, oraz granica jego interwencji w system - od koncepcji do stanu eksploatacyjnego.

Sprawozdanie stwierdza, że zaangażowanie rewidenta właściwie zaczyna się podczas projektowania systemu. Znacznie trudniej wprowadzić odpowiednie środki kontroli, gdy system

jest już w eksploatacji - i kosztuje to więcej. Środki kontroli, które rewident ustanawia, pomagają w uchronieniu się przed błędnymi operacjami i wykrywają działalność oszukańczą. W przeciwieństwie do szeroko rozpowszechnionego mniemania, dobrze kontrolowane środowisko faktycznie przyczynia się także do zwiększenia wydajności w działalności APD, przez zmniejszenie kosztownych czasów powtórnych przebiegów, spowodowanych błędami w programach lub niekompletnymi danymi.

Ważną sprawą dla funkcjonowania dobrze kontrolowanego systemu jest szczegółowy wykaz czynności kontrolnych, pokrywający wszystkie etapy operacji APD, od podstawowych organizacyjnych i administracyjnych środków kontroli, aż do kontroli w zakresie sprzętu i bezpieczeństwa. Taki kompletny wykaz środków kontroli powinien zawierać także: środki kontroli przemieszczania i konwersji danych; środki kontroli stanów wyjątkowych systemu i programów; środki kontroli opracowania, obsługi i dokumentacji, a także środki kontroli proceduralne dla bezpieczeństwa i obsługi komputera.

Sprawozdanie wnioskuje, że dokumentacja jest w dalszym ciągu kluczem do dostatecznej kontroli systemu, i podczas gdy wiele grup APD podziela ten punkt widzenia, to jednak odpowiednia dokumentacja jest bardziej wyjątkiem niż regułą.

Szybko rosnące tempo zmian technologicznych jest nowym obszarem do uwzględnienia przez rewidenta APD. Coraz bardziej ważną sprawą staje się identyfikacja końcówki i użytkownika, bowiem nowa generacja końcówek zdalnego dostępu, pozwala praktycznie każdemu wejść w kontakt z systemem. Hasła są obecnie najbardziej powszechną formą identyfikacji, lecz gubienie i zapominanie kodów występuje tak często, że co najmniej jeden z systemów dostarcza tę formę identyfikacji w sposób zrutynizowany dla każdego użytkownika na zwykłe żądanie.

Inną dziedziną wymagającą uwagi rewidenta APD jest kwestia fizycznego bezpieczeństwa środowiska APD, a w przyszłości prawdopodobnie będzie on musiał poświęcać więcej uwagi tym sprawom. Już kilka dużych instalacji przetwarzania danych zostało poważnie uszkodzonych przez bojówki i grupy radykalne, i być może, nie jesteśmy zbyt oddaleni od czasów, w których instalacje APD zejdą pod ziemię celem ochrony.

Zabezpieczanie właściwie rozpoczyna się na etapie planowania i projektowania systemu i jest bardzo ważną sprawą, by raz ustanowione procedury zabezpieczenia miały zastosowanie do każdego, bez wyjątku, kto działa w środowisku APD. Odpowiednie środki kontroli posiadają żywotne znaczenie dla bezpieczeństwa systemu, lecz autorzy sprawozdania sądzą, że w ostatecznym wyniku o przetrwaniu bezpiecznej i dobrze sterowanej operacji APD decyduje uczciwość jej pracowników.

Lekcja, której udzielił kosztowny pożar w Pentagonie, przyczyniła się znacznie do obecnych poglądów na temat strukturalnego zabezpieczenia instalacji komputera przed zniszczeniem przez ogień, dym oraz wodę. Szczególnie ważne są tu dostateczne i kompatybilne procedury zastępcze, które muszą być stale aktualizowane w celu uniknięcia nieprzewidzianych komplikacji.

Szeroka dostępność elektronicznego sprzętu podsłuchowego wzbudziła obawy na temat przechwytywania danych między zdalnymi końcówkami a bankiem danych. Jak twierdzą autorzy w chwili obecnej nie jest to problem groźny i nie jest prawdopodobne, by stał się nim w bliskiej przyszłości. O ile powstanie potrzeba, należy się spodziewać, że będą dostępne w handlu urządzenia szyfrujące, lecz potencjalni producenci tych urządzeń stwierdzają, że obecnie nie ma na nie zapotrzebowania na rynku.

I. WPROWADZENIE

A. Tło badań

Wiele ze środków kontrolnych, mających obecnie zastosowanie do przetwarzania na komputerze, wzięto z procedur, jakie stosowali księgowi, gdy wykonywali te same prace ręcznie. Księgowy podsumował swoje pozycje w dół strony /suma wzdłużna/ jak i w poprzek strony /suma poprzeczna/, a następnie dodawał te sumy, aby otrzymać sumę ogólną. Suma ogólna musiała się zgadzać w obu kierunkach. Księgowy wiedział, że ma do zaksięgowania pewną liczbę pozycji i kiedy je zaksięgował, zliczenie tych zaksięgowanych pozycji powinno się zgadzać z liczbą, od której rozpoczął operacje. Jego obowiązki polegały na zdjęciu odpowiedniej księgi rachunkowej z półki, położeniu nowych pozycji obok niej na stole, oraz na zapisaniu tych nowych w książce. Także kontrolował on prawidłowość tych nowych pozycji przed wprowadzeniem ich do księgi.

Z chwilą gdy procedury stosowane w księgowości zostały przeniesione do automatycznych systemów przetwarzania danych, księgi rachunkowe stały się znane jako zbiory, nowe pozycje nazwano wejściem, proces księgowania nowych pozycji nazwano aktualizacją, sprawdzanie nowych pozycji nazwano redakcją, a zabezpieczenia przed błędami zostały nazwane obecnie środkami kontroli. Od tego czasu środki kontroli stały się bardziej wyszukane, lecz w APD są one zbyt często ignorowane lub za rzadko używane, z powodu braku zrozumienia ze strony personelu rewizyjnego oraz personelu przetwarzania danych, jak również z powodu innych przyczyn.

Historia dostarcza nam przykładów wielu strat, które poniesiono wskutek braku prawidłowych środków kontroli. Kiepsko kontrolowane systemy kosztowały przemysł wiele milionów dolarów. Wszyscy słyszeli co najmniej kilka tego rodzaju historii

o stratach, zwłaszcza gdy wchodziły w grę sprzeniewierzenia. Opowieści o defraudacjach podniecają publiczność i zwykle są podawane jako rażące przykłady omylności komputerów. Jednak znający się na rzeczy rozpoznają te przypadki jako oczywiste przykłady zaniedbania najbardziej podstawowych czynności zabezpieczających. W większości przypadków zwykły rozdział obowiązków byłby nie dopuścił do powstania przestępstwa. Ten sposób zapobiegania jest co najmniej tak długo stosowany jak sama rewizja. Niezmuszanie pracowników, by brali urlopy jest podstawowym zaprzeczeniem zasad kontroli, a niestosowanie takiego zabezpieczenia przyczyniło się do powiększenia listy podniecającej lektury na temat sprzeniewierzeń. Banki zapytują się jak zabezpieczać się w stosunku do programistów, którzy skierowują kapitały na swoje własne konta przez dokonywanie manipulacji w systemie. Stało się to źródłem niemałej liczby defraudacji. Tak samo podstawową sprawą, jak rozdział obowiązków, jest okoliczność, że programista przede wszystkim nie powinien mieć konta w tym banku. A mimo to wiele banków upiera się przy tym, by ich pracownicy zakładali w nich swoje konta bankowe.

B. Wnioski

Najważniejsze wnioski sformułowane w niniejszym sprawozdaniu można przedstawić w streszczeniu, jak następuje:

. w miarę wzrostu wykorzystania komputera i przenikania APD w coraz większym stopniu, do działalności przedsiębiorstwa, powstaje potrzeba wyznaczenia przedstawiciela kierownictwa, który byłby świadom nie tylko zamierzeń i celów przedsiębiorstwa, lecz także wynikających z tego skutków prawnych, przepisów archiwizacji, wymagań w zakresie rewizji działalności przedsiębiorstwa itp. Działanie jakiegokolwiek zespołu projektowania systemu bez takiego przedstawiciela - rewidenta APD może przyczynić się do powstania niepowodzeń w takiej czy innej formie,

. powszechnie przyjmuje się, że aczkolwiek środki kontroli są konieczne dla wykrywania i uchronienia się przed błędnymi operacjami, to jednak, by z nich korzystać należy poświęcić czas i elastyczność działania. Pomimo, iż w tym argumencie jest zawarte nieco prawdy, nie posiada on wielkiej wartości. Na dłuższą metę, zaoszczędzony czas komputera i personelu przez to, że nie trzeba powtarzać przebiegów - oraz pieniądze zaoszczędzone przez uchronienie się przed błędnymi danymi wyjściowymi - więcej niż uzasadnia koszt spowodowany ustanowieniem i utrzymaniem środków kontroli,

. dla każdego kiedykolwiek zaprojektowanego systemu, najważniejszym środkiem kontroli zawsze była dokumentacja tego systemu - jest to fakt od dawna uznany i często podkreślany. Pomimo to dokumentacja jest w dalszym ciągu traktowana jak zło konieczne,

. sprzeniewierzenia zamierzone nie są uważane na ogół za ważny problem. Przedsiębiorstwom bardziej zależy na kontroli błędów, które prowadzą do niesprawności lub nieprawidłowości, lub które mogą prowadzić do przypadkowych sprzeniewierzeń,

. przedsiębiorstwa opracowują bazy danych oraz zastosowania, w zakresie przetwarzania na bieżąco dla operacji systemami przemysłowymi i handlowymi. Wynikająca z tego koncentracja wrażliwych danych oraz możliwość zdalnego do nich dostępu wymagają zachowania ścisłych procedur zabezpieczenia,

. zatrudnienie w przemyśle rewidentów APD wzrasta szybko, w miarę jak przedsiębiorstwa rozpoznają, że udział rewidenta w etapie planowania systemu jest konieczny, by posiadać dobrze kontrolowany system. Także jest zadaniem trudnym i kosztownym dołączenie niezbędnych technik zabezpieczenia już po wdrożeniu systemu.

C. Zakres i metodologia

Obszerne omówienie wszystkich kategorii i rodzajów kroków zapobiegawczych nie wchodzi w zakres niniejszego sprawozdania; dla tego celu odsyła się czytelnika do świetnych publikacji zestawionych w bibliografii. Także sporządzono odsyłacz w tekście i w bibliografii do specyficznych wypowiedzi, dotyczących wymagań w zakresie bezpieczeństwa, metod zapobiegania katastrofie, oraz do innych opublikowanych materiałów, tam gdzie uznano to za właściwe. Tak więc intencją niniejszego sprawozdania, skierowanego do kierownictwa, jest ustanowienie podbudowy dla zrozumienia wymagań i technologii w omawianym zakresie.

Szczególny nacisk położono na osiągnięcie ścisłej kontroli systemów. Idzie tu głównie o ośrodki obliczeniowe, obsługujące pewną liczbę klientów /przedsiębiorstwa oferujące usługi obliczeniowe w warunkach wielodostępu, operacje w ośrodkach usługowych ogólnie dostępnych itp./. Może wówczas powstać zagadnienie odpowiedzialności prawnej w zakresie nieupoważnionego ujawniania informacji prywatnej lub prawnie zastrzeżonej. W tego rodzaju środowisku są godne polecenia pewne normalne wojskowe środki ostrożności, takie jak narzucenie ograniczeń od strony "potrzeby informowania". Z konieczności takie podejście prowadzi do powstania sytuacji polegającej na ścisłym rozgraniczeniu obowiązków /funkcji/ i do braku wglądu do całości systemu ze strony jakiejkolwiek osoby. Oczywiście w środowisku mniej wyizolowanym atmosfera może być mniej sformalizowana, dopuszczając większą wymianę informacji, oraz nakładanie się obowiązków.

Całokształt sprawozdania zajmuje się następującą tematyką:

- podstawowymi kategoriami środków kontroli oraz ich celami, możnością ich stosowania oraz potencjalnymi konsekwencjami w razie ich zaniedbania,
- metodami i znaczeniem inspekcji, szczególnie w erze wieloprogramowości i zdalnego dostępu,

- krokami zapobiegawczymi w zakresie bezpieczeństwa dla całego środowiska przetwarzania danych, włączając w to użytkowników oraz personel obsługi systemu,
- zmieniającą się rolą wewnętrznego rewidenta w APD, jego współczesnymi kompetencjami oraz aktualnym nań popytem w stosunku do jego podaży.

Dodatkowo sprawozdanie zawiera odpowiednio opracowane streszczenie z niedawnej, poświęconej temu tematowi narady roboczej, oraz przykładową listę kontrolną działalności rewizyjnej w APD, aktualnie używaną w pewnym dużym przedsiębiorstwie.

Metodologia, którą posługiwano się podczas opracowania niniejszego sprawozdania składała się z: przeglądu literatury, zestawienia i opisu przykładów dotyczących wykorzystania komputerów w sprzeniewierzeniach i malwersacjach, wywiadów studialnych z pewnym przekrojem rewidentów, personelu przetwarzania danych, banków i innych większych użytkowników oraz producentów sprzętu, jednodniowej narady roboczej Programu Badawczego Diebold'a w USA oraz z analizy wniosków.

II. ADMINISTRACYJNE ŚRODKI KONTROLI

Środki kontroli - są to procedury nałożone na system celem zapewnienia właściwego manipulowania wejściem, niezawodnego przetwarzania danych, dokładności wyjścia, oraz celem zapewnienia fizycznego bezpieczeństwa informacji oraz sprzętu, które są częścią roboczego środowiska systemu.

Dobrze zdefiniowany program technik zabezpieczających narzuca na system pewien porządek działania, jeśli go się będzie stosować - to chroni on przed stratami z powodu zamierzonych lub przypadkowych sprzeniewierzeń, a także podnosi wydajność. Wyobrażenie, że techniki zabezpieczające podnoszą wydajność, nie cieszy się zbytnią popularnością. Powszechnie przyjmuje się, że są one konieczne dla wykrywania i uchronienia się przed błędnymi operacjami, i że dla nich poświęca się

czas i elastyczność. Pomimo, że w tym argumencie tkwi nieco prawdy, nie posiada on wielkiej wartości. Na dłuższą metę zaoszczędzony czas komputera i personelu przez to, że nie trzeba powtarzać przebiegów - oraz pieniądze zaoszczędzone przez uchronienie się przed błędnym wyjściem - więcej niż uzasadniają pracę włożoną w ustanowienie technik zabezpieczających.

Zalety i wady tzw. zakładu "otwartego" /"open" shop/- gdzie każdy ma dostęp do sali komputera - oraz środowiska kontrolowanego - z dokładnie określonymi kanałami podawania danych, planowaniem przebiegów, bibliotekarzem taśm - powinny być oczywiste. Lecz o ile już ochrona została ustanowiona, rozsądną linią postępowania jest stosować kontrolę na wszystkich szczeblach; reguły, które mają zastosowanie do personelu operacyjnego muszą także być stosowane do kierownictwa.

A. Organizacyjne środki kontroli

Sprzeniewierzenie we właściwie zaprojektowanym systemie wymaga zmówienia się. I im lepiej ten system jest kontrolowany, tym większy jest wymagany stopień zmowy. Stąd wywodzi się zasada podziału obowiązków, tzn. osoba, która zapoczątkowuje daną transakcję nie jest tą samą osobą, która ją wykonuje.

Powyższa zasada wymaga także niezależności wydziałów. Na przykład wydział przetwarzania danych musi być niezależny od wydziałów wykorzystujących komputer. Z powodu istoty przetwarzania danych wiele procedur, które kiedyś było wykonywane niezależnie od siebie, w czasach działalności ręcznej, obecnie jest scalonych, przy czym ogół operacji jest skoncentrowany w komputerze. Wynikające z tego faktu słabe punkty systemu nie powinny stanowić okazji do wyciągania korzyści przez wydziały użytkownika.

Wewnątrz wydziału przetwarzania danych w rzeczywistości istnieją trzy grupy ludzi, przy czym każda z nich posiada rozgraniczone obowiązki, i logika wymaga, by funkcjonowały one, o ile to jest możliwe, oddzielnie. Chodzi tu o grupy: systemu, operowania oraz kontroli.

1. Grupa systemu

Grupa systemu zawiera analityków, projektantów i programistów. Wiedzą oni dokładnie jak system pracuje i dlatego zespolenie ich wiedzy z dostępem operatorów do komputera stwarza potencjalnie niebezpieczną sytuację. Istnieje mało powodów dla bezpośredniej łączności między nimi, a takim kontaktom powinno się być przeciwnym.

2. Grupa operacyjna

Grupa operacyjna /operatorzy/ ma dostęp do komputera, do danych oraz do systemów. Operatorzy potencjalnie mogą wyrządzić najwięcej szkód i wydaje się oczywiste, że przed ich przyjęciem do praoy powinna być gruntownie sprawdzona ich przeszłość. I jest rzeczą zadziwiającą, że w niektórych opisywanych przypadkach sprzeniewierzeń w instytucjach finansowych wszyscy w danej firmie byli przyjęci za kaucją z wyjątkiem personelu przetwarzania danych. Ponieważ przetwarzanie danych jest jednym z najbardziej wrażliwych obszarów w przedsiębiorstwie, operatorzy powinni być pracownikami kontraktowymi i nie powinni pracować w pojedynkę.

3. Grupa kontroli

Grupa kontroli sprawuje nadzór nad środkami kontroli komputera. Dane wejściowe przedkładane są za pośrednictwem tej grupy, która sprawdza, czy dołączono sumy kontrolne itp. i czy prawidłowo zestawiono komplet dokumentów wejściowych. Grupa ta, do której należą bibliotekarze taśm i dokumentacji, sprawdza książkę kontrolną maszyny, wydruki sum kontrolnych i wyjątków, oraz zajmuje się rozdziałem wyników wyjściowych, po sprawdzeniu ich prawidłowości. Grupa jest łącznikiem między operatorami a użytkownikami i programistami, a jej rola nadzorcza wymaga, by była od innych niezależna.

B. Inspekcja

Najważniejszą kontrolą wewnętrzną jest inspekcja, ponieważ właśnie przez inspekcję określa się dostateczność innych środków kontroli. Lecz gdy dochodzi do rozważań, jak należy to ro-

bić w APD oraz kto ma to robić, staje się to przedmiotem wielu dyskusji. Jedną z możliwych odpowiedzi jest ustanowienie personelu inspekcji APD; zagadnienie to jest osobno dyskutowane w rozdziale V pt. "Inspektor wewnętrzny w APD".

Techniki inspekcji zmieniały się wraz z opracowaniem nowych generacji komputerów. Zmiany technologiczne zmierzały do ułatwienia wykonywania bieżącej inspekcji, lecz jednocześnie dodały wymagania w zakresie znacznie bardziej wyspecjalizowanej ekspertyzy technologicznej. Ustanowienie trybu inspekcji jest obecnie bardziej złożonym problemem niż dotychczas, ale gdy się go raz ustanowi to wówczas można łatwiej uzyskać informację i będzie ona bardziej wartościowa.

1. Przetwarzanie partiowe /wsadowe/

Już od dłuższego czasu stosuje się przetwarzanie partiowe. W ciągu tego okresu czasu opracowano różne podejścia do zagadnienia inspekcji tych systemów. Początkowo przyjęła się metoda inspekcji "poza" komputerem, tzn. wykonywano próbne transakcje ręcznie - tak, jakby nie było komputera - i porównywano wyniki z wynikami z komputera. Z postępem technologii powyższa metoda wyszła z użycia i obecnie do wykonywania czynności inspekcji wykorzystuje się komputer.

Następnie zaczęto używać plików danych próbnych - plików danych zaprojektowanych w celu sprawdzenia /przetestowania/ różnych stanów i funkcji sterujących /kontrolnych/ w programach. Metoda ta jest w dalszym ciągu rozpowszechniona. Pliki danych próbnych są użyteczne i pomocne, lecz posiadają swoje ograniczenia, szczególnie w systemach o pewnej złożoności. Przepuszczenie przez system pliku danych próbnych powoduje sprawdzenie programów tylko w tym stanie w jakim istnieją one w komputerze w chwili testowania, lecz trzeba pamiętać o tym, że każdy system jest stale ulepszany i prawdopodobnie mogą zaistnieć w nim zmiany dokonane nawet na następny dzień po jego sprawdzeniu. Także oszukańcze sekcje programów mogą zmniejszyć niezawodność pliku danych próbnych. Sekcje te są omijane przez pewne ustawienie kluczy wyłączających, a także pewne kody mogą włączać "oszustwo", które nie będzie wykryte przez plik danych próbnych, nie posiadający tych kodów.

Czasami jest trudno wydać z przekonaniem pewną opinię na temat technik zabezpieczenia w systemie na podstawie tylko wyników przebiegów na danych próbnych. W celu uzyskania większej pewności, często jest konieczne poparcie tej formy badań innymi badaniami oraz przeglądem wylistowania programu. Jednakże wymaga to od rewidenta pewnej wiedzy w zakresie języków programowania.

2. Programy inspekcji

Jeśli komputer ma być użyty jako pomoc w czynnościach inspekcji, to następnym logicznym krokiem jest opracowanie programów, które wykonywałyby pewne funkcje rewizyjne. Zakres tych programów może się rozciągać od zwykłych procedur porównywania taśm, które porównują dwie taśmy i następnie robią wydruk niezgodności /zastrzeżeń/ aż do złożonych modeli systemów poddawanych inspekcji.

