K O M U N I K A T Y

na kursokonferencję

"ZAPEWNIENIE UŻYTKOWNIKOM POUFNOSCI INFORMACJI W PROCESIE ELEKTRONICZNEGO PRZETWARZANIA DANYCH"

Warszawa 1978

Mgr Waldemar Wiśniewski
Z-ca Dyrektora d/s Eksploatacji
w Centrum Obliczeniowym MPM

Komunikat

Czy kanony estetyki muszą zagrażać zabezpieczaniu informacji w ośrodkach informatyki?

Pracownicy ośrodków obliczeniowych bez względu na ich miejsce /stanowisko/ pracy częstokroć stwierdzają:

> "czemu aż tak poważnie mamy martwić się o informacje, z którymi mamy doczynienia?, są to przecież sprawy właściciela/użytkownika tych informacji".

Istnieją również poglądy, że programy są niezrozumiałe dla większości osób, jak również że informacje w takiej postaci w jakiej dostarczane są do przetwarzania nie są interesujące dla otoczenia poza ich dawcą lub imiennym adresatem. Są to oczywiście poglądy conajmniej staroświeckie, z którymi należy nie tyle polemizować co zdecydowanie zwalczać je.

Jak dotąd w Polsce zagadnieniem zabezpieczenia informacji, a w szczególności informacji znajdujących się w masowych ilościach w ośrodkach obliczeniowych /bez względu na ich lokalizację i podporządkowanie/ nie poświęca się takiej uwagi na jaką zasługują. A wiadomym jest, że wszędzie tam gdzie realizowana jest działalność gospodarcza bądź prowadzona jej analiza istnieje prawdopodobieństwo zaistnienia działalności niezgodnej z prawem. Działalności wynikającej ze złej woli, niedbalstwa lub nierozmyślnie popełnionych błędów.

Odnosi się to szczególnie do ośrodków obliczeniowych gdzie "efekty" tych działań mogą być szczególnie dotkliwe w skutkach a jednocześnie niezmiernie trudne do ujawnienia.

W komunikacie tym pragnę poruszyć problem nie tyle ochrony informacji podczas całego procesu przetwarzania lub ochrony poszczególnych zbiorów. Ponieważ proces ochrony informacji bądź proces jej przetwarzania jest prawie analogiczny we wszystkich

ośrodkach obliczeniowych i jest generalnie rzecz ujmując procesem szeregowym.

Dla mnie istotnym jest inny element wpływający na zabezpieczenie, nazwijmy je fizyczne. W aspekcie fizycznym ośrodki obliczeniowe można podzielić na:

- ośrodki samodzielne, zlokalizowane w wydzielonych, wolno stojących obiektach,
- ośrodki zależne, zlokalizowane w obiektach zagospodarowanych przez więcej niż jednego użytkownika.

I tu bez względu na w/w podział, bądź jak kto woli lokalizację rysują się zbliżone problemy natury nazwijmy je architektoniczno-estetycznej.
A więc np.:

- Wejście do obiektu. Ośrodek obliczeniowy jest nośnikiem postępu i równocześnie w pojęciu osób nie zajmujących się zebezpieczeniem powinien więc również i zewnętrznie wyróżniać się nowoczesną formą rozwiązań architektonicznych. Wyposażymy go więc w maksymalnie duże okna, oczywiście poza kruchym szkłem niczym innym nie zabezpieczone. Ponieważ ich okratowanie kłóci się z pojęciem estetyki, a zabezpieczenie instalacją elektroniczno-alarmową jest albo zbyt drogie albo też wydaje się przesadną ostrożnością. Wyposażamy również ten obiekt w odpowiedno reprezentacyjne, duże dwuskrzydłowe drzwi, maksymalnie przeszklone, najlepiej o delikatnej konstrukcji aluminiowej. Ale do tego instalujemy kilka specjalnych zamków, czasami z kombinacjami liczbowymi. Za tymi drzwiami spotykamy często portiera. zajętego z reguły przeglądaniem ilustrowanych czasopism.
Są również jedne lub dwoje drzwi ewakuacyjnych o równie wątłej konstrukcji, co drzwi główne ale za to już nie strzeżonych przez nikogo a tylko zamkniętych. Ale zgodnie z wymaganiami ppoż. i bhp przy drzwiach tych znajduje się w przeszklonej szafce zamkniętej symbolicznie bądź tylko "okapslowanej" plasteliną tzw. klucz awaryjny.
Sam widziałem, zresztą nie tylko w kraju przy zamkach cyfrowych zamykających drzwi wewnętrzne do pomieszczeń szczególnie chronionych nabazgrany flamastrem /dla trwałości napisu/ numer kodu