O ile rewident posiada kopię oryginalnej taśmy systemu, może on przeprowadzić porównanie między tą taśmą a taśmą będącą aktualnie w użytku. Wykazane różnice powinny odpowiadać zmianom dokonanym w systemie, które są zapisane w dokumentacji. Jeśli to nie ma miejsca, to znaczy, że dokonano nielegalnych lub nie zarejestrowanych zmian, lub że dokumentacja jest nieaktualna. Dla każdorazowych następnych inspekcji można wykorzystywać ostatnią aktualną taśmę.

Rewident może rozporządzać przygotowanymi programami, w których przewidziane są takie techniki zapobiegawcze, które uważa on za konieczne dla systemu. Zestaw danych wejściowych podanych za pomocą tych programów w regularnej eksploatacji systemu ujawni każde niezgodności /zastrzeżenia/ meldowane przez system. Na przykład w programie tworzącym listę wypłat, rewident może przygotować własną jego wersję wcielającą te wymagania, które według jego odczucia powinny się znaleźć w programie użytkownika. Porównanie tych dwóch wersji odsłoni naruszenia technik zapobiegawczych w programie użytkownika.

Do systemu mogą być włączone specyficzne programy sprawdzające, używane, gdy zachodzi konieczność skontrolowania systemu. Mogą one być inicjowane na żądanie lub losowo - przez komputer, w celu próbkowania danych przepuszczanych przez

system. Tym niemniej przy tym podejściu do zagadnienia istnieje możliwość powstania problemu zabezpieczenia, ponieważ jakiś intruz może dostać się do programów sprawdzających i je zmienić.

Programy inspekcji mogą być opracowywane własnymi siłami, lecz taka decyzja musi być poprzedzona skrupulatną analizą efektywności nakładów. Zbadanie kosztów może wykazać, że dla pewnych procedur, takich jak pobieranie próbek, stosowanie programów inspekcji jest grubą przesadą. Dogłębne sprawdzanie może okazać się niepotrzebne, a uzyskana dodatkowa dokładność może być tylko kosztownym upiększeniem. Z drugiej strony nakłady poniesione na opracowanie programów inspekcji mogą się już zwrócić po kilkukrotnym ich zastosowaniu.

Pewne publiczne przedsiębiorstwa usług z zakresu księgowości opracowały uogólnione programy inspekcji. Są one dostępne w sprzedaży lub dzierżawie. Prosty język użytkowy dostarczany z tymi programami pozwala użytkownikowi na wskazanie w programach, których funkcji wykonanie zakłada się w przebiegach na komputerze.

Nabywanie programów inspekcji na zewnątrz jest czasami bardziej ekonomiczne niż opracowywanie ich własnymi siłami, lecz zwykle w związku z korzystaniem z nich powstają problemy ugólnienia. Każde przedsiębiorstwo ustala format danych według własnej wygody i zwykle jest on niezgodny z wymaganiami programów uogólnionych. Format danych można zmieniać za pomocą języka dostarczanego z takim programem. Język ten może się wydawać łatwym dla fachowców, lecz inspektor prawdopodobnie będzie się musiał oprzeć na pomocy programisty przy pisaniu rozkazów. Na ogół stwierdzono, że omawiane programy są ekonomiczne przy ich stosowaniu na dużych zbiorach danych, oraz że nie powinny one być używane na małych zbiorach. Ogólnie biorąc, większość użytkowników tych programów była z nich zadowolona.

Dalszą, dostępną w handlu, pomocą z zakresu oprogramowania dla rewidentów są oprogramowania oferowane przez niektóre biura /tzw. software houses/. Są to programy, które wykonują schematy blokowe /inaczej: funkcjonalne/ innych programów. Inspektor może za ich pomocą sporządzić schematy blokowe programów systemu i następnie porównać je z zawartymi w dokumentacji.

3. Miniprzedsiębiorstwa

Obecnie coraz przychylniejsze przyjęcie uzyskuje technika stałej inspekcji oparta na koncepcji "miniprzedsiębiorstwa". Tworzy się nieistniejące wydziały, zapełnia fikcyjnymi pracownikami, wyznacza się dla nich budżet itd. i oznacza za pomocą specjalnych kodów w celu łatwej ich identyfikacji. Te wydziały figurują w tych samych zbiorach, co prawdziwe /rzeczywiste/ wydziały i są traktowane przez system tak jakby naprawdę istniały, lecz ich wyjście jest oddzielane od wyjścia dla rzeczywistych wydziałów. Dane próbne przebiegają razem przez te same operacje i te same stany co dane rzeczywiste i są poddawane tym samym technikom zapobiegawczym co dane faktyczne.

Zaletę tego podejścia stanowi testowany system, który jest dokładnie tym samym systemem, używanym do przetwarzania regularnych danych, przy czym testowanie jest łatwe i nie wymaga dużej ilości dodatkowego oprogramowania.

Wadą jest tu specjalne traktowanie konieczne dla fikcyjnych wydziałów, oraz podatność na machinacje. Sprytny programista może zmienić system tak, by te zakodowane wydziały były inaczej traktowane. Ogólnie biorąc, zalety, jak to stwierdzono, przewyższają wady, skoro powyższa metoda znajduje coraz większe zastosowanie.

4. Systemy przetwarzające na bieżąco

Systemy przetwarzające na bieżąco stwarzają dla rewidentów nowe problemy, gdyż kilku użytkowników ma dostęp do systemu jednocześnie i każdy z nich dokonuje dostępu do tych samych zbiorów z terminali zainstalowanych w różnych miejscach. Istnieje możliwość ciągłej aktualizacji z każdego miejsca, kopie wprowadzanych do systemu zapisów /na papierze/ przechowywane są w tych zdalnych miejscach dostępu do komputera. Utrudnia to znacznie prześledzenie drogi od bieżącej zawartości zbioru do źródła transakcji, które się do tego przyczyniły.

Istnieją cztery główne obszary zainteresowania, które dogłębna inspekcja systemu przetwarzającego na bieżąco powinna szczegółowo wziąć pod uwagę. Chodzi tu o: procedury wydawni-

cze, które sprawdzają ważność /prawomocność/ i sensowność danych wejścia, techniki zapobiegawcze w celu upewnienia się, by nie zachodziło równoczesne aktualizowanie zbiorów, procedury restartu oraz rejestracją dostępów do zbiorów.

Szczegóły technik kontrolnych, które powinien stosować inspektor podano w rozdziale III pt. "Środki kontroli systemu".

a. Procedury wydawnicze

Procedury wydawnicze są ważne w każdym systemie, lecz w systemach przetwarzających na bieżąco posiadają krytyczne znaczenie. Ponieważ system otrzymuje dane wejściowe ze zdecentralizowanych źródeł przy braku gwarancji znajomości rzeczy ze strony użytkownika wprowadzającego dane, przyjęcie danych powoduje aktualizację zbiorów, a zbiory zaktualizowane służą z kolei do aktualizacji innych zbiorów i wówczas skutki wynikające z niewłaściwie wprowadzonych danych są oczywiste.

b. Równoczesne aktualizowanie

Weźmy pod uwagę dwóch ludzi korzystających z dostępu do jakiegoś zbioru w tym samym czasie, aby go zaktualizować. Kiedy będą oni zapisywać zbiory z powrotem do bazy danych, jedna z tych aktualizacji zostanie wymazana przez drugą. W systemie nadzorczym powinny istnieć techniki zapobiegawcze, które nie dopuszczają dostępu do zbioru, jeśli już miał raz miejsce dostęp do niego w celu aktualizacji. Inspektor powinien sprawdzić czy te techniki zapobiegawcze działają prawidłowo.

c. Procedury restartu

Trudność rekonstrukcji zbiorów narzuca stosowanie częstych punktów kontrolnych dla dokonania wypisów informacji, by mieć pewność, że dostateczna ilość prawidłowej informacji istnieje na zewnątrz komputera w wypadku awarii. Ma to na celu umożliwienie systemowi powiadamianie użytkowników, które komunikaty i w jakim porządku mają oni przesłać ponownie, by spowodować powrót systemu do stanu, w którym powinien się

znajdować. Inspektor powinien pieczołowicie upewnić się, że zachowuje się odpowiednią informację, oraz że zachowuje się ją wystarczająco często.

d. Rejestry dostępu

Systemy przetwarzające na bieżąco prowadzą rejestry transakcji, które wykazują, kto miał dostęp do zbioru, dla jakiego celu, i jakie miał ku temu upoważnienie. Te dane są potrzebne systemowi dla celów restartu. Jednakże inspektor może je oczywiście wykorzystać w swych czynnościach kontrolnych. Faktycznie może on napisać programy na komputer tak, by analizować informację zawartą w tych rejestrach w dowolny, interesujący go, sposób.

Inspekcje systemów przetwarzających na bieżąco powinny być dokonywane częściej niż zazwyczaj. Jest to uzasadnione stale zmieniającym się charakterem zbiorów. Lecz te częste inspekcje będą miały bardziej charakter przeglądu sprawozdania o odchyleniach od normy. Faktycznie rewident może posiadać terminal zainstalowany w jego biurze tak, że może on dokonywać niespodziewanych inspekcji, nie opuszczając swojego biurka.

Kilka banków, w których zainstalowano systemy przetwarzające na bieżąco, informuje, że tam, gdzie kiedyś wykonanie inspekcji zajmowało całemu wydziałowi banku jeden dzień, obecnie wykonanie tych samych funkcji zajmuje dwóm ludziom około 15 minut. W praktyce dokonują oni obecnie co najmniej sześciu inspekcji dziennie.

C. Procedury wspierające

Celem procedur wspierających jest ułatwienie powrotu do stanu normalnego po zaistnieniu sytuacji katastrofalnej, przypadkowej lub umyślnie spowodowanej. Dwa - trzeba przyznać krańcowe - przykłady ilustrują dokładnie, co się może zdarzyć w przypadku przestrzegania - lub nieprzestrzegania - procedur wyprowadzających ze stanu katastrofalnego:

Niezadowolony pracownik wchodzi na salę komputera swojego przedsiębiorstwa ze zwykłym magnesem w kieszeni.

Ponieważ zna komputer oraz wartość zbiorów, rozpoczyna systematyczne niszczenie wszelkich danych przechowywanych na taśmach i dyskach, od najważniejszej informacji, aż do systematycznego zniszczenia wszelkich danych. Przedsiębiorstwo nie posiada zapasowego zabezpieczenia dla tych zbiorów; być może bez tych zbiorów przedsiębiorstwo będzie musiało przestać się liczyć na rynku. Nieprawdopodobne jest, by było ono w stanie zrekonstruować utracone zbiory.

W podobnym zdarzeniu w innym bardzo dużym przedsiębiorstwie, jeden z operatorów w czasie week-endu przedostał się przez straż i znalazł się sam w sali komputera. Włączył komputer i wymazał /skasował/ wszystkie zbiory na taśmach i dyskach, jakie tylko mógł znaleźć. Jednakże przedsiębiorstwo posiadało zapasowe kopie zbiorów, tak że szkody były minimalne.

Poza tym zawsze istnieje możliwość zwykłego, przypadkowego, wymazania /skasowania/ zbioru.

1. Współwymienny /zgodny/ komputer

Rozważania na temat procedur wspierających należy rozpocząć od dostępności współwymiennego /zgodnego/ komputera. Chociaż jest to sprawa oczywista, to jednak nie zawsze się to praktykuje. W pewnych przypadkach przedsiębiorstwa mogą uważać, że ich zapotrzebowanie na zupełnie różny nowy sprzęt przeważa nad koniecznością posiadania alternatywnych instalacji komputerowych w celu użycia w przypadku awarii itp. w nowym urządzeniu. Kierownictwo może zdecydować, że zabezpiecza tylko zbiory przed mechanicznym zniszczeniem. Inne przedsiębiorstwa poczyniły przygotowania w kierunku posiadania alternatywnych instalacji komputerowych, lecz nie poświęcają żadnej uwagi zagadnieniu współwymienności /zgodności/. Niektóre z przedsiębiorstw po prostu nie wzięły zagadnienia posiadania "zapasowego" komputera na wypadek awarii pod uwagę.

2. Oddzielenie komputerów

W większości ośrodków obliczeniowych wyposażonych w więcej niż jeden komputer, są one umiejscowione w jednej części przedsiębiorstwa, często w jednym pomieszczeniu. Posiadanie komputera wspierającego tuż obok zasadniczego, na wypadek przestoju tego ostatniego lub na wypadek nieprzewidzianego wzrostu zapotrzebowania na przetwarzanie jest w pewnym sensie uzasadnione, lecz jest całkowicie nie do przyjęcia jako zabezpieczenie w celu wyprowadzenia systemu ze stanu katastrofy. Nieszczęśliwy wypadek, który może zniszczyć jedną maszynę w tej konfiguracji, prawie na pewno dotknie inne maszyny. Na przykład w przypadku wybuchu pożaru w jednym z komputerów, sama działalność zwalczania ognia może zniszczyć przyległy komputer. W idealnym przypadku, wszystkie komputery danego ośrodka obliczeniowego powinny być umieszczone w osobnych pomieszczeniach.

3. Utrzymywanie kontaktu

Skoro już poczyniono kroki w celu uzyskania dostępu do współwymiennego komputera poza terenem przedsiębiorstwa, powinno się utrzymywać kontakt z tym ośrodkiem obliczeniowym. Jedno z przedsiębiorstw dokonało wszelkich uzgodnień z drugim przedsiębiorstwem, stwierdzając, że w nagłych wypadkach będzie mogło korzystać z zainstalowanego tam komputera. Kierownictwo pogratulowało sobie dobrze wykonanego zadania i na tym poprzestało. Nie mając potrzeby korzystania z tego "zapasowego" komputera, kierownictwo nie utrzymywało kontaktu z tamtym przedsiębiorstwem. Późniejsza inspekcja ujawniła, że przedsiębiorstwo, z którym dokonano uzgodnień, zmieniło komputery na inne i obecnie już nie zachodzi współwymienność sprzętu. Teraz najbliższy współwymienny komputer jest oddalony o przeszło 150 kilometrów i jest on obciążony pełne 24 godziny na dobę.

4. Archiwa

Procedury zachowywania oraz transportowania materiałów w celu bezpiecznego przechowywania poza obrębem danego budynku powinny mieć ustalone formy i tych form należy się trzymać. Nie jest niezwykłe, że nie przestrzega się ustalonego porządku tak często, że w końcu w ogóle zostaje zaniedbany.

Procedury można utrzymać "w świeżości" przez sporadyczne organizowanie przebiegów na "zapasowym" komputerze. Wynikiem takiej działalności może być także dodatkowe zabezpieczenie systemu przeciwko machinacjom operatorów lub programistów. Ten sam system eksploatowany w dwóch różnych miejscach powinien dostarczać w tych dwóch miejscach jednakowe odpowiedzi. Jeśli to nie ma miejsca, to albo nie została zachowana najnowsza wersja danego systemu w jednym z tych miejsc, albo ktoś dokonał machinacji.

W celu wyprowadzenia systemu z poważnej katastrofy, w zachowywanym materiale muszą się znaleźć zbiory główne, dane krytyczne /czyli o dużym znaczeniu dla działalności przedsiębiorstwa/, ostatnio zaktualizowane programy oraz zaktualizowana na dzień dzisiejszy dokumentacja. Powszechnie praktykuje się zachowywanie zaktualizowanych zbiorów głównych oraz taśm i dysków systemowych, lecz nie ma zwyczaju posiadania zapasowych kopii programów na kartach oraz ich dokumentacji, a także nie praktykuje się dokonywania zmian w zapasowych kopiach, ściśle według zmian wprowadzanych do eksploatowanych kopii programów. Oczywiście zbiory główne i dane są bezużyteczne, jeśli nie posiada się do działania na nich zaktualizowanych programów.

Urządzenia do magazynowania zachowywanego materiału mogą się bardzo różnić: od grot znajdujących się głęboko w górach do stojaka w sali komputera, tuż w pobliżu materiałów służących do bieżącej eksploatacji. Najbardziej rozpowszechnione są schrony w banku. Podejmuje się odpowiednie kroki w celu pobierania materiałów z ośrodka obliczeniowego, dostarczania ich do banku, oraz w celu zwrotu zdezaktualizowanego materiału do ośrodka obliczeniowego. Dalsze techniczne szczegóły na temat norm bezpiecznego przechowywania materiałów poza obszarem ośrodka obliczeniowego można znaleźć w pozycji bibliograficznej 9 - Standards for the Protection of Electronic Computer Systems, bulletin number 75, National Fire Protection Association /Normy ochrony elektronicznych systemów komputerowych, biuletyn nr 75, Narodowe Stowarzyszenie Ochrony Przeciwpożarowej/.

D. Zapobieganie katastrofie i wyprowadzanie systemu z katastrofy

Zapobieganie katastrofie jest dziedziną, w której należy się odwoływać do porad specjalistów. Tego rodzaju informacje i usługi oferują producenci komputerów, przedsiębiorstwa ubezpieczeniowe oraz niektóre firmy doradcze. Ideałem byłoby zwracanie się do nich już w momencie planowania ośrodka obliczeniowego. Jednakże ich porady mogą być także cenne w celu wykazania ryzyka, jakie zachodzi w już działających ośrodkach obliczeniowych.

Pierwszą poważną katastrofą, jaka dotknęła system komputerowy, był szeroko omawiany pożar w Pentagonie w 1959 roku /Ministerstwo Obrony USA/. Szkody materialne wyniosły blisko 7 milionów $, ale jednak skrajne oceny wartości zniszczonej informacji szacują wszystkie straty na co najmniej 30 milionów $. W załączniku B podano pełny opis tego wydarzenia.

Z tego doświadczenia wyciągnięto bardzo poważne wnioski i większość obecnych procedur zabezpieczenia przed pożarem wynikło z badań przeprowadzonych nad tą katastrofą. Towarzystwa ubezpieczeniowe opracowały specjalne polisy ubezpieczeniowe dla ośrodków przetwarzania danych. Można uzyskać ubezpieczenie na wypadek straty zapisów informacji, straty dochodu z ośrodka, wydatków związanych z korzystaniem z komputera na zewnątrz w okresie usuwania skutków awarii itd. Warunki, pokrycie finansowe oraz ceny można wynegocjować tak, by spełnić indywidualne potrzeby danego przedsiębiorstwa.

1. Ubezpieczenie

Producenci ubezpieczają swój sprzęt, a warunki dzierżawy zazwyczaj wypunktowują granice odpowiedzialności przyjętej z tytułu ubezpieczenia przez producenta. Nie zawsze oznacza to, że omawiane ubezpieczenie automatycznie obejmuje potrzeby, reprezentowane w tym zakresie przez dzierżawiącego sprzęt. Producent faktycznie prawie nie posiada kontroli nad tym, co może uczynić ubezpieczający go w przypadku katastrofy. O ile można udowodnić niedbalstwo, to wówczas wysoki koszt sprzętu może nakłaniać ubezpieczającego do próbowania

odzyskania tego kosztu od dzierżawiącego. W czasie omawiania kontraktu powinno się wynegocjować zrzeczenie się podstawienia /zrzeczenie się prawa domagania zwrotu pieniędzy/ od towarzystwa ubezpieczeniowego producenta.

2. Nowe ryzyko

Ostatni rozwój wydarzeń dał trochę do myślenia przedsiębiorstwom na temat wystawiania swoich komputerów na widok publiczny, tak jak to robiono w przeszłości. Ruchy "Młodzieżowe" i "Pokojowe" skłaniają się, by uważać komputer za symbol ustalonego Porządku, za narzędzie wojny, albo za symbol jednego i drugiego. Stanowi to zagrożenie fizycznego bezpieczeństwa komputera. Niejeden komputer poszedł z dymem w wyniku działalności demonstrantów.

Postawiono hipotezę, że za parę lat komputery znajdą się w podziemiach i będą dostępne tylko dla inżynierów. Rozwój wykorzystania terminali skłania do popierania tej hipotezy. Tak, jak wyciągnięto naukę z pożaru w Pentagonie, powinno się wyciągnąć wnioski z publicznych ataków na komputery.

Rozważanie tego problemu nie jest ograniczone tylko do Stanów Zjednoczonych. Podobne zamieszki występują i będą występowały w całej Zachodniej Europie.

III. ŚRODKI KONTROLI SYSTEMU

Dokładność wyjścia jest zależna od ustalenia technik zapobiegawczych we wszystkich aspektach systemu, począwszy od wejścia, poprzez przetwarzanie na komputerze, aż do wyjścia. Różne systemy będą miały różne wymagania w tym zakresie i należy stosować odpowiednie techniki zapobiegawcze, by je spełnić. Nie ma ogólnych prawideł określających, jaki zestaw technik zapobiegawczych będzie pasował do jakiegoś szczególnego systemu. W istocie rzeczy rodzaj technik zapobiegawczych jakie należy stosować, jest podyktowany przez wrażliwość informacji, cel oraz architekturę systemu.

A. Środki kontroli wejścia

Celem środków kontroli wejściowej jest upewnienie się, czy na wejściu znajdują się tylko prawidłowe dane; i dalej, czy

wszystkie dane,które z jakiejkolwiek przyczyny odrzucono,zostały właściwie poprawione i tylko jednokrotnie wprowadzone do systemu.

Według ustalonej tradycji dane zbiera się z dokumentu źródłowego i składa w partię. Następnie dla danej partii wylicza się sumy kontrolne pionowe i poziome. Partie danych wydziurkowywuje się na kartach lub taśmie papierowej, a następnie się je sprawdza. Operator, który sprawdza dane - musi być zawsze inną osobą od tej, która wykonuje pierwsze dziurkowanie. Dane, skoro już przedłoży się je systemowi, są redagowane przez program w systemie, który sprawdza ich ważność oraz sensowność.

Kroki zapobiegawcze w zakresie wejścia do systemu rozpoczynają się na etapie dokumentów źródłowych, takich jak faktury i zamówienia. Zwykle zajmuje się tym grupa ludzi, która sprawdza dokładność dokumentów źródłowych. Powinno się robić analizę statystyczną tych błędów, jakie prawdopodobnie mogą wystąpić w dokumentach źródłowych. Będzie to wytyczną dla niezbędnego poziomu kontroli.

Jedno z ankietowanych przedsiębiorstw posiadało personel składający się z 15 osób dokładnie sprawdzających każdą wchodzącą fakturę. Analiza statystyczna wykazała, że zaniechanie sprawdzenia faktur opiewających na sumę poniżej 500 $ spowoduje stratę w wysokości nie mniej niż 3.300 $ - czyli mniej niż połowa poborów jednego pracownika. Jeśli nie będą sprawdzane faktury poniżej 1.000 $, straty wyniosą nieco ponad 5.000 $, lecz cała wymagana liczba czynności kontrolnych mogłaby wówczas być wykonana przez trzech ludzi.

Przedsiębiorstwa Lockheed of California oraz Kaiser Aluminium ustaliły raczej rewolucyjny sposób podejścia do ich transakcji dotyczących rachunku "wierzyciele". Te systemy opisano szczegółowo we wcześniejszej pracy studialnej pn."Działalność finansowa oraz przetwarzanie informacji" /Financial Activity and Information Processing, dokument nr E35/.

Omawiane przedsiębiorstwa wyeliminowały faktury sprzedawców ze swoich systemów. Już tylko w pierwszym roku Lockheed zrealizowało oszczędności w wysokości 200.000 $ z tego nowego systemu, a w przedsiębiorstwie Kaiser w pierwszym roku

działania systemu doprowadziło to do oszczędności w wysokości około 300.000 $.

1. Dziurkowanie kart/taśmy papierowej oraz sprawdzanie

Gdy dane zostaną wydziurkowane, inny operator powtarza tę procedurę na innej klawiaturze, specjalnie skonstruowanej dla porównania danych oraz dla wykazania błędów. Taka kontrola pochłania bardzo wiele czasu i dlatego wiele przedsiębiorstw podjęło środki w celu zmniejszenia czasu potrzebnego do sprawdzania. Tu pomocne jest korzystanie z możliwie dużej ilości danych, które nie muszą być sprawdzane. Zmniejszenie liczby danych, które trzeba wydziurkować i sprawdzić można uzyskać przez odpowiednią konstrukcję systemu, taką że dane wczytane doń raz zostają zapisane w tablicach i można je wielokrotnie pobierać. Prowadzenie analiz na temat rodzaju i liczby błędów, które występują, często wykazywało, że nie jest konieczne sprawdzanie wszystkich wydziurkowanych danych. Jedno z ankietowanych przedsiębiorstw nie dokonywało w ogóle sprawdzania, zostawiając wykrywanie błędów programowi redagującemu.

2. Wejście do systemów pracujących na bieżąco

Wejście do systemów pracujących na bieżąco rzadko wykonuje się za pomocą kart lub taśmy dziurkowanej. Dane do systemu są wprowadzane ze zdalnych terminali przez operatorów o różnym poziomie wiedzy fachowej. W tym środowisku procedury redagujące przyjmują na siebie decydującą rolę. Ogólnie biorąc, wymagane jest, by każdy dialog między maszyną /systemem/ a terminalem był inicjowany przez komunikaty zawierające takie informacje, jak identyfikacja terminalu i użytkownika, czas, data oraz upoważnienie. Skoro tylko system przejdzie przez tę procedurę przyjmowania, użytkownik rozpoczyna transmisję danych, a następnie podprogramy redagujące mogą przeprowadzić weryfikację wprowadzanych danych.

3. Procedury redagujące

Procedury redagujące zaprojektowano dla ściśle określonych systemów. Skoro tylko użytkownik wyspecyfikuje zbiory, na których chce pracować, omawiane procedury w pierwszym rzędzie

kontrolują etykiety zbioru. Zawartości etykiet zbioru ustala się także dla poszczególnych systemów. Ogólnie biorąc, etykieta początkowa /lub skorowidz zbioru/ powinna zawierać identyfikację zbioru i systemu, który na tym zbiorze pracuje, daty, do których ważne są informacje w zbiorze, formaty danych i klucze upoważniające do dostępu oraz inne informacje istotne dla systemu. Etykieta końcowa, jeśli taka istnieje, powinna zawierać informację sterującą,taką jak: czy za nią następuje dalsza szpula /taśmy/ lub ścieżka /na dysku/, albo czy jest to koniec zbioru,oraz powinna zawierać sumy kontrolne dla informacji dotyczącej tej części zbioru.

Formaty dla różnych wejść do systemu są znane procedurze redagującej poprzez informację przechowywaną w etykietach lub skorowidzach zbiorów, a dane wprowadzane do systemu są sprawdzane pod względem ich przystosowania do tych formatów, tj. czy: nie brakuje żadnych danych o ile powinny się tam znajdować, w polach numerycznych nie znajdują się dane alfabetyczne i na odwrót, czy dane są zawarte w określonych uprzednio granicach, na przykład czy numery rachunków lub numery wydziałów korespondują ze zbiorem usankcjonowanych liczb lub bilansują się z ich cyframi kontrolnymi,i dalej czy wejścia są uporządkowane sekwencyjnie,oraz wszelkie inne próby wymagane przez system w stosunku do danych.

Procedura redagująca nie daje żadnej możliwości sprawdzenia, czy dane są ścisłe, może jedynie sprawdzić,czy dane posiadają sens w warunkach systemu. Na przykład numer ewidencyjny pracownika występujący w systemie obliczania płac może być 4475. Numer ten nie posiada znaków alfabetycznych. Jeśli numery ewidencyjne pracowników zawsze znajdują się między wartościami 1000 a 5000, to liczba ta jest sensowna. Sprawdzenie czynnego zbioru pracowników może wykazać, że pod numerem 4475 figuruje aktualnie zatrudniony pracownik, oraz że pracuje on w wydziale, który wskazuje związana liczba dla wydziału. Liczba jest ważna /prawomocna/, lecz w dalszym ciągu jest możliwe, że ta liczba powinna posiadać wartość 4473.Nie ma sposobu, by procedura redagująca mogła to rozpoznać.

Istnienie logicznych współzależności między różnymi polami na wejściu może być bardzo pomocne w znajdowaniu błędów. Jakiś kod może być sensowny i ważny jeśli się zgadza z innym

kodem. Jego nieważność wychodzi na jaw wówczas, gdy nie zachodzi ta zgodność. Na przykład gdy na wejściu wprowadza się zarówno nazwisko pracownika, jak i jego numer, odpowiednia procedura może je porównać ze zbiorem zawierającym dane personalne, by upewnić się czy te dane są zgodne.

Wyjątki znalezione w danych muszą być bardzo szczegółowo wykazane przez procedurę redagującą. Niewiele warta jest wiadomość o tym, że w wejściu zawarte są błędy, jeśli nie wiadomo gdzie i jakie one są. Decydowanie o postępowaniu z błędami zależy całkowicie od systemu.

W niektórych systemach procedury redagujące przekształcają dane wejściowe wg określonego kodu w celu ich zapamiętania. Na przykład nazwy alfabetyczne miesięcy mogą być przekształcone na kod dwucyfrowy, gdzie STY lub STYCZEŃ byłby przekształcony na 01, LUT lub LUTY - na 02 itd. Celem tego działania jest oszczędzanie pojemności pamięci, lecz wówczas podczas wyprowadzania danych na wyjściu musi zachodzić drugie przekształcanie w celu zamiany kodu wewnętrznego na format czytelny dla użytkownika.

4. Redagowanie w systemach pracujących na bieżąco

Procedury redagujące zależą od systemu, w którym mają być użyte. W systemach pracujących na bieżąco najważniejszą cechą jest szybka odpowiedź, a redagowanie zabiera czas. Lecz nieścisłe dane, jeśli zostaną dopuszczone do systemu, mogą w wyniku spowodować wadliwą aktualizację kilku zbiorów. Wielu projektantów systemów pracujących na bieżąco woli poświęcić natychmiastową odpowiedź na korzyść niemal natychmiastowej odpowiedzi, ale zapewnić przy tym ścisłość danych. Procedury redagujące w systemach pracujących na bieżąco określają upoważnienie użytkownika /do dostępu do systemu/, sprawdzają wejście, zapisują komunikaty w rejestrze oraz wprowadzają pozycje do rejestru badań kontrolnych.

Problemy mogą powstać z powodu możliwych błędów ze strony operatora terminalu i wzrosnąć z powodu tego, że dane są przesyłane do komputera poprzez łącza telekomunikacyjne. W celu zapewnienia dokładnego /niezniekształconego/ odbioru komunikatu ma miejsce dokładna kontrola bitów parzystości, oraz sum kontrolnych.

Na dodatek procedura redagująca w systemie pracującym na bieżąco musi się zajmować identyfikacją i upoważnianiem użytkownika i terminalu. Ogólnie biorąc, nie wszyscy użytkownicy będą dopuszczeni do aktualizowania zbiorów, a ci, którzy są upoważnieni,są dopuszczani do aktualizowania tylko niektórych zbiorów lub ich części. Zbiory także będą miały różną wrażliwość i nie będą dostępne dla odczytu przez wszystkich użytkowników. Te problemy będą przebadane bardziej szczegółowo w rozdziale IV "Bezpieczeństwo".

B. Zaprogramowane środki kontroli

Celem działania zaprogramowanych technik zapobiegawczych jest zapewnienie dokładności wewnętrznych obliczeń oraz nienaruszalność zbiorów w systemie. Typowy przebieg przetwarzania danych składa się z wczytania danych do zbioru wejściowego, następnie z pamięci zewnętrznej ściąga się zbiór główny do pamięci głównej, po czym dane są przetwarzane w stosunku do zbioru głównego i albo aktualizuje się zbiór główny, albo wyjście jest produkowane w formie raportów lub zachodzą równocześnie te dwie możliwości. Czynności kontrolne charakteryzują się sprawdzaniem sum kontrolnych i liczników, zarówno pochodzących z wejścia, jak wytwarzanych wewnętrznie.

1. Sumy kontrolne dla partii /wsadu/

O ile jest rzeczą wiadomą z danych na wejściu, że zbiór główny będzie zmieniony o pewną ilość pozycji, np. że będzie dodanych 2000 nowych pozycji do stanu,lub że rachunek "dłużnicy" będzie zmniejszony o 50.000 $, to wówczas zbiory te mogą być podsumowane przed i po przetwarzaniu, by zobaczyć czy dokładnie zgadza się suma, o którą dany zbiór został zmieniony. Jeśli to nie ma miejsca, przetwarzanie nie zostało wykonane właściwie. W obliczaniu liczby, o którą zbiór ma się zmienić jest rzeczą ważną,by pamiętać, że niektóre pozycje na wejściu mogą zostać opuszczone w procesie redagowania; z tego powodu należy dokonać potrąceń.

2. Sumy kontrolne dla zbioru

O ile jakiś zbiór ma pozostać nie zmieniony podczas przetwarzania, można obliczyć sumę kontrolną /suma wszystkich po-

zycji w zapisie lub w zbiorze, która poza tym nie posiada żadnego znaczenia/ i porównać ją do tej samej sumy obliczonej przed przetwarzaniem. Jeśli sumy te się nie zgadzają, jest sprawą oczywistą, że coś zmieniło ten zbiór. Taką kontrolę często się przeprowadza na stałych zbiorach, by określić, czy nie dokonano na nich oszukańczych manipulacji, lub czy przeniesienie zbioru z jednego nośnika na inny nie zostało zakłócone przekłamaniem, lub przeniesienie z jednego programu do drugiego nie spowodowało powstania błędu.

3. Zliczanie pozycji

Przed rozpoczęciem przetwarzania zlicza się liczbę pozycji, a podczas przetwarzania zlicza się liczbę wykonanych transakcji. Na koniec porównuje się te dwie sumy, by sprawdzić czy zostały przetworzone wszystkie zapisy wejściowe. Tę kontrolę wykorzystuje się celem upewnienia się, że przy przesyłaniu zapisów między programami żaden nie został usunięty.

4. Sprawdzanie na "krzyż"

Dokładność procedur wykonywanych na zbiorach jest często kontrolowana w niemal ten sam sposób w jaki księgowi sprawdzają pozycje wciągnięte na konto. Sumuje się kolumny oraz sumuje się rzędy, następnie sumy te dodaje się w obu kierunkach i porównuje.

5. Raporty błędów

Żadna z tych technik zapobiegawczych nie uwypukla ściśle, czym jest błąd lub jaki występuje problem. Wskazują one po prostu, że na poszczególnych etapach coś "nie jest tak". Raporty błędów powinny być, o ile to możliwe, kompletne, by pozwolić operatorowi na ocenę, czy można kontynuować przebieg przetwarzania czy też nie, by pozwolić grupie kontroli ocenić użyteczność wyjścia, oraz by pozwolić programiście na zawężenie poszukiwań błędów w programach do poszczególnych części jakiegoś ściśle określonego programu.

C. Środki kontroli przetwarzania w systemach pracujących na bieżąco

Użytkownicy wywołujący programy w systemie przetwarzającym na bieżąco będą przedstawiali różny stopień przygotowania tech-

nicznego oraz różnorodne zastosowania dla danych i zbiorów tworzących bazę danych. Niektórym z użytkowników można dać sporą dozę swobody w manipulacjach na zbiorach, podczas gdy inni muszą być ograniczeni w tym zakresie. Środki zapobiegawcze stosowane w systemach przetwarzających na bieżąco, jako dodatkowe do stosowanych w systemie wsadowym, będą się przede wszystkim zajmować nienaruszalnością zbiorów.

1. Listy upoważnień

Kiedy użytkownik zgłasza się do systemu przetwarzającego na bieżąco, bierze się pod uwagę jego upoważnienie. Będzie ono zależeć od takich względów jak przeszkolenie, stanowisko w przedsiębiorstwie oraz potrzeba przejrzenia zbiorów w związku z wykonywaną pracą. Upoważnienie jest porównywane ze zbiorem upoważnień w zakresie materiałów, których żąda użytkownik. Jego upoważnienie może dawać mu prawo do dostępu do zbioru w celu jego aktualizacji, albo tylko do odczytu danych. Jego 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. Może on wyciągać nazwiska i adresy niektórych pracowników, lecz może być dlań niedozwolone przeglądanie ich zarobków oraz oceny wydajności, chociaż nawet zapisy zawierające nazwiska i adresy mogą także zawierać płace i oceny wydajności.

Kiedy dokonano dostępu do zbioru, fakt ten jest odnotowywany w zbiorze dostępów lub transakcji, łącznie z upoważnieniem oraz łącznie z tym, co się działo ze zbiorem. Tego rodzaju zbiór może być nieocenioną pomocą dla rewidenta w czasie dokonywania przez niego inspekcji, oraz w wypadku konieczności rekonstrukcji zbioru z powodu przypadkowych jego zniekształceń.

2. Równoczesna aktualizacja

Kiedy użytkownik dokonuje dostępu do zbioru, posiadając na to upoważnienie, musi być włączony specjalny przełącznik "blokady", który nie pozwala na dostęp do zbioru innym użytkownikom aż do momentu, gdy zbiór zostanie zwrócony do bazy danych. Zbiór odczytywany z bazy danych nie podlega zniszczeniu i jest

dostępny dla odczytu przez kogoś innego. Kiedy zbiór zostaje ponownie zapisany w bazie danych, niszczy on zbiór, który się tam przedtem znajdował - pozostawiając tylko zbiór zaktualizowany. Pomyślmy o dwóch użytkownikach aktualizujących ten sam zbiór w tym samym czasie, przy czym jeden z nich nie jest świadom obecności drugiego. Kiedy ci użytkownicy ponownie zapiszą zbiór w bazie danych, użytkownik, który zrobi to później, wymaże zbiór, który tam zapisał drugi użytkownik i w ten sposób treść pierwszej aktualizacji będzie stracona. Bardziej wyszukane sterowanie blokadą ma zastosowanie tylko do pojedynczych aktualizowanych zapisów, tak, że inni użytkownicy zachowują przywilej dostępu do reszty danego zbioru.

D. Środki kontroli wyjścia

Techniki zapobiegawcze w zakresie wyjścia są używane celem zapewnienia, że końcowy wydruk z przetwarzania danych został wytworzony w możliwych do przyjęcia granicach dokładności oraz że wszystkie niezbędne sprawozdania, raporty zostały dostarczone na czas /w odpowiednim momencie/.

Członek grupy kontroli powinien otrzymać wyniki wyjściowe z przebiegu systemu. Wyjście musi zawierać wszystkie raporty o wyjątkach /zastrzeżeniach/ oraz wskazania dotyczące możliwych błędów. Członek grupy kontroli poddaje dokładnej analizie raport wyjątków, by się upewnić, że pozycje, które zostały opuszczone w bieżącym przebiegu będą skorygowane i umieszczone w następnym przebiegu. Jeśli wyniki są zadowalające oraz jeśli dziennik pracy maszyny nie wykazuje poważnych problemów, członek grupy kontroli dostarcza materiały wyjścia użytkownikowi. Jeśli zachodzą problemy, które wydają się mieć związek z programowaniem, przekazuje on materiały wyjścia programiście, który przegląda materiał w celu znalezienia błędu.

W systemie pracującym na bieżąco kontrola nad wyjściem jest sprawowana przez system, tj. upoważnienie użytkownika wskazuje, jakie wyjście może on otrzymać, a jakiego nie może otrzymać.

E. Dokumentacja

Dla każdego systemu najważniejszym środkiem kontroli jest zawsze należyta dokumentacja. Patrząc w przeszłość dochodzimy do wniosku, że dokumentacja była mało wykorzystywana tam, gdzie naprawdę mogła się przydać.

Ogólnie biorąc, największe niedociągnięcia zdarzają się w dokumentacji programów komputera. A właśnie programy komputera są sercem systemu, są częścią,w której mają miejsce bieżące transakcje przeprowadzające manipulacje i obliczenia na majątku przedsiębiorstwa. Są one tą częścią systemu, która jest najbardziej podatna na machinacje. O ile nie jest zapisane i to bardzo szczegółowo, co one robią i jak one to robią, może to być po prostu zaproszeniem do przestępczej działalności.

Programiści są znani ze swego uporu, jeśli idzie o niedostarczanie dokumentacji dla opracowanych przez siebie programów. Dokumentacja, a szczególnie dobra dokumentacja, jest czasochłonna, a programistom niemal zawsze brakuje czasu. Często programiści nie potrafią jasno wyrażać się na papierze i pisanie jest dla nich bolesną koniecznością.Często nie są oni pewni lub nie wiedzą, co powinno być zawarte w dokumentacji, by uczynić ją wiarygodną. Czasami właśnie jest dobrym zabezpieczeniem sobie pracy, być jedynym na danym terenie, który wie jak pracują niektóre programy.

Zaprojektowane zawczasu wzory i formularze dokumentacji mogą pomóc programiście przezwyciężyć niektóre z tych problemów. Jeśli to, co ma on powiedzieć o swoich programach,jest mu dosyć jasno przedłożone, cały proces powstawania programu staje się dlań znacznie łatwiejszy i mniej bolesny.

Cała dokumentacja systemu i procedur tworzy pokaźnych rozmiarów księgę, z której poszczególne rozdziały interesują tylko ludzi zajmujących się ściśle określonymi dziedzinami wymienionymi w tytule rozdziału. Każdy z rozdziałów powinien być niezależny i osobno dostępny. Z punktu widzenia rewidenta, rozgraniczenie obowiązków narzuca, by takie same rozgraniczenie miało zastosowanie do rozdziałów dokumentacji. Na przykład operator, mając własny rozdział lub podręcznik nie potrzebuje zaglądać do podręcznika programisty i prawdę mówiąc, nie powinno się zezwalać mu, by tam zaglądał.

Poniższe zalecenia na temat tego, co powinno tworzyć dobrą dokumentację systemu, zostały opracowane dla wrażliwego systemu przez komitet określenia problemu, który bada zapotrzebowania na nowe programy, przez komitet projektowania, który formułuje specyfikacje dla nowych programów oraz przez grupę kontroli, która nadzoruje działalność kontrolną. Jednakże poniżej przedstawione ograniczenia mogą być złuźnione dla systemu mniej wrażliwego lub opracowanego w odmienny sposób.

Księga systemu

a. Rozdział I. Sprawozdanie komitetu określającego problem. Omawiane sprawozdanie jest ważne dla celów poszukiwania u samego źródła uzasadnienia obecności takich czy innych programów w systemie. Sprawozdanie powinno posiadać następujące **nagłówki działów:**

- członkowie komitetu,
- określenie problemu.

  W tej części koniecznie należy opisać wydział inicjujący, osoby inicjujące, wymagania programu oraz uzasadnienie konieczności jego opracowywania.

- plan podejścia do rozwiązania problemu.

  Taki plan w żadnym razie nie jest usiłowaniem zaprojektowania programu. Ta działalność jest poza zakresem prac komitetu określającego problem. W tym planie ataku komitet analizuje problem, przydziela analityków systemu do prac nad projektowaniem programu, przydziela grupę kontroli, wyznacza ludzi, którzy będą upoważnieni do zatwierdzania zmian w programie oraz, mówiąc krótko, działa jako koordynator dla rozpoczęcia prac.

- lista osób przydzielonych do komitetu projektowania,
- lista osób przydzielonych do grupy kontroli,
- lista osób upoważnionych do zatwierdzania zmian,
- rejestr zmian.

Zmiany w początkowo obmyślonym systemie będą występowały na etapie projektowania, wdrażania i konserwacji. Jest to obo-

wiązkowa pozycja raportu. Tu powinien być prowadzony zapis wszystkich dokonanych zmian.

- modyfikacje.