otwierający dostęp do tych chronionych stref. Używano to dla wygody zapominalskich spośród personelu. Jakże łatwo dostać się do takiego obiektu a szczególnie wówczas gdy jeszcze na dodatek kolejny esteta występujący w procesie projektowania życzył sobie aby obiekt otoczony był bogatą o różnej wysokości zielenią.

To w przypadku obiektu wolnostojącego. A co dzieje się jeżeli w budynku poza ośrodkiem obliczeniowym znajduje się jeszcze jedna czy więcej instytucji.
Wówczas w zależności od rangi tych instytucji oraz lokalizacji budynku również występują drzwi główne oraz co najmniej jedno wejście tzw.boczne.
Z zasady w godzinach rozpoczynania pracy drzwi otwarte są na całą szerokość. Strażnicy /jeżeli są/ wówczas w ogóle nikogo nie sprawdzają, każdy się spieszy zasiąść za swoim biurkiem. Jakże łatwo wejść wówczas do owych "strzeżonych" obiektów.

Sprawa okien w tych "twierdzach".
Ponieważ są to obiekty zlokalizowane przy ulicach oczywiście zgodnie z kanonami estetyki nie mogą być okratowane. Ba, mało tego ponieważ są to również okna duże a więc przynajmniej w 90% wypaczone i niedomykające się.

W jednym z miast wojewódzkich widziałem taki wspaniały paro piętrowy obiekt z odpowiednio dużym dziedzińcem, na którym wybudowano estetyczny z ażurowej cegły śmietnik zlokalizowany pod oknami pomieszczeń sanitarnych. Zadaszenie śmietnika było tylko 50 cm, niższe od parapetu okna WC. Wchodząc do ośrodka obliczeniowego dostałem przepustkę, do której z dowodu osobistego portier pracowicie wpisał moje dane. Załatwiłem sprawę, poszedłem do WC, wyjżałem przez stale uchylone okno, wyszedłem przez nie na dach śmietnika dalej zeskoczyłem na ziemię, porozmawiałem z kierowcami, którzy stali przy swoich służbowych samochodach i co, ano nic. Przepustki nie oddałem, choć była numerowana i jej część grzbietowa również pracowicie wypełniona moimi danymi personalnymi pozostała w tym ośrodku. Minął już ponad rok i dotychczas nikt się o nią nie upomniał.

Tak przykładowo wygląda ochrona naszych ośrodków obliczeniowych.

Wniosek: Koniecznym jest w trybie nadzwyczaj pilnym w porozumieniu z odpowiednimi organizacjami służb budowlano-architektonicznych opracowanie odpowiednich wytycznych do projektowania zapezbieczania ośrodków obliczeniowych. Niezbędnym jest również częstsze niż dotąd organizowanie:

- konferencji, jak nasza dzisiejsza,
- szkoleń dla służb ochrony, pracowników i kierownictw ośrodków obliczeniowych.

mgr Jerzy Knast
Centrum Informatyki
Gospodarki Morskiej
Gdynia

ZABEZPIECZENIE DANYCH W SYSTEMIE PRACUJACYM W TRYBIE ON-LINE

1. Dynamiczny rozwój informatyki w ostatnim okresie w Polsce wpłynął na wzrost zainteresowania oraz wymagań użytkowników odnośnie stosowania nowoczesnych technik przetwarzania. Szybszy obieg informacji oraz związany z nim zwiększony przepływ danych spowodował między innymi konieczność stosowania w projektowaniu i przetwarzaniu systemów technik odpowiednich dla pracy w czasie rzeczywistym.
Wychodząc naprzeciw potrzebom PLO, w Centrum Informatyki Gospodarki Morskiej w Gdyni został zaprojektowany i oprogramowany System Ewidencji i Kontroli Ruchu Kontenerów - ASERK. U podstaw decyzji o tym, aby system pracował w trybie ON-LINE była m.in. konieczność dostosowania się do wymogów szybkiego i bieżącego kontrolowania stanów i zasobów głównego podmiotu działalności - tj. kontenerów, a w szczególności:
   - bezpośredni i operatywny charakter rejestrowanych danych służących do wydawania szybkich dyspozycji;
   - rozproszenie terytorialne i duża niezależność użytkowników /Zakładów Liniowych PLO/;
   - znaczna liczebność i różnorodność parku kontenerowego;
   - duży obszar geograficzny, który objęty jest sferą działalności PLO;
   - konieczność zapewnienia wysokiego poziomu obsługi klientów.