  W trakcie etapów projektowania i wdrażania, dla wielu nie dających się przewidzieć przyczyn, zainteresowany personel będzie miał powody, aby modyfikować uprzednio uzgodnione aspekty problemu. Te rewizje powinny być sformułowane w memorandach oraz zapisywane w tym rozdziale.

b. Rozdział II. Sprawozdanie komitetu projektowania systemu. Wszelkie wątpliwości co do zamiarów projektantów powinny być wyjaśniane poprzez odsyłanie do tego sprawozdania. Nagłówki części tego sprawozdania powinny być następujące:

- lista członków komitetu projektowania systemu,
- kopia specyfikacji z komitetu określenia problemu,
- opis programu,

  Opis powinien zawierać cel, wykorzystanie, opisy zbiorów, opisy zapisów, wejście oraz wyjście programu. Ten punkt będzie częścią specyfikacji, którą przekaże się programistom.

- lista środków kontroli,

  Wchodzą tu proponowane środki kontroli dokonywane za pomocą komputera, wrażliwość różnych zbiorów, wymagania w zakresie archiwizacji dla każdego zbioru, rozpowszechnienie wyjścia, oraz przygotowania w zakresie środków zastępczych. Proponowane kroki zapobiegawcze, które ma wykonać komputer, mogą być zmienione przez programistów, lecz muszą być zatwierdzone przez komitet projektowania. W ten sposób komitet projektowania posiada ostateczną odpowiedzialność w zakresie środków kontroli nad ruchem danych.

- makro-schemat blokowy /flowchart/ systemu,

  Schemat ten pokazuje jak dany program "leży" w całym systemie.

- makro-schemat blokowy programu,

  Obszary w programie, w których mają być ustanowione różne środki kontroli, powinny być także wykazane w tym schemacie blokowym,

- lista programistów przydzielonych do projektu,
- lista członków grupy kontroli,
- lista członków komitetu określenia problemu,
- rejestr zmian,
- rejestr modyfikacji problemu.

c. Rozdział III. Dokumentacja poszczególnych programów. System zawiera szereg programów, każdy z nich musi być oddzielnie udokumentowany. Dokumentacja każdego programu powinna istnieć w postaci samodzielnej, ponieważ w konserwacji będzie konieczne odwoływanie się do niej. Ta dokumentacja powinna być jak najbardziej szczegółowa, chociażby z powodu tego, że jest trudno zrozumiała, a także ponieważ dokumentuje najsłabszy punkt systemu. Nagłówki części powinny być jak następuje:

- dane osobowe programistów,
- lista członków komitetu projektowania,
- lista członków grupy kontroli,
- kopia specyfikacji z komitetu projektowania systemu,
- cel programu,
- wejście do programu,

  Tu powinny być podane szczegółowe opisy układu komunikatów lub kart, zapisów oraz zbiorów, które tworzą wejście do programu. Jeśli możliwe, powinny być podane rysunki lub przykłady.

- opis programu,

  Różnica między opisem oraz celem programu jest taka, że cel programu jest to deklaracja dotycząca roli jaką, według oczekiwań, ma ten program odgrywać w przetwarzaniu danych; opis programu nakreśla metody użyte w przetwarzaniu. Tu wchodzi także przepływ danych oraz operacje wykonywane na zbiorach oraz zapisach w czasie ich ruchu poprzez program.

- definicje i układy/topografie/ zbiorów,

  Tu powinny być umieszczone nazwy zbiorów, przeznaczenie zbiorów oraz ich fizyczny wygląd, jak również nośniki, na których mają być zapisane.

- formaty zapisów,

  To samo co wyżej, powinno być powiedziane tutaj o poszczególnych zapisach w każdym zbiorze, wiążąc w ten sposób każdy zapis z jego zbiorem.

- makro-schematy blokowe,

  W formie schematu blokowego powinien być tu podany ogólny plan /układ/ programu bez wchodzenia w szczegóły. Tzn. powinny być tutaj określone związki logiczne, ideowe.

- mikro-schematy blokowe,

  Powinna istnieć bardzo ścisła zależność między poszczególnymi rozkazami programów oraz wpisami w każdym bloku mikroschematu blokowego /micro flowchart/. Jednakże ta zależność powinna być całkowicie wolna od języka programowania użytego przy konstruowaniu programu.

- słownik nazw zmiennych,

  Głównie dla potrzeb konserwacji powinny być podane opisy i zastosowanie pozycji wewnętrznych.

- listowania programu.

  Listowanie programu powinno być,o ile to możliwe, samodokumentujące. Jeśli językiem programowania jest COBOL oraz jeśli dokonano właściwego wyboru nazw zmiennych, wylistowany program będzie się czytać bardzo podobnie do tekstu w języku angielskim i z pomocą schematu blokowego można go bardzo łatwo prześledzić. Wszystkie języki programowania posiadają klauzule na zamieszczenie komentarzy wewnątrz programu celem objaśnienia wylistowania. Z tej właściwości należy robić szeroki użytek. W wyniku tego schemat blokowy może być niejako "osadzony" w wylistowaniu programu.

- objaśnienie wyjścia.

  Wszelkie komunikaty dla wyświetlenia na konsoli, dla maszyny do pisania na konsoli lub dla drukarki na wyjściu itp. powinny być szczegółowo wyjaśnione. Nagłówki kolumn, komunikaty o błędach itp. są często bardzo lapidarne i czasami niejasne z powodu ograniczenia miejsca lub wad sprzętu. Powinny je wyjaśnić odsyłacze do tego rozdziału dokumentacji.

Jeśli wyjście z programu zawiera zbiór lub grupę zbiorów, ich konstrukcja i formaty powinny być tutaj wyjaśnione.

- próbki wyjścia,

W dokumentacji powinna być załączona kopia każdego wydrukowanego wyjścia, łącznie z jego formatem. Jeśli wyjście posiada formę zbiorów, powinien być załączony rysunek pokazujący format.

- procedury awaryjne,

Tu powinny być wymienione działania, jakie należy podjąć w wypadku błędów lub pogwałcenia procedur zabezpieczenia.

- wyniki próby sprawdzającej,

Składnikami tej części dokumentacji są: kopia użytych danych, lista własności, dla których sprawdzenia zaprojektowano dane oraz kopia wyjścia z przebiegu sprawdzającego. Nie tylko wyjście powinno być prawidłowe, lecz dane powinny być tak zaprojektowane,aby naruszać każdą z technik zabezpieczenia i pogwałcać warunki - celem sprawdzenia w każdej sytuacji zagrożenia.

- kopia przyjęcia przez użytkownika.

Użytkownik powinien podpisać formularz wykazujący, że przejrzał i zaakceptował nie tylko program i wyniki przebiegu sprawdzającego, lecz również dokumentację.

- wylistowania zmienionych programów.

Wylistowania programów, zarówno przed jak i po zmianach,powinny być zachowane co najmniej między kolejnymi inspekcjami.

- rejestr zmian,
- rejestr modyfikacji problemu.

d. Rozdział IV. Procedury operacyjne. Operator, aby eksploatować system na sprzęcie trzeciej generacji, nie potrzebuje dużo o nim wiedzieć. Nie powinien on mieć więcej informacji do swojej dyspozycji niż potrzebuje. Nagłówki tego odcinka są następujące:

- oznaczenie /nazwa/ programu,
- instrukcje inicjowania przebiegu,

  Można sporządzić znormalizowany formularz dla określonej konfiguracji, na której działa system programów. Instrukcje ustawiania są wówczas sporządzane po prostu na pojedynczym arkuszu, wskazującym,które taśmy mają być zamontowane, na które jednostki, które pakiety dysków należy zamontować,które klucze sprawdzane przez program należy włączyć itd.

- wydruki lub wyświetlanie na konsoli.

  Należy załączyć listę komunikatów na konsoli, które mogą być generowane przez program, łącznie z opisem działań, jakie powinien podjąć operator w wypadku,gdy te komunikaty się ukażą. O ile jest to możliwe do przeprowadzenia, działania, jakie powinien podjąć operator, powinny być wskazane w komunikacie. Często jest to niepraktyczne i zamiast tego daje się odsyłacz do podręcznika operatora.

- wymagania w zakresie archiwizacji /danych, zbiorów itp./,
- procedury bezpieczeństwa,
- rozdzielnik wyjścia,

  Osobą, której się przekazuje dane wyjściowe, powinien być członek grupy kontroli. Operator nie powinien osobiście rozdzielać materiału z wyjścia komputera.

- lista członków grupy kontroli,

  Może to być również po prostu wskazanie osoby, z którą należy się kontaktować w przypadku powstania jakichś problemów. Nie powinni to być programiści. Należy utrzymywać,o ile to możliwe, jak najmniejszy kontakt między operatorami a programistami.

e. Rozdział V. Przygotowanie danych. Większą część podręcznika przygotowania danych powinny stanowić uprzednio wydrukowane znormalizowane formularze. Zawartość podręcznika powinna zawierać następujące nagłówki:

- tytuł,
- wstępnie przygotowany materiał wejściowy,

W interesie dokładności, jak również wydajności, jest pożądane, tam gdzie to możliwe, przygotowywanie wstępnie możliwie dużo danych o stałym charakterze. Pewne pola zmiennych pozostawia się wolne celem wypełnienia, skoro tylko odpowiednie dane będą dostępne. Przykładem mogą być pozycje w zbiorze rachunku "dłużnicy". Do stałych danych będą tu należeć: nazwisko i kod klienta, adres pocztowy oraz wyrób. Z momentem nadejścia każdego nowego zamówienia od klienta, jako część przygotowania danych wypełniałoby się ilość i koszt. Tu powinna też znaleźć się informacja, które dane zostały wstępnie przygotowane i gdzie są one przechowywane.

- formaty kart lub zapisów,
- wyjaśnienia na temat wejść do uznania.

Zależnie od różnych warunków, wprowadzenie niektórych danych może być pozostawione do uznania użytkownika. Pewne pola wejściowe mogą na przykład posiadać wcześniej określone "zaniechane"wartości, by pozwolić użytkownikowi wyspecyfikować nominalną wartość przez ominięcie tego szczególnego pola. Należy wyjaśnić, kiedy załączyć tego typu dane , oraz jak wskazać w danych, kiedy należy korzystać z decyzji wyboru.

- kody sprawdzające, wymagania w zakresie weryfikacji oraz sprawdzanie partii /wsadu/ - jeśli mają zastosowanie.

f. Rozdział VI. Środki kontroli należące do danego systemu. Niniejszy rozdział jest zdecydowanie najbardziej "czuły"z całej księgi. Bezpieczeństwo całego systemu zależy od nieujawniania zawartej tutaj informacji. Rozdział ten jest niezbędny dla celów rewizji. Kontrola nad środkami kontroli dyktuje, by ten rozdział traktować z priorytetem najwyższego rzędu. Treścią rozdziału powinna być lista procedur zabezpieczających oraz schemat blokowy /flowchart/ wskazujący, gdzie i jak omawiane procedury są stosowane.

IV. ZABEZPIECZANIE

Zabezpieczanie polega na ochronie danych przed przypadkowym lub zamierzonym ich ujawnieniem osobom nieupoważnionym dla niewłaściwego wykorzystania lub modyfikacji. Procedury zabezpieczenia mogą być włączone tylko do sprzętu komputera, albo również do programów i podprogramów. Zabezpieczenie obejmuje także znormalizowane procedury fizycznej ochrony całego środowiska systemu, włączając w to dane, programy, karty dziurkowane oraz magnetyczne nośniki informacji, jak również te procedury, które identyfikują i ograniczają dostęp ze strony personelu do tego środowiska.

Wzrastające wykorzystywanie centralnych banków danych, do których można dokonywać zdalnego dostępu za pomocą terminali, dało w wyniku większą wrażliwość systemu niż dawniej, oraz rozszerzyło problem zabezpieczenia do takiego rozmiaru, że może on stanowić znaczną część kosztu założenia i eksploatacji komórki APD. Banki danych koncentrują olbrzymie ilości informacji - często są to bazy danych dla całego systemu - w jednym miejscu, mnożąc skutki nawet pojedynczego nieupoważnionego dostępu, ze względu na wielką liczbę danych udostępnianych włączającemu się. Terminale zdalnego dostępu oraz systemy przetwarzania na bieżąco są zaprojektowane, by zwiększyć możliwości zastosowań i dostępność systemów APD. Lecz w połączeniu z tendencjami, zarówno w sprzęcie jak i w oprogramowaniu, do ułatwiania dostępu dla personelu nie obeznanego z komputerami i działania w systemie, wrażliwość systemu na złodziejstwa, defraudacje, malwersacje oraz fałszerstwa znacznie wzrosła.

A. Projektowanie

Gdy projektuje się system, należy ustalić równowagę między potrzebą informacji a stopniem dostępu do systemu, jaki osoby mające zapotrzebowanie na informację będą miały. Idealną byłaby, oczywiście, sytuacja, w której niemal każdemu by się zezwalało na dostęp do systemu, gdy taka potrzeba powstanie. Lecz środowisko bez ograniczeń nie jest środowiskiem zabezpieczonym.

Wpadając w drugą skrajność w dostępności systemu, nie trudno wyobrazić sobie zbyt ściśle kontrolowane środowisko z procedurami zabezpieczenia tak surowymi, że tylko ograniczona grupa operacyjna ma dostęp do systemu i strumień informacji wejściowej do środowiska APD jest znacznie uszczuplony.

Szczególnie projektowanie systemów powinno uwzględniać cztery podstawowe momenty, które przyczyniają się do bezpieczeństwa operacji APD: rozpoznanie użytkownika, upoważnienie użytkownika, natychmiastowe wykrycie nieupoważnionego dostępu, oraz środki inspekcji.

1. Rozpoznawanie

Przy rozpoznawaniu chodzi o upewnienie się, że przede wszystkim zapytujący o informacje ma prawo dostępu do systemu. Rozwiązania tego problemu korzystają z haseł, fizycznych cech użytkownika oraz sposobów wykorzystujących sprzęt.

Metoda korzystania z haseł jest najbardziej rozpowszechnioną obecnie procedurą rozpoznawania, lecz w wielu przypadkach jest daleka od zadowalającej. W teorii użytkownik prosi o dopuszczenie do systemu i podaje systemowi, albo sam, albo na żądanie, prawidłowe hasło podane upoważnionym użytkownikom tego systemu. O ile zostanie podane prawidłowe hasło, to wówczas dostęp zostaje udzielony i użytkownik otrzymuje informację, o którą zabiega. Lecz w praktyce stwierdzamy, że liczni użytkownicy zapominają swoje hasła i w wyniku tego, co najmniej jeden system w sposób zrutynizowany dostarcza hasła gdy użytkownik poda, że go nie posiada.

Odciski warg, odciski palców oraz obrazy głosu są obecnie przedmiotem badań jako niektóre nowsze dziedziny rozpoznawania. Istnieje wiele bardziej wyszukanych sposobów jednoznacznego rozpoznawania jakiegoś osobnika. Lecz prawdopodobnie najbardziej obiecujące są metody korzystające z usług sprzętu, a w tym zakresie największe szanse sukcesu posiada karta z paskiem magnetycznym.

Jest to karta plastykowa, podobna do znajdujących się obecnie w powszechnym użyciu kart kredytowych, na której naniesiono pasek materiału magnetycznego. Na tym pasku magnetycznym terminal może zapisywać i odczytywać informację. Zaletę

karty z paskiem magnetycznym stanowi to, że informacja identyfikująca zapisana na pasku w jednej wersji może być przez system zmieniona w razie potrzeby, i to w taki sposób, że nie jest to widoczne na karcie. Tak więc, gdy karta zostanie zgubiona, znalazca nie będzie miał pojęcia do czego może być użyta. /Inny rodzaj kart z paskiem magnetycznym posiada bity informacji odciśnięte w plastykowym korpusie karty, co eliminuje możliwość zmian i wymazania/.

2. Upoważnienie użytkownika

Po zweryfikowaniu zapytującego, system musi sprawdzić, czy ma on prawo otrzymać określoną informację, o którą zapytywał. Wejście do systemu nigdy nie powinno być jednoznaczne z dowolnym dostępem, jaki pozwalałby użytkownikowi na myszkowanie i przypadkowy dostęp do zbiorów. Każdy zbiór posiada oddzielną i wyróżnialną wrażliwość w stosunku do innych i powinno to być zapisane w zbiorze upoważnień, który wskazuje, kto posiada upoważnienie na wgląd do określonej części, określonego zbioru w bazie danych, oraz kto może dokonywać zmian w tych zbiorach.

3. Metody wykrywania

Natychmiastowe wykrycie polega na zapewnieniu, że intruz zostanie odrzucony zanim dokona on dostępu do zbioru, a nie po jego dokonaniu. Powinien być prowadzony rejestr wszystkich usiłowań nieupoważnionego dostępu do zbioru, a taki nieupoważniony dostęp powinien automatycznie otrzymywać negatywną odpowiedź. Pierwsze usiłowanie dostępu może z powodzeniem być niezamierzonym błędem, lecz dodatkowe usiłowania powinny być zbadane, ponieważ według wszelkiego prawdopodobieństwa były one przeprowadzone w złym zamiarze.

Drugie usiłowanie nieupoważnionego dostępu powinno w wyniku spowodować wyłączenie terminalu użytkownika z systemu w taki sposób, aby tylko inspektor bezpieczeństwa mógł go ponownie włączyć.

4. Środki inspekcji

Inspekcja systemu powinna być przeprowadzana w taki sposób, by ujawniała charakterystyczne szczegóły każdego dostępu do

systemu. Powinny być prowadzone rejestry każdego dostępu oraz usiłowania dostępu do zbioru, w których powinna być zawarta informacja na temat tego, kto pytał o co, oraz czy dana osoba była upoważniona do zadawania takich pytań.

Omawiane rejestry powinny być tworzone przez sam system i powinny być przedmiotem częstej inspekcji ze strony inspektorów bezpieczeństwa. W akcji tej może pomagać sama maszyna i właściwie powinna ona okresowo dokonywać kontroli częstotliwości dostępu, aby zmieniać rozmieszczenie zbiorów, aby umożliwić optymalne czasy dostępu w oparciu o częstotliwość korzystania ze zbiorów.

Rewident powinien zdawać sobie sprawę, że bardzo rzadkie usiłowania dostępu do zbioru mogą faktycznie być wskazówką o ustanowieniu przez obejście systemu nowej drogi dostępu do zbioru, nie pozostawiającej śladu tego działania.

B. Zabezpieczenie fizyczne

Dobre zabezpieczenie fizyczne jest problemem wspólnym dla systemów rządowych i finansowych, jak również dla operacji APD i nauka - czasami opłacona poważnymi kosztami w sensie strat finansowych oraz zdradzonych bardzo ważnych spraw z zakresu bezpieczeństwa narodowego - zdobyta w innych dziedzinach powinna być dobrze zapamiętana przez użytkownika komputera.

Nawet doskonale zaplanowany, wyszukany system zabezpieczenia nie jest odporny na manipulacje. Tu godnym przytoczenia przypadkiem jest bank, który dosyć niedawno był sześć razy obrabowany w ciągu kilku miesięcy. Zainstalowano wszystkie możliwe urządzenia podsłuchowe i alarmowe. Telewizja wewnętrzna nadzorowała każde wejście i wyjście, automatyczne kamery zapisywały każdą transakcję, a ultraczułe czujniki, działające w czasie godzin zamknięcia banku mogły uruchomić alarm przy wtargnięciu jakiegokolwiek gryzonia.

Bank był umiejscowiony w wielkim centrum handlowym, które było otwarte jeszcze po godzinach, w których zamykano bank pod koniec normalnego dnia pracy. Miejscowi kupcy korzystali z depozytu nocnego dla wpływów dziennych, a w dniu rabunku schludnie umundurowany strażnik informował deponujących, że depozyt jest zablokowany.

Jeśli zostawią pieniądze jemu - mówił strażnik każdemu, kto zbliżał się do rzekomo źle funkcjonującego otworu wrzutowego - to wówczas zaniesie je do wewnątrz. "Depozyty" tej nocy wyniosły ponad 250.000 $ i naturalnie ani strażnika, ani pieniędzy nigdy już więcej nie widziano. Przytaczając powyższy przykład, chcemy udowodnić, że najlepszy na świecie system bezpieczeństwa jest bezwartościowy, o ile operacje mogą mieć miejsce poza kontrolowanym środowiskiem.

Jednakże nawet w ściśle kontrolowanym systemie zabezpieczeń może mieć miejsce nieupoważniony dostęp. Stopień zagrożenia jest jednakże ograniczony tym, jak dalece przestrzegane są i stosowane znormalizowane procedury bezpieczeństwa, wypracowane w podręcznikach lub udostępnione przez producentów i grupy konsultacyjne.

Należy pamiętać, że momentem kluczowym w ustanowieniu jakiegokolwiek systemu bezpieczeństwa jest uwzględnienie całej instalacji komputerowej, powiązanych z nią bibliotek danych oraz wspomagających wydziałów kontroli administracyjnej, jako jednej jednostki dla celów bezpieczeństwa. Zbyt często zabezpieczanie ześrodkowuje się na centralnym procesorze, z wyłączeniem tych innych obszarów, które w istocie są integralną częścią systemu, choć nawet nie są częścią fizyczną pomieszczeń przetwarzania danych. Wynikająca słabość systemu bywa często wykorzystywana.

Dostęp do jednostki przetwarzania danych jako całości powinien być ograniczony za pomocą użycia straży i procedur identyfikacji tylko do tych osobników, którzy biorą bezpośredni udział w operacjach komputera. Kamery, mikrofony i inne urządzenia nadzorujące powinny zapewnić automatyczną i ciągłą inwigilację obszaru. Zamki powinny ograniczać, a rejestry zawierać wpis wszystkich dokonanych dostępów do pokoi, schowków i zbiorów, w których są przechowywane wrażliwe dane.

Rzeczywisty problem dla fizycznego bezpieczeństwa stwarza jednakże dostępność wyszukanej technologii. Skomplikowane elementy sprzętu elektronicznego, optycznego i akustycznego są dostępne w handlu i zwalczanie intruza korzystającego z takiego sprzętu może być trudnym zadaniem.

Szklane ściany, które często otaczają ośrodki przetwarzania danych są na przykład otwartym zaproszeniem dla penetracji optycznej za pomocą kamery wyposażonej w teleobiektyw. Otwarte okna i drzwi są dosyć wrażliwe dla urządzeń wyposażonych w mikrofon z parabolicznym reflektorem, który, gdy się go sprzęże z licznymi elementami wzmacniaczy dostępnymi od producentów sprzętu stereofonicznego i hi-fi, może podsłuchać rozmowę z odległości wynoszącej setki metrów.

Dwa obszary wymagają coraz większej uwagi ze strony użytkownika komputera. Chodzi tu o podsłuch elektroniczny i telegraficzny, szczególnie w konfiguracjach zdalnego dostępu. Nie **ma na razie doniesień o kradzieży jakichś danych przez podłączenie się do łączy telefonii nośnej, lecz nie wyklucza to działalności szpiegowskiej w przyszłości.**

Jedną z możliwych odpowiedzi na tego rodzaju zagrożenie są handlowe urządzenia szyfrujące. Technologia ich budowy jest opanowana,lecz co najmniej jeden z potencjalnych producentów ocenia, że nawet gdyby takie urządzenia były dostępne, według obecnego rozeznania nie byłoby na nie dużego zbytu.

Urządzenia zdalnych terminali są z pewnością wrażliwe na podsłuch, lecz koszt przechwytywania informacji szybko rośnie w miarę wzrostu odległości od terminalu. Koszty podsłuchu wymagają wydatku kilku setek dolarów, by otrzymać wystarczającą kopię w odległości 5 metrów od terminalu, lecz z kolei dalsze 30 metrów oddalenia będzie wymagało zastosowania ciągnika z przyczepą najeżonego antenami i będzie kosztowało ponad 1000$ na godzinę jeśli idzie o obsługę.

C. Eksploatacja

Zagrożenie elektronicznym atakiem fizycznej nienaruszalności środowiska systemu sprowadza się do zasadniczych rozważań na temat pieniędzy i odpowiedniego zaopatrzenia: jeśli wartość przechwyconych danych usprawiedliwi koszt ich zbierania, to wówczas przechwytywanie wchodzi w zakres możliwości, które trzeba uwzględnić. Lecz bezpieczeństwo eksploatacji, a szczególnie uczciwość poszczególnej jednostki w środowisku wielodostępnym jest sprawą bardziej skomplikowaną niż kwestia pieniędzy i sprzętu.

Oczywiście podstawą bezpieczeństwa eksploatacji jest włączenie tych standardowych technik zapobiegawczych do procedur i metod systemowych, by sprawdzać czy system jest nienaruszony po dokonaniu wszystkich wejść. Lecz eksploatacja w środowisku wielodostępu rodzi zagadnienia swobód obywatelskich, dotychczas nie znane i niemożliwe do rozwiązania przez użytkownika po prostu dlatego, że są czynniki, nad którymi nie posiada on kontroli w tego rodzaju środowisku.

Zagrożenie tajemnicy informacji może posiadać charakter przypadkowy lub zamierzony, może być bierne lub czynne, oraz może być wynikiem błędu ze strony użytkownika lub ze strony systemu. Przeciwdziałanie może sięgać od zwykłych ograniczeń dostępu - jest to wcześniej przedyskutowany problem upoważniania - do pewnych nowych i raczej wymyślnych propozycji w zakresie kodowania danych, opartych na podstawieniu i transpozycji znaków oraz na algebraicznym łączeniu znaków komunikatów ze znakami "klucza", by uformować zaszyfrowany komunikat.

Lecz te mechaniczne metody nie są ukierunkowane na samo sedno zagadnienia, którym jest faktyczna istota samego wielodostępu, tam, gdzie dostęp do komputera nie jest organicznie ograniczony wyłącznie do członków tej samej organizacji lub "rodziny".

Szczególnie wrażliwe dane muszą być gdzieś przechowywane i jakoś przetwarzane, a nie można rezygnować z możliwości APD tylko ze względu na bezpieczeństwo. W komputerach wieloprogramowych z dołączonymi bezpośrednio zdalnymi terminalami, podstawową zasadą pracy jest, by nie przetwarzać tajnej informacji jednocześnie z innymi o bardziej ogólnej naturze. Innym podstawowym prawidłem w tym środowisku programów jest, by nie mieć zdalnych wyjść z tego wszystkiego, co jest tajne. A samo zdalne wprowadzanie - jeśli chodzi o nienaruszalność danych - odbywa się na odpowiedzialność użytkownika i trudno obarczać tą odpowiedzialnością odbierającego.

Ostatnim kluczowym momentem w bezpieczeństwie eksploatacji jest obejmujący całość system technik zapobiegawczych, który jest ręcznie opracowany i który zapewnia niezależne kontrolowanie wyjścia i uzgadnia je z wejściem.

D. Personel

Bezpieczeństwo w dalszym ciągu, po większej części, zależy od ciągłej lojalności, uczciwości oraz niezawodności personelu przydzielonego do operowania komputerem oraz jego wspomagającymi funkcjami. Powinny być ustalone procedury dla uprzedniego egzaminowania oraz doboru personelu. Dodatkowe procedury do wyboru zawierają, tak jak to ma miejsce w wojsku, badanie pewności, przysięgi na lojalność itd., lecz te procedury, ogólnie mówiąc, w naszym społeczeństwie są historycznie ograniczone do wyraźnie wydzielonych komórek rządowych.

Istnieją znormalizowane procedury dające rękojmię zabezpieczenia ze strony personelu i w połączeniu z rejestrami dostępu oraz badaniami kontrolnymi, powinny one mieć zastosowanie do każdego bez względu na jego stanowisko i kompetencje. Nie jest celem niniejszego sprawozdania wyliczanie tych podstawowych procedur, które można znaleźć w normalnych publikacjach i podręcznikach dostarczanych przez producentów komputerów, grupy konsultacyjne oraz przedsiębiorstwa ubezpieczeniowe. Trzeba jednak podkreślić, że kluczem do bezpieczeństwa w dziedzinie personalnej musi być ścisłe i ciągłe stosowanie ustalonych procedur w stosunku do każdego, od góry do dołu, w obszarach operacyjnym i nadzorczym.

Sprzeniewierzenia i malwersacje są możliwe w każdym systemie i najczęściej wychodzą na światło dzienne przez przypadek. Sprzeniewierzenia i malwersacje są także formalnie możliwe"wokół" systemu, nie koniecznie w nim i dlatego procedury inspekcji powinny być dosyć rozległe by wykryć te nieregularności, czego przykładem jest jak daleko, w pomysłach posunął się pewien malwersant.

> Pewien rewident "prześwietlając" konfigurację komputera w jednym z zakładów produkcyjnych wykrył, że maszyny są wykorzystywane tylko przez 40 procent czasu. Na dodatek, jak to wykazała kontrola, kierownik APD uzyskał zgodę na zwiększenie tej, w sposób oczywisty, niedociążonej instalacji APD.

W rzeczywistości ów kierownik podnajmował swój "dodatkowy" czas przedsiębiorstwom na zewnątrz dla korzyści osobistych, a dalsze zwiększenie sprzętu jeszcze bardziej zwiększyłoby zyskowność tej spekulacji. Przeliczając na gotówkę, otrzymywał on 10.000 $ rocznie, a zwiększenie konfiguracji powiększyłoby tę liczbę kilkakrotnie.

Jednym z wyników tej nielegalnej działalności ze strony kluczowego i zaufanego pracownika było ustanowienie wytycznych dla podnajmowania sprzętu i w ciągu dwóch miesięcy przedsiębiorstwo uzyskało dodatkowy dochód wynoszący około 30.000 $, przeliczając w skali rocznej.

Truizm, mówiący, że łańcuch jest tylko na tyle mocny na ile jest mocne jego najsłabsze ogniwo, ma zastosowanie szczególnie do dziedziny zabezpieczenia personelu w środowisku APD. Odpowiednie kontrole mogą być zawsze wcielone do sprzętu i programów, lecz jednostka ma możliwość wyboru w działaniu.

V. INSPEKTOR WEWNĘTRZNY W APD

Już od momentu powstania przetwarzania danych istnieje kwestia, w jakim rozmiarze rewident wewnętrzny powinien wnikać w funkcje APD. Sprawa ta i obecnie wywołuje debaty. Przeszukanie literatury na temat problemu udziału rewidenta doprowadziło do przekonania, że w tym zakresie nie dokonano żadnego postępu w ciągu ostatnich dziesięciu lat. Artykuły datowane z 1970 roku mówią to samo o konieczności zmiany sposobu pracy i zaangażowania się w sprawy APD, co mówiły artykuły z 1960 r. Badania w terenie ujawniły, że sytuacja nie jest w żadnym wypadku tak zastała jak to wydaje się wynikać z literatury.

Wydaje się, że nie ma co zadręczać niechętnych tradycyjnych rewidentów, by się przyłączyli do szeregów tych, którzy stawiają na doniosłość przetwarzania danych. Istnieje wiele innych dziedzin inspekcji, które wymagają ich uwagi, i być może, rewident, który jest doskonały w tych dziedzinach, nie będzie miał szczególnych uzdolnień niezbędnych w dokonywaniu inspekcji APD.

Bieżącym trendem jest ustanawianie personelu inspekcji APD - specjalistów inspekcji w APD. Ci rewidenci znają się na dwóch dziedzinach: inspekcji i APD. Nie wykonują oni żadnego innego rodzaju inspekcji. Ich rola i wartość została wyjaśniona w odcinku B niniejszego rozdziału.

Niektórzy kierownicy wydziałów inspekcji wyrażali rozsądną opinię, że obowiązkiem kierownika jest dać tym, którzy pracują dla niego, tak gruntowne przeszkolenie jak tylko możliwe. Pozbawienie stałego personelu szansy przeszkolenia się w zakresie systemów komputerowych tylko dlatego, że istnieje sztab specjalistów wykonujących funkcję byłoby - według ich odczucia - krzywdzeniem pracowników.

Wielu kierowników odczuwa, że problem inspekcji systemów APD jest tak złożony, że wymaga specjalizacji. Na dodatek,rewident który poświęca się tylko APD może spędzić więcej czasu - i bardziej konstruktywnie - z projektantami systemów,by wytworzyć lepsze systemy z lepszymi technikami zabezpieczenia. Pożytek z udziału rewidenta w etapie planowania projektu systemu jest przedstawiony w ustępie A.

A. Udział inspektora

Jedną z najbardziej doniosłych funkcji rewidenta jest jego rola jako niezależnego inspektora. Wielu rewidentów od dawna argumentowało przeciw udziałowi w sprawach dotyczących APD, ponieważ boją się utraty obiektywizmu. Stwierdzają słusznie, że nie można zaprojektować technik zabezpieczenia w systemie, a następnie dokonywać inspekcji tego systemu bez przychylnego nastawienia. Rzeczywiście doniosłość obiektywizmu rewidenta jest uważana za podstawę w wykonywaniu jego obowiązków. Ta sprawa jest jasno postawiona w opracowanej przez Instytut Rewidentów Wewnętrznych /Institute of Internal Auditors/ Deklaracji Obowiązków Rewidenta Wewnętrznego /załącznik A/.

Wydawałoby się, że inspektor nie powinien brać udziału w projektowaniu systemów lub w projektowaniu procedur zabezpieczenia w systemach. Jednakże nie tego oczekuje się od niego. Oczekuje się od niego porady dotyczącej możliwych niezbędnych technik zabezpieczenia, jakie mają być narzucone w systemie w czasie jego projektowania. W momencie, kiedy system jest go-

towy do wdrożenia, niektóre środki zabezpieczenia będą wykluczone przez techniki projektowania lub programowania, niektóre zostaną zmienione lub zastąpione przez inne środki zabezpieczenia, a będą dodane niektóre nowe.

Dokonywana przez niego inspekcja będzie wówczas miała do czynienia z oceną trafności ostatecznie wdrożonych środków zabezpieczenia. Rewident może nawet natrafić na nowe metody kontroli podczas dokonywanych przez niego inspekcji, takie które nie przyszły mu do głowy na etapie planowania. Taka ocena nie ma nic wspólnego z jego początkowym udziałem. Zostałyby także włączone do systemu takie środki zabezpieczenia, których być może nie byłoby bez jego udziału, oraz bez których przedsiębiorstwo mogłoby ponieść nieobliczalne w skutkach konsekwencje.

Inspektor także skorzysta z dobrodziejstwa upewnienia się, że system będzie podatny na inspekcję. Będzie wiedział, że określony rodzaj systemu jest w danej chwili wdrażany, oraz będzie miał przez to szansę na przygotowanie planu inspekcji dla tego systemu, zanim będzie on eksploatowany. Będzie to wynikiem jego zaznajomienia się z celem systemu, które on osiągnął spełniając rolę doradcy projektantów. Ma on także sposobność wpajania projektantom, w czasie narad dotyczących planowania systemu, świadomości potrzeb inspekcji, tak, że kiedy będą pracowali nad przyszłymi systemami potrzeba udziału rewidentów może nie być tak wielka.

Podczas wywiadów kilku kierowników przetwarzania danych uskarżało się, że ich systemy były zbyt mocno kontrolowane, co powodowało znaczne zmniejszenie wydajności. Stawiali oni zarzuty rewidentom mówiąc, że w swoich badaniach kontrolnych mają tendencje do stawiania zbyt dużych wymagań, ponieważ niewiele wiedząc o przetwarzaniu danych albo o komputerach chcą się upewnić czy czegokolwiek nie przeoczyli. Kierownicy ci mają odczucie, że gdyby mogli wciągnąć rewidentów do działalności na etapie planowania systemów, byłoby to wzajemnie korzystne. Rewidenci mogliby się czegoś więcej nauczyć na temat problemów APD, a jednocześnie przekazywać swoje doświadczenie, uświadomienie o potrzebie inspekcji oraz znajomość celów przedsiębiorstwa dla potrzeb planowania systemu. Mogliby oni udzielać

porad na temat środków zabezpieczenia, aspektów prawnych oraz tego co powinno być włączone do badań kontrolnych.

Często zdarza się, że potrzeby badań kontrolnych oraz wymagania w zakresie przechowania danych nie zostały dostatecznie wyjaśnione personelowi APD, a te czasochłonne procedury, które mogą wyglądać jak bezużyteczne dla człowieka z APD, mogą być ważne. Chodzi tu między innymi o spełnienie warunków narzuconych przez różne ustawodawstwo podatkowe. Udział rewidenta w planowaniu systemów naświetla potrzebę stosowania tych procedur.

W erze komputerów rola rewidenta uległa znacznemu rozszerzeniu. Wprowadzenie systemu APD w przedsiębiorstwie jest niezmiernie kosztownym przedsięwzięciem. Rewident, jako strażnik majątku przedsiębiorstwa, powinien czuć się zobowiązany do wzięcia w tym udziału. Taka koncentracja żywotnej informacji, niezbędnej dla działania systemu przedsiębiorstwa, jaka istnieje w komputerze przedstawia sobą potencjalne ryzyko i rewident, o ile ma spełniać funkcje strażnika interesów kierownictwa, nie może sobie pozwolić na jego ignorowanie. Świadomość celów i zamierzeń przedsiębiorstwa oraz szeroki pogląd na temat całej działalności przedsiębiorstwa, dają inspektorowi szeroki pogląd, który powinien on przekazać na etapie planowania każdego rozpatrywanego systemu. Komputer zmienił sposób działania przedsiębiorstwa, a sposób działania przedsiębiorstwa dyktuje rolę rewidenta.

B. Inspektor APD

Inspektor APD posiada umiejętności oraz przeszkolenie zarówno w dziedzinie inspekcji jak i w dziedzinie przetwarzania danych. Musi on posiadać instynkt w zakresie inspekcji, zdolność zrozumienia i przyswajania technik komputerowych,oraz powinien być w stanie działać na pograniczu tych dwóch dyscyplin. Jednakże jest to ewolucja najświeższej daty.

Tradycyjny inspektor zazwyczaj był zajęty, gdy mowa była o komputerze. Czuł się świetnie w innych dziedzinach inspekcji, lecz był zrozumiale zdenerwowany jeśli chodzi o przekazywanie opinii na temat właściwego doboru operacji, o których wiedział mało lub zgoła nic. Personel przetwarzania danych mówił

innym językiem i łatwo go zagłuszał potokiem żargonu technicznego. Najłatwiejszym sposobem pozbycia się rewidenta było zaproponowanie mu, by przedyskutował problem z programistą.

W wyniku tego wiele ośrodków obliczeniowych było pozbawionych nawet najbardziej elementarnych środków kontroli nadzorczych, takich jak rozgraniczenie obowiązków. Taka sytuacja prowadziła do poważnych strat przedsiębiorstwa zarówno przez sprzeniewierzenia jak i przez kiepsko kontrolowane systemy. Kierownictwo obecnie ponownie dostało nauczkę, że żadna grupa w działalności gospodarczej nie powinna mieć monopolu w zakresie pewnej specjalizowanej wiedzy, co umożliwia jej uniknąć nadzoru i utrzymania w ryzach.

Tak długo, jak automatyzacja operacji, których inspekcji przedtem dokonywał, była ograniczona do przetwarzania na sprzęcie przetwarzania jednostkowego /maszyny licząco-analityczne/, tradycyjny rewident w dalszym ciągu czuł się dosyć pewnie, ponieważ mógł stosować te same techniki korelacji wyników z dokumentami źródłowymi, a następnie prześledzić obliczenia ręcznie. Kiedy te procesy przestawiono na komputery, czuł się mniej swobodnie, lecz w dalszym ciągu był w stanie używać wielu swoich starych technik do prowadzenia czynności rewizyjnych **"wokół"** komputera. Jednakże, o ile rewident nie przystąpi do nauczenia się czegoś na temat tego, jak komputery działają i jak się je programuje, nie będzie w dalszym ciągu w stanie właściwie zaopiniować **trafności** środków zabezpieczenia w przetwarzaniu.

Gdy komputery przeszły już ewolucję do trzeciej generacji, zaawansowana technologia oraz duży wzrost masy przetwarzanych danych uczyniły stare techniki przestarzałymi. Bez znajomości tego, jak pracują komputery, tradycyjny rewident był zgubiony. Zazwyczaj reagował on przez nadgorliwość. Powodował on stosowanie w systemach każdej techniki zabezpieczenia, jaką mógł wymyślić, jako zabezpieczenie przed opuszczeniem czegokolwiek. W wyniku tego otrzymywano systemy tak zawikłane, że były one niewydajne.

Siły Powietrzne /lotnictwo wojskowe w USA - przyp. tłum./ oraz przedsiębiorstwo AT and T, pierwsze uznały w 1958 r. potrzebę specjalistów APD w dokonywaniu inspekcji przedsiębiorstw

i stworzyły odpowiednie komórki. ATa.T utworzyło taką komórkę w ramach przedsiębiorstwa Bell Telephone Laboratories.Ci specjaliści koncentrowali się na problemach kontrolowania systemów APD oraz zapewnienia, by system nadawał się do inspekcji po wdrożeniu.

Rewident APD jest dla personelu APD konsultantem w zakresie technik zabezpieczenia systemu, a dla wydziału inspekcji - ekspertem w zagadnieniach związanych z instalowanymi systemami. Dokonywana przez niego inspekcja polega na ocenie wdrożonych technik zabezpieczenia. Zwykle nie dokonuje on inspekcji finansowej.

W ciągu ostatnich kilku lat troska kierownictwa przedsiębiorstw na temat stosunku między rewidentami a komputerem spowodowała, że coraz większa liczba przedsiębiorstw rozpoczęła budowę swojej własnej służby inspekcji APD. Ostatnio powstało kilka przedsiębiorstw konsultacyjnych dla dokonywania inspekcji w zakresie APD, podobnie w zaraniu przetwarzania na komputerach powstawały biura usługowe z zakresu oprogramowania /ang.: software house/.

Niewielu jest stosunkowo inspektorów APD i trudno ich znaleźć. W wyniku tego ich żądania w zakresie płac są wysokie. Podczas gdy nie ma pewnych danych statystycznych na temat liczby inspektorów APD lub przedsiębiorstw ich zatrudniających, to agencje pośrednictwa pracy wskazały na nagły wzrost popytu na tego rodzaju fachowców. Tu może być przykładem, że agencja pn. Robert Half przepytała swoje biura w całym kraju i ustaliła, że w pierwszych ośmiu miesiącach 1969 roku popyt na inspektorów APD wzrósł o 62 procent w stosunku do 1968 r. Przeciętne ofiarowane zarobki wynosiły $ 20.000 rocznie. Prawdopodobnie nie popełniając większego błędu można przepowiedzieć, że na tym polu będzie miała miejsce taka sama płynność kadr oraz kaperowanie inspektorów APD przez przedsiębiorstwa, jakie charakteryzowały wczesne lata programowania komputerów.

ZAŁĄCZNIK A

OBOWIĄZKI INSPEKTORA WEWNĘTRZNEGO

Po raz pierwszy w 1947 roku komitet badawczy opracował Deklarację obowiązków inspektora wewnętrznego. Wymieniona deklaracja została zatwierdzona następnie przez kolegium dyrektorów Instytutu Inspektorów Wewnętrznych /The Institute of Internal Auditors - instytut w USA - przyp.tłum./. Ewolucja i rozwój zawodu inspektora wewnętrznego spowodowały konieczność opracowania skorygowanej deklaracji celem wyrażenia szerszej koncepcji nowoczesnej działalności w zakresie inspekcji wewnętrznej.