   Chodziło więc m.in. o uzyskiwanie szeregu informacji i dokumentów charakteryzujących:
   - bieżące rozlokowanie poszczególnych kontenerów;
   - sprawność i gotowość eksploatacyjna kontenerów;
   - stan i zaangażowanie kontenerów, np. gotowe do załadunku na statek, przemieszczenia w transporcie lądowym, uszkodzone w naprawie, na depot itp.

Zakres oraz różnorodność funkcji realizowanych przez system zrodził potrzebę organizacji pracy która zapewniałaby:

- stałe oraz szybkie wprowadzanie informacji;
- automatyczną sygnalizację odchyleń od założonych stanów;
- bieżącą kontrolę zaawansowania pracy na poszczególnych terminałach/monitorach;
- możliwość łatwego odtworzenia informacji przechowywanych w zbiorach;
- płynną i nieprzerwaną pracę systemu.

System ASERK bazuje na następującym sprzęcie:

- jednostka centralna ODRA 1305 z pamięcią 128 k;
- pamięć na dyskach magnetycznych 60 mln zn.;
- procesor komunikacyjny ICL 7903;
- sieć linii transmisyjnych do użytkowników;
- 7 terminali zainstalowanych w Zakładach Liniowych PLO /5 w Gdyni, 2 w Szczecinie/.

Przez terminal/monitor umożliwiający bezpośredni dostęp do komputera ODRA 1305 zainstalowanego w CIGM Gdyni rozumie się monitor ekranowy ICL 7181/2 oraz dalekopis spełniający funkcję drukarki zestawień sporządzanych na żądanie /hard copy/.

2. Stosowanie systemów transakcyjnych*/ pracujących w czasie rzeczywistym stwarza zupełnie nowe warunki pracy oraz problemy technologiczne w porównaniu z systemami przetwarzanymi tradycyjnie /batch/.

W każdym systemie ON-LINE sprawy:

1. zabezpieczenia przed dostępem do zbiorów,
2. kontroli systemu z punktu widzenia rzetelności i prawidłowości pracy operatorów /użytkowników/,
3. zabezpieczenia poprawności i aktualności danych dla celów restartu i statystyk,

---

*/ Transakcja - pojęcie s. ON-LINE, oznacza pewien komplet komunikatów wejściowych i wyjściowych dotyczących tego samego żądania operatora terminala /np. żądanie podania określonej informacji lub wprowadzenie do zbioru informacji z danego dokumentu/.

są ze sobą nierozerwalnie związane i wzajemnie uwarunkowane. Aby system kontenerowy - ASERK mógł sprostać w/w zadaniom został opracowany specjalny system Zabezpieczeń i Restartu, który został włączony do s. ASERK stanowiąc obecnie jego integralną całość.

Jakkolwiek s. Zabezpieczeń i Restartu zabezpiecza odpowiednie działania w każdej z trzech powyższych dziedzin, to jednak jego zakres, przydatność i wykorzystanie zależy w dużej mierze od wymagań i potrzeb użytkowników.

W systemie Z i R wydzielono trzy czynniki, które mogą powodować nieprawidłowości w pracy systemu, przechowywaniu i przetwarzaniu danych:

- awarie hardware /sprzęt, urządzenia/,
- awarie software /programy, pakiety standardowe/,
- czynnik ludzki /obsługa w ośrodku obliczeniowym, użytkownicy/.

Obsługa sprzętu komputerowego oraz programów i zbiorów w zakresie zabezpieczenia prawidłowości działania /serwis techniczny, odpowiednia gospodarka zbiorami systemowymi, przeszkolony personel operatorski/ jest określona i wyznaczona odrębnie w każdym ośrodku obliczeniowym.