Obecna Deklaracja została zaaprobowana przez kolegium dyrektorów wspomnianego instytutu w dniu 30 maja 1957 roku.

Istota inspekcji wewnętrznej

Inspekcja wewnętrzna jest niezależną działalnością w zakresie oceny wewnątrz organizacji. Celem jej jest zbadanie operacji w księgowości, finansach i innych jako podstawy obsługi kierownictwa. Jest to kontrola ze strony kierownictwa, której działanie polega na mierze i ocenie skuteczności innych ustanowionych organizacyjnie środków kontroli.

Cel i zakres inspekcji wewnętrznej

Ogólnym celem inspekcji wewnętrznej jest pomoc wszystkim członkom kierownictwa w skutecznym wywiązywaniu się z ich obowiązków, przez dostarczanie im obiektywnych analiz, ocen, zaleceń oraz istotnych komentarzy dotyczących badanych działalności. Dlatego inspektor wewnętrzny powinien się zajmować każdym etapem działalności przedsiębiorstwa tam, gdzie może on służyć kierownictwu. Celem osiągnięcia tego ogólnego zadania służenia kierownictwu powinno się wziąć pod uwagę takie działalności, jak:

- badanie i ocena trafności i stosowania technik zabezpieczenia w księgowości, finansach i działalnościach operacyjnych,

- upewnienie się co do stopnia zgodnośoi z ustaloną polityką, planami i procedurami,
- upewnienie się co do zakresu w jakim jest zaksięgowany majątek trwały przedsiębiorstwa oraz chroniony przed ubytkami wszelkiego rodzaju,
- upewnienie się co do niezawodności rozliczeń i innych danych opraoowanych wewnątrz organizacji,
- ooena jakości wykonywania przypisanych obowiązków służbowych.

Władza i odpowiedzialność

Inspekcja wewnętrzna jest funkcją sztabową a nie liniową. Dlatego inspektor wewnętrzny nie sprawuje bezpośredniej władzy nad innymi osobami w organizacji, której pracę bada.

Inspektor wewnętrzny powinien mieć swobodę w zakresie badania i oceny polityk, planów, procedur oraz protokołów i innych notatek służbowych; lecz przeprowadzane przez niego badania i oceny nie mogą w jakikolwiek sposób zwolnić innych osób w organizacji od nałożonej na nie odpowiedzialności.

Niezależność

Niezależność jest podstawą w skutecznym wykonywaniu programu inspekcji wewnętrznej. Ma ona dwa główne aspekty.

1. Statut organizacyjny inspektora wewnętrznego oraz udzielane mu poparcie są głównymi ozynnikami określającymi zakres i wartość usług, jakie kierownictwo otrzyma w wyniku działalności inspekcji wewnętrznej. Naczelnik wydziału inspekcji wewnętrznej powinien być odpowiedzialny przed urzędnikiem o wystarczającej randze w organizacji, oo zapewni szeroki zakres działalności oraz odpowiednie znaczenie i skuteczność akcji w wyniku przedstawionych przez niego wniosków i zaleceń.
2. Ponieważ zasadniczą sprawą w funkcji rewidenta jest pełna obiektywność,rewident wewnętrzny nie powinien opraoowywać i wdrażać procedur, sporządzać protokołów i notatek służbowych, lub angażować się w jakiejkolwiek innej działalności, którą normalnie oczekuje się, że będzie on badał i oceniał.

ZAŁĄCZNIK B

OCHRONA PRZECIWPOŻAROWA SYSTEMÓW KOMPUTEROWYCH

Poniższy materiał jest oparty na przemówieniu wygłoszonym przez Roberta W.Meyera w dniu 22 kwietnia 1965 roku na konferencji pn.: UNIVAC Users Association Spring Conference /konferencja wiosenna stowarzyszenia użytkowników komputerów UNIVAC/ w Phoenix, stan Arizona. Pan Meyer jest inżynierem ochrony przeciwpożarowej w firmie Johnson and Higgins w Nowym Jorku, stan Nowy Jork.

Normy opracowane przez przemysł ochrony przeciwpożarowej dla ochrony instalacji komputerowych są oparte na ubiegłych doświadczeniach i można się z nimi zapoznać w broszurze pn. National Fire Protection Association's Pamphlet No. 75 /Broszura Narodowego Stowarzyszenia Ochrony Przeciwpożarowej Nr 75/.

Dwa straszliwe przykłady tego problemu, który może powstać jeśli nie poświęci się dostatecznej uwagi ochronie przeciwpożarowej w czasie instalacji systemów komputerowych, udowodniły wartość pieczołowitego planowania. Jednym z tych przykładów jest niesławny pożar, który wybuchł w Pentagonie w Waszyngtonie, D.C. /siedziba Ministerstwa Obrony USA - przyp.tłum./ w dniu 2 lipca 1959 roku. Była to pierwsza poważniejsza strata w instalacji komputerowej. Skutkiem tego uzyskano znaczne ilości informacji źródłowej dla opracowania przyszłych norm.

Późnym rankiem zauważono mały płomyk w podwieszonym suficie sali zajmowanej przez Ośrodek Obliczeniowy Sił Powietrznych. W sześć godzin później, kiedy dymy opadły oraz kiedy do szpitala zabrano 40 strażaków, trzy komputery zamieniły się w spopielałe kadłuby, a 5.200 krążków taśmy leżało na dymiącej hałdzie w poczerniałym pomieszczeniu.

Szkielet budynku Pentagonu jest skonstruowany z żelbetonu. Jednakże sala komputera zawierała dwie ścianki drewniane. Podłogi i drzwi tego pomieszczenia były z drzewa, a nad pomieszczeniem wisiał łatwopalny sufit w odległości 1,2 metra od

żelbetowego stropu. W jednym rogu sali Siły Powietrzne magazynowały około 5.200 krążków taśmy w małym drewnianym ogrodzeniu, które było przeznaczone jako schowek zabezpieczający. Ten schowek zawierał taśmy magnetyczne ułożone na półkach metalowych, a niektóre z tych półek posiadały metalowe drzwiczki. Na tym obszarze znajdowało się pięć jednostek klimatyzacji powietrza i chociaż centralny system klimatyzacyjny budynku nie zasilał omawianego obszaru, kanały centralnego systemu przechodziły przez przestrzeń między sufitem żelbetowym a sufitem podwieszonym.

Kiedy do sali zaczął się przedostawać dym, jeden z inżynierów rozpoczął poszukiwanie przyczyny w towarzystwie cywilnego pracownika Sił Powietrznych. Wydawało się, że dym pochodził z sufitu, w pobliżu pomieszczenia magazynu taśm. Pomieszczenie to zostało niedawno powiększone i w czasie zmian zaistniała konieczność przemieszczenia armatury oświetleniowej.

Inżynier usunął szereg płyt z podwieszonego sufitu i zajrzał do przestrzeni między stropem żelbetowym a podwieszonym sufitem. Zauważył on płonące rumowisko i przy pomocy innych zastosował gaśnicę z dwutlenkiem węgla. Wydawało się, że ogień zlokalizowano, lecz wkrótce dym pojawił się znów i widziano płomienie; prawdopodobnie ogień był rozdmuchiwany przez system klimatyzacyjny budynku.

Prawdopodobnie nie było zorganizowanej wewnętrznej brygady straży przeciwpożarowej i do akcji nie włączono węży do polewania, ani innych gaśnic poza początkowo użytymi z dwutlenkiem węgla. Zawołano straż pożarną.

Prawdopodobną przyczyną tego pożaru było zwarcie w instalacji oświetleniowej w podwieszonym suficie, które spowodowało zapalenie łatwopalnych śmieci pozostawionych przez przedsiębiorcę budowlanego. Do tego pożaru głównie przyczynił się materiał akustyczny w podwieszonym suficie /wyłożony w celu pochłaniania dźwięków/, który ze swej natury był łatwopalny.

Przy pierwszych oznakach ognia, inżynier odciął dopływ energii elektrycznej do całego sprzętu komputera. Gdy komendant straży pożarnej usiłował odłączyć system klimatyzacyjny od płonąoych pomieszczeń stwierdził, że pomieszczenie central-

nego systemu klimatyzacji jest zamknięte i nie ma nikogo,kto miałby klucze. System klimatyzacyjny działał w całym czasie trwania pożaru znacznie rozdmuchując ogień i niewątpliwie powodując jego szybkie rozprzestrzenianie się.

Pojemniki i krążki taśmy nie były wówczas uważane za wysoce łatwopalny materiał; były one wykonane z plastyku polistyrenowego, który, jak się później okazało, posiada punkt zapłonu 221°C /430°F/. Materiał ten poddany intensywnemu nagrzaniu zamienia się z wolnopalnego na szybkopalny i oszacowano, że w czasie omawianego pożaru temperatura w pomieszczeniu osiągnęła około 1100°C /2000°F/. Płonąc, pojemniki i krążki wytwarzały ciężki czarny dym, który nie był toksyczny,lecz obezwładniał strażaków i wielu z nich musiano wysłać do szpitala. Pojemniki także wytworzyły popiół, który rozprzestrzenił się kanałami klimatyzacji powietrza do innych części budynku.

Następujące czynniki przyczyniły się do tak poważnych i rozległych strat:

- łatwopalne materiały konstrukcyjne użyte w całym pomieszczeniu,
- wielka liczba taśm magnetycznych przechowywana w niechronionym obszarze,
- brak jakiejkolwiek zorganizowanej wewnętrznej straży pożarnej,
- brak jakiegokolwiek sprzętu do wykrywania ognia,
- opóźnienie w powiadomieniu straży pożarnej,
- niemożność wyłączenia systemu klimatyzacji powietrza i brak dostępu do głównego wyłącznika tego systemu, łącznie z brakiem zasuw przeciwpożarowych we wszystkich kanałach, które przenikały przez ściany otaczające omawiane pomieszczenie.

W innym przykładzie dużych strat w tego typu sprzęcie chodziło o całą instalację komputerową. Gmach, w którym umieszczono system, był konstrukcji całkowicie niepalnej.Mieścił on bardzo złożony i stłoczony system komputerowy, z licznymi kablami sieciowymi i połączeniowymi,schowanymi w zamkniętej przestrzeni w suficie na wysokości linii dachu.

O godzinie 3 po południu zaobserwowano iskrzące zwarcia elektryczne, które operatorzy zwalczyli przy pomocy gaśnic z dwutlenkiem węgla. Węże strażackie i woda nie były dozwolone w budynku z powodu obecności sprzętu komputerowego. Wszczęto alarm o pomoc ze strony zakładowej straży pożarnej.

Około godziny 3.10 zarządzono, by cały personel opuścił budynek z powodu gęstego dymu i wyziewów i chociaż było tam wiele gaśnic z dwutlenkiem węgla użyto zaledwie kilku. Straż pożarna użyła motopomp wyposażonych w zbiorniki wodne, lecz nie mogła wejść do budynku z powodu gęstego dymu. O godzinie 3.38 wyłączono całe zasilanie energetyczne, wliczając w to energię dla pomp wodnych. Całe zwalczanie ognia było prowadzone z zewnątrz budynku i w wyniku tego powstały poważne uszkodzenia w strukturze budynku, a także w sprzęcie umiejscowionym w obszarze ośrodka obliczeniowego.

Później zbadano cały obszar objęty pożarem; pożar zniszczył wszystkie przewody w przykrytych kanałach, a sprzęt komputerowy umieszczony na sali doznał poważnych uszkodzeń.

Ogień w pierwszych chwilach rozprzestrzeniał się na plastykowych izolacjach kabli i przewodów dając gęsty i drażniący dym, który utrudniał akcję zwalczania ognia. Dokumentacja powinnabyła określić, że w tych zamkniętych kanałach w suficie można było użyć tylko kabli zatwierdzonych przez uznane laboratoria do użytku w systemach komputerowych. Gdyby to miało miejsce, wątpliwe czy pożar mógłby się tak rozprzestrzenić i spowodować tak rozległe szkody.

Powyższe dwa przykłady przedstawiają jasno, że w ośrodku obliczeniowym mogą powstać poważne straty, nawet mimo tego, że podstawowy sprzęt sam ze swej natury nie jest łatwopalny.
Z powodu tego potencjału strat Narodowe Stowarzyszenie Ochrony Przeciwpożarowej utworzyło komitet złożony z przedstawicieli wszystkich poważniejszych produoentów komputerów, a także z przedstawicieli rządu, przemysłu i ubezpieczeń. Jego zadaniem było opracowanie norm dla właściwej ochrony przeciwpożarowej omawianego sprzętu. Komitet ukonstytuował się na początku roku 1960, a nieobowiązujące normy po raz pierwszy przedstawiono w 1961 roku na posiedzeniu Konwencji Narodowego Stowarzyszenia Ochrony Przeciwpożarowej. W 1962 roku przyjęto

ostateczną formę tych norm. Poniżej przedstawiamy zarys zasadniczych zaleceń tego komitetu.

Gdzie to możliwe, wszystkie instalacje komputerowe powinny być umieszczone w budynkach niepalnych lub ognioodpornych. O ile jest to niemożliwe, instalacja komputera powinna być lokalizowana w pomieszczeniu zbudowanym z całkowicie niepalnych materiałów, wytrzymujących co najmniej jednogodzinny pożar i oddalonym od wszelkich obszarów o dużym zagrożeniu, takich jak reprezentowane przez płyny łatwopalne lub niebezpieczne materiały wybuchowe. Wszystkie materiały pokrywające podłogę, materiały akustyczne, wykończenie wnętrz oraz podwieszone sufity powinny posiadać szybkość rozszerzania płomienia mniejszą od 25, potwierdzoną przez jedno z upoważnionych laboratoriów doświadczalnych.

Podłogi podniesione, tam gdzie to jest wymagane ze względu na ułożenie kabli oraz klimatyzację, powinny być z materiałów całkowicie niepalnych, przy tym powinien być zapewniony dostęp do przestrzeni pod podłogą. O ile podposadzka wykonana jest z materiału palnego, to wówczas ten cały obszar powinien być osłonięty materiałem niepalnym takim, jak twarde płyty azbestowe. Powinien być zapewniony właściwy odpływ wody, by się zabezpieczyć przed gromadzeniem wody podczas zwalczania pożaru oraz na wypadek ulewnych deszczów.

Należy ograniczyć ilość materiałów łatwopalnych dopuszczalnych w każdym pomieszczeniu przeznaczonym dla komputerów. Zaleca się, by wszystkie meble były z materiałów niepalnych oraz by jakiekolwiek biura kierownictwa umieszczone na omawianym obszarze były ograniczonej wielkości oraz ilość umieszczonych tam materiałów łatwopalnych ograniczono do minimum.

By wyeliminować możliwość zupełnego przerwania obsługi, dwa oddzielne komputery nie powinny być umieszczane w jednym pomieszczeniu. Może to się okazać niepraktyczne w wypadku gdy systemy są połączone elektronicznie, wykorzystują ten sam sprzęt wejścia-wyjścia, albo z przyczyn operacyjnych muszą być umieszczone w tym samym pomieszczeniu. Lecz wszędzie tam, gdzie to możliwe, wszystkie systemy powinny być oddzielane w swoich indywidualnych strefach ochrony przeciwpożarowej.

Operowanie systemem komputerowym często wymaga znacznych ilości dostaw papieru na wydruki i innych łatwopalnych materiałów pomocniczych. Tego rodzaju materiały mogą sobą przedstawiać poważne niebezpieczeństwo pożaru w sali komputera. Wszelkie zapasy papieru, niewykorzystywane nośniki zapisu informacji oraz inne materiały łatwopalne, powinny być ograniczane w sali komputera do absolutnie niezbędnego minimum, koniecznego do sprawnego operowania maszyną. Każdy tego rodzaju materiał w sali komputera powinien być przechowywany w całkowicie zamkniętych metalowych ognioodpornych pudłach lub skrzynkach, a pozostały materiał powinien być przechowywany na zewnątrz sali komputera.

Elektroniczne wyposażenie komputera jest podatne na poważne uszkodzenia przy dłuższym stykaniu się z ogniem, dymem, lub wodą. Przegrzanie / do zaledwie 60°C może spowodować złe funkcjonowanie niektórych tranzystorów, a temperatury powyżej 150°C mogą trwale uszkodzić te urządzenia.

Dotychczas nie skonstruowano systemu komputerowego z całkowicie niepalnych materiałów. W większości z nich korzysta się z przewodników, które zależnie od rodzaju instalacji, są w pewnym stopniu palne. W tych systemach także znajdują się plastykowe płytki z obwodami drukowanymi, oporniki, pojemności, transformatory, różnego rodzaju materiały izolacyjne oraz sprzęt pomocniczy taki, jak wentylatory z silnikami, filtry oraz klimatyzatory powietrza, które posiadają różny stopień łatwopalności.

O ile te materiały są zgromadzone we wspólnej obudowie, ogień może się szybko rozprzestrzenić, szczególnie, jeśli różne części posiadają podwyższoną temperaturę gdy nastąpi zapłon. O ile łatwopalne elementy w jakiejś jednostce zapalą się i nie zostaną szybko ugaszone, ta jednostka może ulec zniszczeniu.

Jest mało prawdopodobne, by ogień rozprzestrzenił się na inne jednostki, jeśli są one oddzielone nawet cienkimi ściankami metalowymi, a w pomieszczeniu i w przestrzeni pod podniesioną podłogą jest zapewniona właściwa ochrona. Dym i sadza wydzielające się wewnątrz sprzętu i przenoszone przez system rozdziału powietrza, mogą spowodować złe działanie urzą-

dzeń elektrycznych i elektronicznych. Jest niesłychanie ważne, by każdy ogień wewnątrz sprzętu był wykrywany tak szybko jak to jest możliwe. Skoro zostanie wykryty, całe zasilanie tej jednostki powinno być odłączone, aby zapobiec dalszemu podgrzewaniu sprzętu.

Zaleca się, by w przestrzeni pod podniesioną podłogą oraz ponad podwieszonym sufitem, były umieszczone wykrywacze dymu lub ognia, o ile te obszary zawierają kable energetyczne i pomocnicze oraz jakikolwiek materiał łatwopalny. Wykrywacze takie powinny być instalowane w salach komputerowych dla małych instalacji oraz wewnątrz szaf komputera w dużych rodzajach jednostek. Ten sprzęt powinien wykrywać ogień w jego początkowych etapach, kiedy jest produkowana tylko mała ilość dymu oraz powinien natychmiast uruchamiać alarm dźwiękowy, wskazujący,że w tym obszarze występuje złe funkcjonowanie urządzenia.

W następstwie tego alarmu powinno zostać wyłączone zasilanie z sieci elektrycznej dla systemu komputerowego i o ile system ostrzegawczy jest dosyć rozległy, obszar, w którym wykryto ogień, powinien być wskazany na panelu centralki przeciwpożarowej. O ile ogień zostanie wykryty na dosyć wczesnym etapie, to w większości wypadków może on być ugaszony w sprzęcie komputera za pomocą małej gaśnicy ręcznej na dwutlenek węgla, a niezbędne naprawy ograniczą się do minimum.

O ile pozwoli się na rozszerzenie ognia, może on spowodować całkowite zniszczenie sprzętu komputera. Oczywiście wszystkie osoby pracujące na terenie ośrodka obliczeniowego powinny być dokładnie przeszkolone w użyciu dostępnych typów sprzętu do zwalczania ognia i to przeszkolenie powinno wyeksponować możliwości i ograniczenia tego rodzaju sprzętu przeciwpożarowego.

W dużych instalacjach, których strata spowodowałaby nie do odrobienia szkody w działalności gospodarczej, albo w jednostkach zaprogramowanych do sterowania procesem w jakiejś działalności wytwórczej, jest konieczne, aby wszelkie pożary były stłumione,a czas przerwy w korzystaniu z tego sprzętu tak mały, jak tylko możliwe. W tego rodzaju jednostkach zaleca się, by do wnętrza ich obudowy był automatycznie doprowadzany dwutlenek węgla.

Większość operacji komputera zależy całkowicie od zachowania nośników informacji. Nawet wówczas, gdy sprzęt komputera jest zniszczony, wiele operacji może być podjętych na innych instalacjach, o ile zostały zachowane zapisy z informacjami. Jednakże zniszczenie zapisów może spowodować całkowite zatrzymanie wszystkich operacji na czas nieokreślony.

Wielu użytkowników przechowuje duplikaty zapisów, niekoniecznie w tej samej formie, ale przechowywane oddzielnie i szybko dostępne tak, że informacja wymagana dla nieprzerwanej operacji może być szybko przygotowana lub reprodukowana. Duplikaty zapisów mogą być przechowywane w postaci kart dziurkowanych i taśm dziurkowanych, ręcznie lub maszynowo wypisanych arkuszy oraz w postaci taśm magnetycznych, bębnów, kart magnetycznych, dysków i rdzeni.

W czasie aktualizacji na jednoczesną stratę są narażone w sali komputera dwa zestawy zapisów informacji. Dla tej przyczyny niektórzy użytkownicy przechowują potrójne taśmy wejściowe, chociaż informacja na wszystkich trzech nie jest identyczna. Pierwsza będzie posiadać ostatnią informację, druga będzie nieco zdezaktualizowana, a trzecia jeszcze bardziej, zależnie od częstotliwości operacji aktualizacji. Lecz nawet ta trzecia będzie zwykle posiadać większość podstawowych danych niezbędnych dla ciągłości operacji i może ona zostać szybko zaktualizowana za pomocą innych zapisów w przypadku, gdy te dwa pierwsze zostaną zniszczone.

Wszystkie żywotne dla organizacji zapisy powinny być umieszczone w skrytkach lub w zatwierdzonych szafach do ich przechowywania, posiadających etykietę klasy "C"; wskazuje ona na to, że taka szafa jest ognioodporna w ciągu jednej godziny, gdy temperatura otoczenia wynosi 940°C. Duplikaty żywotnych dla organizacji materiałów informacyjnych, przechowywane na zewnątrz pomieszczeń komputera, powinny być umieszczane w ognioodpornych skrytkach posiadających wytrzymałość co najmniej dwugodzinną.

By mieć pewność, że ogień powstały w innych częściach zakładu nie przeniesie się do obszaru zajmowanego przez komputer, jest koniecznością, by dla wszystkich instalacji komputera był zapewniony oddzielny system klimatyzacji powietrza oraz by ten system nie był połączony z jakimikolwiek innymi część-

ciami budynku. Filtry używane w tym systemie powinny być zapewnione we wszystkich kanałach, które przecinają ściany sali komputera.

Dla systemu klimatyzacji powietrza w obszarze komputera powinien być przewidziany wyłącznik instalacji. Najlepiej,by był on ulokowany przy drzwiach wejściowych do obszaru komputera tak, by urządzenie klimatyzacyjne mogło być wyłączone w przypadku niebezpieczeństwa pożaru.

Całe zasilanie energią elektryczną powinno być sterowane przez oddzielny wyłącznik mocy, także umieszczony przy drzwiach wejściowych. Przyłącza transformatorowe autotransformatory i inne nie powinny być dozwolone na sali komputera, a na wszystkich przyłączach mocy powinna być zapewniona wystarczająca ochrona odgromowa.

Ostatnim - i być może najważniejszym - etapem ochrony przeciwpożarowej w instalacji komputera jest właściwe przeszkolenie personelu.

Powinny być wypracowane pełne procedury postępowania w nagłych wypadkach, a ich kopia na piśmie powinna być dostarczona całemu personelowi. By być pewnym, że będzie się postępować według tych procedur, są niezbędne okresowe ćwiczenia.

ZAŁĄCZNIK C

LISTA KONTROLNA INSPEKCJI SYSTEMU

Poniższy materiał wzięto z publikacji pt. "Przewodnik oceny kontroli wewnętrznej w systemie komputerowym i w instalacji komputerowej", opracowany i używany w Texas Instruments Incorporated. Lista kontrolna została podzielona na pięć głównych działów:

- organizacyjne środki kontroli
- środki kontroli przemieszczania i konwersji danych
- programowane środki kontroli
- środki kontroli programowania
- proceduralne środki kontroli

Oczywiście podstawowym celem tej listy kontrolnej jest wykrycie obszarów niedostatecznych środków kontroli wewnętrznej tak, aby główna poprawa mogła być uzyskana w określonych systemach informacji ekonomicznej, w zabezpieczeniu instalacji, w procedurach itd. Po zakończeniu każdej podlisty, inspektorowi zaleca się wykonanie wszelkich niezbędnych testów, by sprawdzić mocne strony /odpowiedź "tak"/, lub by ocenić potencjalne braki /odpowiedź "nie"/ lub by poprzeć spisane notatki. Listę kontrolną reprodukujemy w całości po przedstawieniu kluczowych definicji:

Funkcje Systemu Zarządzania dotyczą operacji opracowania i wspomagania skomputeryzowanych systemów informacji kierownictwa. Do tej funkcji można także włączyć obsługę komputera, jednostek dziurkowania /przygotowania danych/ oraz jednostki kontroli danych.

Funkcje Przetwarzania Danych zawierają obsługę komputera, kontrolę danych oraz przygotowanie danych /wszystko z Systemów Zarządzania z wyjątkiem projektowania i programowania/.

Funkcje Operacyjne jest to działalność organizacji, która jest użytkownikiem usług Przetwarzania Danych lub planowanym odbiorcą projektowanego systemu komputerowego.

Inspekcja Operacyjna /Eksploatacyjna/ Instalacji Komputera polega na przebadaniu organizacji Systemów Zarządzania w aspektach przetwarzania informacji ekonomicznej.

Zakres i cele:

- przegląd zastosowań komputera i związanych z nimi kosztów,
- określenie zasięgu zgodności z zasadami organizacji Systemów Zarządzania i ich procedurami,
- stwierdzenie, czy wewnętrzne operacyjne środki kontroli istniejące w Systemach Zarządzania są właściwe dla zapewnienia ścisłości i niezawodności przetwarzanej informacji,
- ujawnienie niebezpieczeństw zagrażających nienaruszalności systemów komputerowych /włączając przechowywane dane oraz przetwarzanie/, środków trwałych i personelu,
- wszelkie istotne stwierdzenia, które mogą zainteresować kierownictwo, zostaną uwidocznione, niezależnie od tego, czy objęte są powyższym zakresem inspekcji, czy nie.

Inspekcja Systemu Zarządzania polega na przebadaniu określonego systemu informacji ekonomicznej.

Zakres i cele:

- stwierdzenie, czy techniki zabezpieczenia wewnętrznego, zastosowane w organizacji używającej i przetwarzającej omawianą informację, są właściwe,
- stwierdzenie, czy informacja przetwarzana przez te systemy jest materialnie poprawna,
- przegląd: kroków podjętych dla zapobieżenia oszustwom i dla zwiększenia wydajności i efektywności, potrzeb w zakresie prawnym i podatkowym, potrzeb następnych inspekcji, zgodności z polityką przedsiębiorstwa i wykorzystania nakładów przez system,
- poza tym powinny zostać uwidocznione wszystkie istotne stwierdzenia, które mogłyby zainteresować kierownictwo, bez względu na to, czy są zawarte w powyżej przedstawionym zakresie inspekcji.

LISTA KONTROLNA INSPEKCJI

OCENA WEWNĘTRZNYCH ŚRODKÓW KONTROLI SYSTEMÓW

I. ORGANIZACYJNE ŚRODKI KONTROLI

Środki kontroli nad rozgraniczeniem obowiązków

Są to środki kontroli zawarte w strukturze obowiązków i odpowiedzialności, by zapewnić odpowiednie rozgraniczenie obowiązków. Wynikiem jest system kontroli i decyzji w całej organizacji i jej strumieniu przetwarzania informacji. Tego rodzaju środki kontroli wówczas zmniejszają niekontrolowane skoncentrowanie odpowiedzialności na każdym szczeblu organizacyjnym.

A. Przygotuj schemat organizacyjny dla badanego obszaru. Schemat ten ma przedstawiać przydzielone funkcje.

B. Czy jednostki operacyjne oraz jednostki Systemu Zarządzania są niezależne funkcjonalnie i organizacyjnie?

C. Czy funkcja Systemu Zarządzania wyklucza kontrolę nad aktywami przedsiębiorstwa niezwiązanymi z jego funkcjami usługowymi?

D. Czy w ramach przetwarzania danych operacje na maszynie są funkcjonalnie oddzielone od kontroli danych?

E. Czy istnieją na piśmie zakresy obowiązków dla opracowania i konserwacji systemów, dla przetwarzania danych oraz dla jednostek operacyjnych?

F. Czy odpowiedzialność jest łatwa do ustalenia i wyodrębnienia tak, by można było wskazać, kto jest odpowiedzialny za:

- zbieranie danych źródłowych według rodzaju,
- przepisywanie danych źródłowych na formularze, które będą wykorzystane do konwersji na maszynowe nośniki informacji,
- konwersję danych na formę czytelną dla maszyny,
- planowanie i odbiór wyników działalności w zakresie przetwarzania danych /włączając w to decydowanie o kolejnoś-

ci i pierwszeństwie zadań/,

. przegląd każdego przebiegu:

a/ na dokładność ze strony systemu,
b/ na dokładność danych,

. korekcję błędów,

. przegląd poważniejszych błędów przez kierownictwo,

. dystrybucję wyjścia,

. transmisję danych.

G. Oceń jak dalece pracownicy znają zakres swoich obowiązków oraz obowiązki pracowników, z którymi stykają się roboczo.

Administracyjne środki kontroli

A. Czy praca jest tak planowana, by wyeliminować problemy przeciążenia?

B. Czy płynność kadr w jednostkach systemowych, przetwarzania danych oraz operacyjnych jest mniejsza niż 10% w ciągu ostatniego roku? Jeśli powyżej 10% - omów sytuację.

C. Czy harmonogramy prac ustalające godziny robocze są przestrzegane i czy nie występuje zbyt duża liczba godzin nadliczbowych?

D. Czy pracownicy są opłacani za zaplanowane lub spowodowane koniecznością godziny nadliczbowe? Jeśli była ich znaczna ilość, wynotuj liczbę godzin w roku na pracownika.

E. Czy absencja i spóźnienia mają niewielkie rozmiary?

F. Czy jest odpowiedni nadzór nad pracownikami?

G. Czy obowiązki, uprawnienia i odpowiedzialność pracowników wydają się współmierne z innymi pracownikami przedsiębiorstwa, uwzględniając wynagrodzenie?

H. Czy wymaga się od pracowników, by brali urlopy zgodnie z polityką przedsiębiorstwa?

I. Czy pracownicy zmieniają kolejno przydziały prac, by zapewnić wzajemną kontrolę przy pracy?

J. Czy w jednostkach organizacyjnych personel podnosił problemy typu organizacyjnego?

II. ŚRODKI KONTROLI PRZEMIESZCZANIA I KONWERSJI DANYCH

A. Środki kontroli ustalone w jednostkach operacyjnych w celu sprawdzenia, że wszystkie dane zostały przesłane do jednostki Przetwarzania Danych oraz środki kontroli mające na celu upewnienie się, że wszystkie dane zostały włączone do procesu przetwarzania.

1. Przygotuj notatkę opisującą dla każdego źródła danych[x/] przekazywanego z jednostki operacyjnej do Przetwarzania Danych środki kontroli[xx/], mające na celu zabezpieczenie się przed:

   . stratą pola z jakiejś transakcji,
   . stratą transakcji z wsadu /partii/,
   . stratą wsadu /partii/ transakcji,
   . stratą wyjścia z komputera odzwierciadlającego wprowadzenie danych,
   . stratą danych lub dodaniem danych z powodu przerwy

   /wskazać kto jest odpowiedzialny za każdy rodzaj kontroli/.

---

x/ Za źródła danych uważamy:
   . formularze dla dziurkowania,
   . formularze kontrolne dla wsadów /partii/ wykazujące sekwencję wsadu, sumy kontrolne/pieniężne oraz zaliczanie transakcji,
   . dokumenty źródłowe,
   . transakcje na końcówce /terminalu/,
   . karty wstępnie dziurkowane.

xx/ Za środki kontroli uważamy:
   . zliczanie formularzy,
   . program,
   . zliczanie dokumentów/danych itp.,
   . potwierdzenie przyjęcia przy przetwarzaniu na bieżąco,
   . sprawdzanie wszystkich pól danych na żądany rodzaj danych oraz na znane ich kombinacje, jeśli takie występują.

2. Czy wyżej przedstawione techniki zabezpieczenia są spisane i zrozumiane przez wszystkich, którzy są odpowiedzialni za ich wykonanie? Wskazać kto kontroluje stosowanie.

3. Jakiej techniki zabezpieczenia używa się na wejściu do systemu takiego, jak karty sterujące lub karty etykiet danych, by upewnić się, że jest odpowiedni stan i dokładność ustawienia systemu przed rozpoczęciem przetwarzania danych?

4. Jeśli używa się dokumentów "obiegiem", jakie środki są użyte by zweryfikować ich prawidłowość? /Dokumenty "obiegiem" są przygotowywane przez przetwarzanie danych, przesyłane do jednostki operacyjnej i następnie zwracane z ewentualnie zakodowanymi dodatkowymi danymi - na przykład: karty magazynowe lub karty obecności wstępnie wydziurkowane/.

5. Czy są przygotowywane określone raporty /wylistowanie transakcji itp./, które są pomocne przy weryfikowaniu kompletności lub obecności danych?

6. Czy wykonuje się kontrole poprawności formy /wydruki kontrolne/ lub pobiera próbki by się upewnić, że wymienione wyżej funkcje kontrolne działają, a dane są ważne?

B. Środki kontroli ustanowione w wydziale przekształcającym dane na formę czytelną dla maszyny. /Wyłączając kontrole przemieszczania/.

Te techniki zabezpieczenia dają pewność, że dane źródłowe są prawidłowo przekształcone z formularza /lub innego źródła/ na formę czytelną dla maszyny.

1. Opis techniki zabezpieczenia przy przekształcaniu danych /konwersji danych/, mające na celu zapewnienie dokładności. Należy tu włączyć takie pozycje jak:
   - sprawdzanie za pomocą klawiatury po dziurkowaniu /karty i taśmy/,
   - redakcję na bieżąco danych kontrolnych dla terminali,

. cyfry kontrolne dla maszyn dziurkujących lub inne kontrole logiczne.

2. Jaką wykonuje się sprawozdawczość dotyczącą wydajności przy przekształcaniu danych, by się upewnić, że częstotliwość błędów i "przerób" są możliwe do przyjęcia?

3. Czy błędy wykrywane przy weryfikacji są systematycznie analizowane oraz czy bierze się próbki z pól niezweryfikowanych?

4. Jakie mogą być skutki pochodzące z pól danych, których przekształcanie nie jest kontrolowane?

5. Jakie, zdaniem personelu, jest największe ryzyko w omawianym obszarze dla przedsiębiorstwa?

III. PROGRAMOWANE ŚRODKI KONTROLI

Programowane środki kontroli są to techniki zabezpieczenia zawarte w programie komputera, których zadaniem jest wykrycie błędów, zwrócenie uwagi na wątpliwe pozycje oraz odpowiednie uwidocznienie takich wyjątków. Te techniki są podzielone na środki kontroli odchyleń w danych, środki kontroli odchyleń w systemie oraz na uzupełniające środki kontroli.

A. Programowane środki kontroli odchyleń w danych

Są to techniki zabezpieczenia, mające na celu uniknięcie nieścisłych lub niezatwierdzonych danych, kwestionowanie anomalii w danych, które mogą być prawidłowe lub nie oraz mające za zadanie wykrycie danych niekompletnych lub obcych /niezwiązanych z danym przetwarzaniem/. Te techniki zabezpieczenia mogą mieć zastosowanie, zarówno do danych historycznych, jak i do nowych transakcji wprowadzanych do systemu.

Należy udokumentować sprawdzanie programowane na prawomocność danych. Należy omówić redagowane pola oraz rodzaj redagowania. O ile to możliwe, należy wymienione omówienie przedstawić w postaci tabelarycznej. Można uwzględnić następujące rodzaje redagowania danych:

a/ czy dokonuje się sprawdzenia linii postępowania i zatwierdzeń, by określić czy wskazany wydział lub szczebel zatwierdzania jest właściwy dla danej transakcji?

b/ czy wykonuje się testy na obecność i kompletność, by się upewnić, że dane, które mają być przetwarzane, są dla właściwego okresu czasu, oraz że są obecne wszystkie dane dla tego okresu? /problemy wyłączenia systemu - np. brak dopływu prądu, przyp.tłum./,

c/ czy programy dokonują sprawdzenia danych wejściowych na okoliczność ich utraty lub zmiany?

Należy uwzględnić następujące rodzaje testów:

- sumy kontrolne dla wsadu /partii/ danych. Spowoduje to wykrycie utraty lub zmiany danych, które wpływają na kontrolowane pole,
- zliczanie zapisów we wsadzie /partii/ wykryje utratę kompletnego zapisu nawet wówczas, gdy utracone dane nie wpływają na sumy kontrolne lub te ubytki wpływają na sumy kontrolne lub straty wzajemnie się równoważą,
- zliczanie wsadów /partii/ wykryje utratę kompletnego wsadu danych,

d/ jeśli dla pewnych pól dopuszczalne są jako ważne tylko pewne wybrane /wg uznania użytkownika/ dane lub kody, czy dokonuje się kontroli zapewniającej, że wszystkie dane bezwzględnie odpowiadają tym ograniczeniom? Można to zrobić przez porównanie z tabelą wyliczającą ważne kody itp.,

e/ czy wykonuje się testy dla innych wykrywalnych błędów?

Należy tu uwzględnić:

- liczby samokontrolujące się,
- kontrole ograniczeń dla zakresu,
- kontrole kombinacji logicznych,
- badania znaków,
- badania charakteru danych.

B. Środki kontroli odchyleń w systemie

Są to techniki,mające na celu uniknięcie niewykrytych błędów spowodowanych przez pominięcia lub niedokładności w systemie oprogramowania, sprzęcie lub w procedurach operacyjnych.

1. Czy programy sprawdzają w wystarczający sposób wtedy, gdy inicjowany jest przebieg przetwarzania, czy korzysta się z właściwych zbiorów danych? Należy uwzględnić następujące punkty:

   - czy używa się kart sterujących pracą /Job Control Language cards/ do niewątpliwego rozpoznawania używanych zbiorów danych? /Czy istnieją różne wersje lub generacje tych samych nazwach zbiorów danych?/,
   - czy używane są "Słowa Kluczowe" Języka Sterowania Pracą /czyli JCL = Job Control Language/ dla ochrony przed nieupoważnionym lub mylnym użyciem lub zniszczeniem zbiorów danych?,
   - czy programy /na pewno/ sprawdzają karty wejściowe /oraz inne dane źródłowe/ co do danych, rodzaju oraz według innych niezbędnych klasyfikacji? Można to zrobić za pomocą kart nagłówkowych /z etykietą/ dołączonych jako część danych do programu,
   - czy aby uniknąć pełnego ponownego powtarzania przebiegów korzysta się z własności restartów od punktów kontrolnych? O ile zbiory główne aktualizuje się na bieżąco, restart może być jedynym sposobem odtworzenia danych gdy występują błędy.

2. Czy w oprogramowaniu istnieją techniki kontrolne mające na celu wykrycie złego funkcjonowania sprzętu, oprogramowania lub danych?

   - jakie jest przetwarzanie przez system błędu na wejściu/wyjściu? /Podano przykłady odnoszące się do konkretnego oprogramowania dla konkretnej konfiguracji - przyp.red./,

- czy przerwania typu błędu w programie powodują zakończenie prac? /Jak wyżej - przyp.red./,
- czy liczniki zapisów, używane w pakietach oprogramowania, są tego typu, co używane do wykrycia straty danych?

3. Czy w systemie zaprojektowano techniki kontrolne dla wykrywania złego funkcjonowania jego własnych programów? Należy uwzględnić:
   - redakcje kontrolne zbiorów głównych, które okresowo badają wyczerpująco wszystkie dane na prawidłowość,
   - wzajemne kontrole między programami, które w przypadku występowania błędów logicznych tworzą komunikaty o odchyleniach,
   - techniki programowania,
   - czy programy zawierają procedury redagujące zależności logiczne, mające na celu zapewnienie nienaruszalności logiki programu? /Amortyzacja całkowita ≤ amortyzacja w tym roku ≤ amortyzacja w tym miesiącu/. Tu przyjmuje się, że kontrola redakcyjna za pomocą programowanych danych kontrolnych uchroni przed wystąpieniem takiego zjawiska, a zatem każdy taki przypadek sugeruje błąd systemu,
   - czy programy zapewniają kontrolę kolejności, która ma na celu sprawdzenie dokładności oczekiwanej kolejności, jeśli taka istnieje?

C. <u>Uzupełniające środki kontroli</u>

Są to techniki zabezpieczenia, mające zapewnić, że odchylenia w danych oraz odchylenia w systemie zostaną odpowiednio uwidocznione, oraz że zostaną podjęte odpowiednie akcje korygujące, gdy zajdzie tego potrzeba.

1. Czy istnieje kontrola redakcyjna odchylenia typu wyjątek/przekroczenie? Na przykład rozpatrzmy płatne godziny w tygodniu:

. mniej niż 80 godzin: przetwarzać bez wyjątków,

. więcej niż 80 godzin, lecz mniej niż 158 godzin:
  - jeśli brak wskaźnika przekroczenia, traktować jako błąd,
  - jeśli jest obecny wskaźnik przekroczenia, przetwarzać,

. przygotować raporty wykazujące przekroczenia i błędy.

Jeśli używa się tego typu systemu, czy dostatecznie uwidoczniono przekroczenia?
Czy przekroczenia zachowano dla potrzeb inspekcji?

2. Czy użyto odpowiednich procedur dla korekcji i ponownego wprowadzenia odchyleń danych wejściowych z odchyleniami, potraktowanych jako błędy i odrzuconych?Uwzględnij techniki zabezpieczenia, mające na celu zapewnienie, że wszystkie odrzuty na wejściu są ponownie wprowadzane, oraz że nie robi się podwójnych korekcji.

3. Jeśli błędy lub odchylenia zostają wykryte po aktualizacji zbiorów historycznych lub po wykorzystaniu takich danych w raportach, czy użyto wystarczających środków w celu ujawnienia tej informacji? /Ten rodzaj raportu błędu powinien być oddzielony od błędów omówionych w poprzednim pytaniu/.

4. Jeśli zostaną wykryte błędy systemu, to jakie techniki zabezpieczenia nadzorują ich korekcję?

5. Jeśli w systemie wystąpią większe zmiany lub błędy, czy jednostki tym dotknięte wiedzą o potrzebie zachowania danych historycznych dla celów inspekcji?

6. Kto jest odpowiedzialny za przebadanie:
   . odrzutów danych wejściowych,
   . błędów w danych użytych do sprawozdań /raportów/,
   . błędów w systemie.

IV. ŚRODKI KONTROLI PROGRAMOWANIA

Obejmują metody kolektywne, które mają zapewnić, aby postępowano zgodnie z odpowiednimi procedurami w czasie opracowywania systemu, jego konserwacji, dokumentacji i konwersji.