3. W systemie ASERK - z wbudowanym systemem Zabezpieczeń i Restartu - duży nacisk położono na zabezpieczenie przez ewentualnymi błędami w operowaniu oraz awariami, które mogą być spowodowane działaniem operatorów /użytkowników/.

Prace z zakresu legalności i prawidłowości w dostępie do zbiorów, zabezpieczenia danych, ochrony zbiorów i wyników w czasie przetwarzania systemu są realizowane poprzez:

1. sprawdzanie legalności podejmowania określonych czynności,
2. ograniczanie zakresu prac realizowanych przez poszczególnych operatorów,
3. prowadzenie rejestracji prac /transakcji/ realizowanych przez użytkowników,
4. analizę danych wyjściowych otrzymywanych z obliczeń,
5. ochrony bibliotek zbiorów /systemowe, transakcyjne - archiwalne/.

Ad. 1. Każda osoba spełniająca funkcję operatora monitora /VDU/ może przyłączyć się do systemu znając odpowiednie hasło. Dla każdego operatora VDU /w każdym Zakładzie użytkownika/ może być inne hasło wprowadzające. Wydzielony /jeden/ terminal posiada kompetencję zmiany haseł przypisanych poszczególnym zakładom PLO. Hasło uzupełnione jest kodem systemu obligatoryjnie wprowadzonym przez operatora i sprawdzonym przez system.

Ad. 2. Ograniczenia w pracy użytkowników mogą być prowadzone na trzech kierunkach działania systemu:
- wyznaczenie limitu czasu pracy,
- ograniczenie kompetencji dostępu do informacji przetwarzanych przez innych użytkowników /operatorów/,
- blokada łączności komputera z wybranymi terminalami.

Na polecenie osoby odpowiedzialnej za pracę systemu w Ośrodku Obliczeniowym /u użytkownika/ istnieje możliwość wyznaczenia /zmiennego/ limitu czasu, po upływie którego żadna nowa praca /transakcja/ nie będzie mogła być rozpoczęta. Umożliwia się tu jedynie dokończenie bieżąco realizowanych prac.

Od początku pracy systemu ASERK - s. eksploatowany jest od grudnia 1977 r. - zgodnie z zaleceniami użytkownika, wprowadzono ograniczenia w dostępie do informacji między poszczególnymi zakładami. Znaczna część informacji systemu kontenerowego podzielona jest /logicznie/ między użytkowników /zakłady/, którzy posiadają kompetencje w dostępie i przetwarzaniu przydzielonych im /w danej chwili/ danych. Istnieje wreszcie możliwość zawieszenia pracy bieżąco wykonywanej przez określonego użytkownika /operatora/ poprzez zablokowanie wszelkiej komunikacji hardware na linii VDU - ODRA 1305 oraz sprawdzenie i ewentualne anulowanie jego bieżącej transakcji.

Ad. 3. W celu sprawdzenia i kontroli informacji wprowadzanych do systemu z punktu widzenia ich rzetelności i kompletności system Z i R rejestruje na bieżąco dane o pracy operatorów. Zapis - do osobnego zbioru transakcyjnego-identyfikatorów użytkownika: adres /Nr VDU/,

czas i kod transakcji, zawartość zbiorów /rekordów/ przed i po realizacji transakcji - dokonywany jest w sposób ciągły w czasie sesji ON-LINE systemu. Dane te traktowane są ponadto jako wejściowe dla modułu RESTARTU, który uruchamiany jest w sytuacjach błędnych zapisów do zbiorów lub awarii sprzętu, a więc przerw w pracy systemu.

Ad. 4. Rejestracja id. użytkownika i transakcji dokonywane jest na oddzielnym nośniku - taśmie magnetycznej - tworząc zbiór transakcyjny LOG-MT.
W celu przeprowadzenia analiz przekrojowych można /bez przerywania bieżącej pracy systemu/ otrzymać z LOG-MT zestawienia i raporty ujmujące syntetycznie dane o typach, rodzajach i czasie transakcji realizowanych przez poszczególnych operatorów w ciągu dnia. Ponadto można uzyskać szczegółowy wykaz zmian dokonanych w zbiorach systemowych w określonym przedziale czasu /zmiana, godzina/.