A. Środki kontroli planowania i opracowania

Są to techniki kontrolne, zapewniające sprawdzenie w zakresie właściwego upoważnienia na opracowanie nowych systemów, oraz w zakresie porównania celów postawionych dla nowych systemów z celami osiągniętymi po zainstalowaniu tych systemów.

Środki kontroli planowania

1. Czy przestrzegana jest polityka Systemów Zarządzania przedsiębiorstwa w zakresie planowania?
2. Czy istnieje dokumentacja długookresowych planów systemów zarządzania?
3. Czy istnieją konsekwentne metody oceny kosztu dla proponowanych systemów?
4. Czy dla proponowanych systemów załączono ocenę w kategoriach odmiennych metod lub systemów?
5. Czy w proponowanym systemie przedstawiono koszty wynikające ze stosowania obecnych metod?
6. Czy w proponowanym systemie załączono ocenę i zatwierdzenie ze strony kierownictwa? /Dołącz dowody/.
7. Czy w proponowanym systemie przewidziano wynikowe porównanie oszacowanych i aktualnych kosztów i celów? /Czy przekroczenie kosztów i nieosiągnięcie celów mają być przedmiotem przeglądu i zatwierdzenia ze strony kierownictwa?/.
8. Czy w proponowanym systemie może zachodzić współwymienność oraz możność stosowania w innych wydziałach?
9. Czy system pomaga w samoocenie? Jeśli tak, należy to pokrótce opisać.

10. Czy w obszarze Systemu Zarządzania istnieje system upoważnień dla różnych poziomów wydatków?

11. Czy proponowany system jest udokumentowany /posiada dokumentację/ zanim przystąpi się do programowania oraz czy dokonano jego przeglądu wspólnie z użytkownikiem, by się upewnić, że są zaspokajane potrzeby użytkownika?

Środki kontroli opracowania

1. Czy etykiety, względnie znaczniki programowania w języku symbolicznym są znormalizowane?

2. Czy wszystkie raporty wytwarzane przez system są rzeczywiście wykorzystywane oraz czy korzyści są współmierne do kosztu przygotowania? Czy jednostka operacyjna wie ile może kosztować opracowanie i generowanie na maszynie proponowanego raportu?

3. Czy zwiększone ilości danych mogą być obsłużone przez proponowany system bez proporcjonalnego wzrostu kosztu?

4. Czy podstawowe rodzaje dokumentów wejściowych są znormalizowane i ograniczone tak, aby ułatwić kontrolę i wydajność przetwarzania?

5. Czy w Systemach Zarządzania używa się właściwych procedur kontroli jakości, by przetestować nowe programy przed konwersją?

B. Środki kontroli konserwacji

Obejmują środki upewnienia się, że wszystkie konieczne zmiany w istniejących systemach są przetestowane, udokumentowane oraz zakomunikowane wszystkim zainteresowanym organizacjom.

1. Czy istnieje formalny system upoważniania dla dokonywania zmian w programach? Czy zmiany są zatwierdzane przez osoby inne niż programiści bezpośrednio zaangażowani w dokonywaniu zmian?

2. Czy rzadko dokonuje się większych zmian w ustanowionych systemach i procedurach?

3. Czy zmiany w programach są udokumentowane w zakresie przyczyn zmiany oraz jej wpływu na inspekcję? /Zmiany w bazach danych mogą powodować stratę nie dających się zastąpić danych i powinny być ściśle kontrolowane/.

4. Czy zmiany w bazie danych są udokumentowane w zakresie jej zawartości w poprzednim okresie? /Przykład: reorganizacja może dać w wyniku tę samą nazwę pozycji w raporcie, zawierającej wielkości odmienne od pierwotnych/.

5. Czy zmiany w programie są udokumentowane w zakresie dotyczącym zawiadomienia wszystkich zainteresowanych obszarów?

6. Czy po zmianie w programie zachowuje się zarówno starą jak i nową wersję dokumentacji?

7. Czy zmiany w tabelach wartości danego programu oraz w innych stałych inicjowane są na piśmie przez osoby upoważnione, aby dokonać zmian oraz, czy te zmiany są zapisane w dokumentacji i zachowane dla celów inspekcji?

8. Czy programy są testowane po zmianie? Kto spełnia funkcję kontrolera jakości?

C. Środki kontroli konwersji

Czy w procesie instalacji nowego systemu podjęto kroki w zakresie sprawdzenia warunku, że nastąpiło prawidłowe przekształcenie /przejście na nowy system/ oraz że wszystkie wątpliwe pozycje, napotkane w czasie tego procesu, są przebadane i rozstrzygnięte?

1. Czy wszystkie nowe systemy i programy /włączając tu ważniejsze nowe wersje/ są zatwierdzane przez kierownictwo i aprobowane przez użytkowników przed ich wykorzystaniem?

2. Czy ustalone jest postępowanie, które ma zapewnić, że przejście /na nowy system/ jest prawidłowe i równoległe?

3. Czy w stosunku do danych podlegających konwersji mają zastosowanie dodatkowe procedury redagowania, niezależnie od zwykłych programowanych procedur redagowania? /Omówione w podliście II niniejszej listy kontrolnej/.

4. Czy użytkownik dokonuje testowania i inspekcji w czasie konwersji i po konwersji?

5. Czy użytkownicy rozumieją przed przejściem jak korzystać z systemu?

6. Czy, gdy następują poślizgi w przejściu, dokumentuje się przyczyny poślizgów?

7. Czy potencjalni użytkownicy nowych systemów są zadowoleni z planowanego zakresu i procedur?

D. Dokumentacja

Kontroluje ona ciągłość operacji i zapewnia punkt odniesienia, który może zmniejszyć błędy powstałe na tle braku zrozumienia. Przez dobrą dokumentację można także w przyszłości uniknąć kosztów przy dokonywaniu zmian; /tak więc należy zbilansować koszty dokumentacji z uzyskiwanymi korzyściami/.

1. Czy procedury dla działań Systemu Zarządzania zostały zestawione w podręczniku operacyjnym i czy ten podręcznik jest aktualny?

2. Czy istnieje podręcznik programowania, który opisuje normy programowania i procedury dla dokumentacji programowania i procedury dla dokumentacji programów, testowania programów, zachowania danych i zmian w programach?

3. Czy dokumentacja systemu komputerowego jest właściwa? Należy uwzględnić:

   . dokumentację użytkownika,

   . dokumentację konserwacji systemu,

   . dokumentację operacyjną systemu,

   . zbiorową dokumentację dla całego przedsiębiorstwa.

4. Czy procedury sporządzania schematów blokowych wyższego szczebla /flowchart/ dla systemów są w swych podstawowych elementach znormalizowane? Czy dla wszystkich systemów i programów istnieją schematy wyższego szczebla?

5. Czy istnieją normy i spisane procedury dla przeprowadzania przeglądów systemów danych i badania systemów danych?

6. Czy procedury testowania programów i ich wyników dla systemu są prawidłowo ustanowione oraz czy są napisane dla każdego systemu?

7. Czy utrzymuje się na minimalnym poziomie wykorzystanie przełączników zewnętrznych lub parametrów wejściowych Języka Sterującego Pracą w programach oraz czy instrukcje dla ich użycia są sporządzone na piśmie?

8. Czy istnieje udokumentowany plan przechowywania danych, który specyfikuje okres przechowywania oraz rekonstrukcję zbiorów na nośnikach maszynowych w wypadku nieumyślnego zniszczenia zbiorów?

9. Czy istnieje dokumentacja obejmująca poczynania w zakresie bezpieczeństwa i ochrony przeciwpożarowej dla głównych kopii programów i zbiorów danych? /Może być pożądane posiadanie zapasowych danych o ograniczonym dostępie dla "czyszczenia" lub "strojenia" środków zabezpieczenia/. Należy rozważyć zapasową pamięć dla danych oraz procedury awaryjne na przypadek przedłużającego się przestroju maszyny.

10. Czy istnieje udokumentowana procedura zapewnienia jakości dla kontrolowania dokładności i niezawodności operacji całego systemu?

V. ŚRODKI KONTROLI PROCEDURALNEJ W PRZETWARZANIU DANYCH

Są to metody używane w wydziałach Przetwarzania Danych w celu kontroli danych wejściowych, danych historycznych, programów, sprzętu, środowiska fizycznego oraz bezpieczeństwa danych.

A. Środki kontroli w ramach Funkcji Kontroli Danych

Są to metody, mające na celu zapewnienie, aby wszelkie zaopatrzenie oraz programy zastosowań były dostarczone do sali komputera dla przetwarzania oraz by wszystkie wyniki

wyjściowe z komputera osiągnęły właściwe przeznaczenie. W tych technikach zabezpieczenia są zawarte procedury dla nadzoru prawidłowości oraz terminowości omawianego przetwarzania informacji.

1. Czy są zapewnione właściwe procedury dla zamawiania formularzy związanych z komputerem, taśm, pakietów dyskowych itd.? Należy rozważyć cenę i ilość.
2. Czy istnieje dostateczna kontrola nad przedkładaniem prac, sprawdzaniem i rozdziałem wyjścia?
3. Czy w tej jednostce wykonuje się jakiekolwiek techniki zabezpieczenia nad przemieszczaniem i konwersją danych?
4. Czy zwykle dotrzymuje się zaplanowanych terminów?
5. Czy są ustanowione procedury dla kontroli korekcji niewłaściwych danych wykrytych w Jednostce Kontroli Danych?
6. Czy istnieją procedury powiadamiania ludzi opracowujących systemy o problemach w programach? Jakie są to procedury?
7. Czy użytkownicy usług komputerowych są zadowoleni z tych usług?

Czy istnieją ilościowe kryteria usług lub zadań produkcyjnych?

Rozważmy na przykład:

Miary wydajności dla operacji na komputerze

Zorientowane na klienta /użytkownika/

- Czas całkowity usługi - procentowo według kategorii prac
- Czas niemożności otrzymania odpowiedzi - licząc tygodniowo /dla terminali - przyp.tłum./
- Procent dotrzymanych terminów dla przetwarzania prac działalności przemysłowo-handlowej
- Niedotrzymane zaplanowane terminy
- Zażalenia licząc tygodniowo
- Powtórne przebiegi jako procent wszystkich prac

Zorientowane na sprzęt i oprogramowanie

- Procentnie wykonanej zaplanowanej konserwacji zapobiegawczej
- Awarie sprzętu licząc tygodniowo /według rodzaju/
- Czas wyłączenia Centralnego Procesora żądany przez dostawcę sprzętu
- Czas włączenia CP, licząc w godz/dobę
- Godziny nadliczbowe jako procent czasu włączenia CP
- Godziny płatne z zewnątrz, licząc dziennie jako procent czasu włączenia CP
- Czas przestoju terminali/urządzeń zewnętrznych /według rodzaju/
- Czas roboczy jako procent czasu włączenia CP
- Czas przebiegów dla potrzeb metody porównawczej /Benchmark deck run time/
- Koszt przebiegów dla potrzeb metody porównawczej
- Wykryte błędy oprogramowania, licząc na miesiąc
- Błędy nieustalone
- Błędy naprawione, licząc miesięcznie

Zorientowane na ludzi z przetwarzania danych

- Liczba przekazywanych prac /obrót/
- Żądane godziny pracy
- Miary określenia grup prac

Zorientowane na koszt usług

Koszt na jednostkę obliczeń podzielony przez czas całkowitej usługi ważony czasem przebiegu itp.

B. Środki kontroli operacji na komputerze

Są to techniki, mające na celu zmniejszenie możliwości błędów operatora, nieupoważnionej interwencji lub innych zdarzeń, które mogą narazić na szwank nienaruszalność informacji w komputerze.

1. Czy instrukcje operatorskie są ujęte na piśmie i rozumiane właściwie? Rozważmy następujące punkty:
   - czy uwzględniają one sytuacje, w których dane można wprowadzać poprzez konsolę?

- czy zawierają jasno określone instrukcje dla każdej osoby?
- czy zawierają one procedury na wypadek wystąpienia błędu lub innych trudności w przetwarzaniu?

2. Czy zachowuje się i przegląda wydruki z konsoli, by wykryć interwencje operatora lub inne przerwy w przetwaniu lub wprowadzenie informacji do komputera poprzez konsolę?

   Należy rozważyć takie pozycje jak:

   - czy wydruki zawierają wszystkie komunikaty dla i od operatora?
   - czy wydruki zawierają cechy identyfikujące przetwarzanego w danym momencie programu?
   - czy wydruki są przeglądane przez osobę zaznajomioną z wykonywaną działalnością?

3. Czy jest wystarczająco kontrolowany czas pracy komputera?

   Rozważ:

   - czy wykorzystanie komputera jest zapisywane przez program, jeśli chodzi o czas przebiegu, czas ustawiania oraz nie wykorzystanie /konserwacja i czas wyłączenia/?
   - czy wykorzystanie komputera jest analizowane periodycznie przez odpowiedzialnych ludzi z eksploatacji?
   - czy rejestruje się dla każdej maszyny uwagi dotyczące wydajności i dokładności oraz czy jest podejmowana dostateczna akcja korekcyjna w przypadkach kiepskiej wydajności?
   - czy operatorzy prowadzą raporty rejestrujące trudności lub inne rejestry?
   - czy dla każdej pracy na komputerze podaje się maksymalne czasy przebiegu /jako parametr Języka Sterowania Pracą JCL/?

4. Czy istnieją techniki kontrolne dla zapewnienia uniezależnienia się od operatora?

Należy rozważyć następujące przypadki:

- czy programy są prowadzone przez wszystkich operatorów w przeciwieństwie do prowadzenia pewnych prac stale przez pewnych operatorów?
- czy operatorzy są świadomi ryzyka, jakie ponoszą przy przyjmowaniu specjalnych ustnych instrukcji od programistów zastosowań?
- czy pracownicy systemowi i programiści są poinstruowani, by nie obsługiwać komputera lub by nie zmieniać wejść i nie inicjować regularnych przebiegów przetwarzania, które są potencjalnie przedmiotem sprzeniewierzeń - płace itp.?
- czy operatorzy komputera nie mają dostępu do dokumentacji programów?

C. Biblioteka na maszynowych nośnikach

Techniki zabezpieczenia w tej dziedzinie zapewniają, by zbiory danych były prawidłowo identyfikowane, zachowywane tak długo jak to jest potrzebne oraz zabezpieczone przed zagrożeniem fizycznym i przed nieupoważnionym dostępem.

1. Czy zbiory są przechowywane stosownie do zaleceń producenta?
2. Czy zatwierdzone kopie wszystkich programów komputera oraz koniecznych dokumentów pomocniczych przechowywane są w bibliotece i wydawane zainteresowanym osobom tylko za upoważnieniem?
3. Czy istnieją procedury dla zabezpieczenia zapasowych kopii wszystkich krytycznych zbiorów w systemie? Rozważyć zapasowe dane w wypadku błędu We/Wy, fizycznego zniszczenia biblioteki itp.
4. Czy istnieją procedury i fizyczne techniki zabezpieczenia w celu ochrony przed nieumyślnym wymazaniem zbiorów?

5. Czy ustalono politykę /linię postępowania/ dla kasacji krążków taśmy i pakietów dyskowych w wypadku występowania nadmiernych błędów zapisu, względnie odczytu?

6. Czy jest dostępna informacja potrzebna do umiejscowienia każdego podanego zbioru danych lub jednostki przechowywania zbioru fizycznego?

7. Czy prowadzi się rozliczenia w zakresie własności przedsiębiorstwa, takiej jak taśmy magnetyczne i pakiety dyskowe?

D. Środki kontroli w zakresie bezpieczeństwa

Zapobiegają przed nieupoważnionym dostępem do informacji. Te techniki zabezpieczenia powinny szczególnie chronić informacje zakwalifikowane przez Departament Obrony i przez przedsiębiorstwo jako tajne, oraz inne dane o charakterze delikatnym lub prawnie zastrzeżonym.

1. Czy informacje utajnione przez przedsiębiorstwo oraz przez rząd mają zapewnioną właściwą ochronę?

2. Czy istnieją jakiekolwiek dane zastrzeżone prawnie? Jeśli tak, to jakie podjęto środki ostrożności w zakresie ich zabezpieczenia?

3. Czy przedyskutowano zabezpieczenie danych przedsiębiorstwa z odpowiednimi pracownikami lub zleceniobiorcami? Należy sporządzić listę wszystkich pracowników, którzy byli zapytywani w tej sprawie, podając ich odpowiedź.

4. Czy są pracownicy, którzy byli przyjęci za kaucją?

5. Czy dla wszystkich nowych pracowników sprawdza się referencje?

6. Czy do poniżej podanych obszarów dostęp jest ograniczony w celu ochrony przed nieupoważnioną sposobnością przejrzenia, ukradzenia lub zmiany danych lub systemów i czy narażenie fizyczne jest minimalne?
   a. Jednostka operacyjna
   b. Jednostka kontroli danych
   c. Jednostka dziurkowania
   d. Sala komputera

e. Obszar przechowywania danych na nośnikach maszynowych

f. Miejsca tymczasowego przechowywania, gdy dane są przesyłane z jednego miejsca do drugiego.

7. Jakie istnieje narażenie przedsiębiorstwa, jeśli idzie o oszustwo lub sabotaż jako wynik procedur systemu?

8. Jaką ochronę posiada przedsiębiorstwo w formie ubezpieczenia w dziedzinie przetwarzania danych?

E. Środki kontroli sprzętu

Techniki zabezpieczenia mające zapewnić, by sprzęt wpływający na koszty był dostępny, gdy zajdzie tego potrzeba.

1. Czy spełnione są wskazane przez producenta wymagania w zakresie temperatury i wilgotności?

2. Czy istnieje ustalony i właściwy plan konserwacji zapobiegawczej i czy jest on realizowany?

3. Czy poczyniono odpowiednie przygotowania w zakresie wypożyczenia, względnie zapasowego sprzętu na wypadek przeciągającego się uszkodzenia maszyny?

4. Czy przeciętny miesięczny czas przestoju spowodowany nieplanowaną konserwacją jest dopuszczalny /awarie maszyny/? Zależy to od czasu usługowego koniecznego dla użytkowników sprzętu.

5. Czy istnieje ustalona spisana instrukcja lub zasady postępowania odnośnie odwiedzania ośrodka, palenia, jedzenia, picia itd. w sali komputera?

6. Kto w przedsiębiorstwie jest bezpośrednio odpowiedzialny za sprzęt?

7. Czy sprzęt jest opłacalny?/Czyli efektywny ekonomicznie/.

Należy rozważyć takie rzeczy jak:

a/ czy użytkowanie sprzętu jest planowane?

b/ czy odchylenia od planu /harmonogramu/ są dobrze udokumentowane i usprawiedliwione?

c/ czy sprzęt wydaje się wystarczający dla potrzeb systemu i czy jest dobrze wyważony?

d/ czy badano kosztorysy przed zakupem lub dzierżawą? /Należy dołączyć kopię uzasadnienia kosztów/,

e/ jakie jest wykorzystanie sprzętu?

f/ czy uzgodniono zestawienie kosztów sprzętu z inwentarzem sprzętu? /Należy dołączyć kopię/,

g/ czy porównuje się obciążenia amortyzacją i podział wykorzystywania?

F. Środki kontroli w zakresie BHP

Czy pracownicy przedsiębiorstwa oraz zleceniobiorców są zabezpieczeni przed przypadkowym zranieniem; jak dalece da się to przewidzieć?

BIBLIOGRAFIA

1. The Control and Audit of Electronic Data Processing Systems, American Management Association, New York, 1965

2. Davis, Gordon B., Auditing & EDP, American Institute of Certified Public Accountants, Inc., New York, 1968

3. The Diebold Research Program, Financial Activity and Information Processing E35, The Diebold Group, Inc., May 1967

4. The Diebold Research Program. Turnover Among ADP Personnel E54, The Diebold Group, Inc., December 1968

5. Internal Auditing of Electronic Data Processing Systems, The Institute of Internal Auditors, Inc., New York, 1967

6. The Internal Auditor, Journal of the Institute of Auditors, New York, selected articles:

   Lundgren, G.E., "Management Considerations for EDP, Audits, and Control", Fall 1966
   Graham, K., "Internal Control Problems Arising from EDP", Fall 1966
   Raymond, R.H., "The Impact of EDP on Auditing", January/February 1968
   Diamond, T.D. and Krallinger, J.C., "Controls and Audit Trails for Real-Time Systems", November/December 1968
   Porter, F.J., "What the EDP Executive Expects of the Internal Auditor", November/December 1968
   Nigra, A.L., "Statistical Sampling with EDP Equipment", March/April 1969
   Moloney, R.F., "A Computer Instruction Program for the Internal Auditor", March/April 1969
   Thomason, F.J., "Management Controls in EDP", March/April 1969
   Moore, M.R., "EDP Audits: A Systems Approach", May/June 1969

Carmichael, D.R., "Fraud in EDP Systems", May/June 1969
Pauley, C.A., "Audit Responsibilities in the Design of Computerized Systems", July/August 1969
Sheffield, R.J., "EDP Audit Techniques", November/December 1969
Shelton, L.B. and Reid, E.W., "Unauthorized Intervention in Computer Processing", November/December 1969
Tagen, W.G., "Educating the Internal Auditor in EDP", January/February 1970

7. International Business Machines Corporation, The Considerations of Data Security in a Computer Environment, publication 520-2169-0, 1969

8. Ross, Franz E., "Internal Control and Audit of Real Time Digital Systems", The Journal of Accountancy, April 1965, p.49

9. Standards for the Protection of Electronic Computer Systems, Bulletin No. 75, National Fire Protection Association, Boston, 1964

10. Wasserman, Joseph J., "Plugging the Leaks in Computer Security", Harvard Business Review, September-October 1969

11. Weiss, Harold, "The Danger of Total Corporate Amnesia", Financial Executive, June 1969

Cena zł 92.-