Ad. 5. Prowadzenie kontroli zbiorów archiwalnych w zakresie przechowywania, wydawania do przetwarzania oraz kasowania uregulowane jest szczegółowymi instrukcjami i zaleceniami. W szczególności łączy się to z:
- prowadzeniem kartoteki osobowej dla każdej nowopowstałej taśmy /w danym dniu może powstać kilka taśm/,
- wydawaniem właściwych taśm dla celów sprawdzania czy Restartu,
- zabezpieczeniem /nazwa, czas powstania GG/MM/SS/ taśm przed przedwczesnym zniszczeniem /kasowaniem/.

K o m u n i k a t

na Kursokonferencję nt. "Zapewnienie poufności informacji w procesie przetwarzania danych".

W Resortowym Centrum Obliczeniowym Ośrodka Ekonomiki i Organizacji Przemysłu Lekkiego EKORNO w Łodzi opracowany został system RESTABU, zapewniający poufność zbiorów pośrednich resortowego systemu informatycznego dla kierownictwa MPL-RESIL.

Wchodzące w skład RESILu podsystemy dziedzinowe są obecnie eksploatowane na zestawie komputerowym:

- jednostka centralna ODRA 1305 /pamięć operacyjna 128 K słów/
- 4 jednostki EDS8
- 10 jednostek taśmy magnetycznej
- 2 czytniki kart
- 1 czytnik-dziurkarka taśmy
- 2 drukarki wierszowe.

Planowane jest zainstalowanie w Centrali MPL w Warszawie, terminala 7502, wyposażonego w drukarkę wierszową i monitory ekranowe i dyski elastyczne.

Jako system operacyjny obsługujący system RESIL przyjęty został GEORGE 2.

System RESTABU umożliwia zapis zbiorów pośrednich na taśmach magnetycznych. Taśmy te zaopatrywane są w katalog opisujący zawartość taśmy /zawarte na taśmie podzbiory/, określający hasła dostępu do zbioru i poszczególnych podzbiorów. Głównym zastosowaniem systemu RESTABU jest tworzenie, aktualizacja i zapewnienie poufności zbiorów wyjściowych. Taśmy zawierające zbiory wyjścio-

we tworzą wydzieloną pulę taśm, z których wydruk może odbywać się jedynie przy użyciu specjalnego programu wydruku, sprawdzającego hasła dostępu. Na początku taśmy umieszczone są bloki techniczne, zabezpieczające przed przypadkowym odczytem. System przewiduje również możliwość szyfrowania danych.

System RESTABU dostarcza innych udogodnień, jak np:

- uniezależnienie godzin przetwarzania podsystemów dziedzinowych RESILU od czasu pracy terminala 7502,
- zmniejszenie zapotrzebowania systemu operacyjnego GEORGE 2 na pamięć o bezpośrednim dostępie.
- udostępnienie 160-znakowej drukarki wierszowej programom opracowanym w języku programowym COBOL.

Inne metody i techniki zabezpieczenia i ochrony danych są ponadto objęte pracami prowadzonymi w WIC.KC, w ramach tematu "Metodyka budowy i wdrażania systemu RESIL".

Zastępca Dyrektora
ds. informatyki
mgr Marian Polski

dr PAWEŁ MIJAL
Ośrodek Informatyki
CENTRALA TURYSTYCZNA ORBIS

Warszawa, 3.10.1978 rok

K O M U N I K A T

o stanie prac w zakresie zabezpieczenia danych w Ośrodku Informatyki Centrali Turystycznej O R B I S

Ośrodek Informatyki Centrali Turystycznej ORBIS dysponuje następującym sprzętem komputerowym:

- 2 minikomputery NCR-8200,
- 11 rejestratorów danych ADDO M-10,
- 7 stanowisk do kas walutowych D5/20 DATA SAAB.

Na urządzeniach tych są eksploatowane Systemy:

- rozliczeń grupowej turystyki zagranicznej wyjazdowej,
- rozliczeń zagranicznej turystyki indywidualnej przyjazdowej,
- zautomatyzowanej wymiany walut na stanowiskach kasowych,
- obliczeń statystycznych dla potrzeb CT ORBIS,
- ewidencji i analizy wyników dla PZLA,

W fazie testowania znajdują się systemy:

- bilansowania miejsc noclegowych ,
- gospodarki materiałowej dla gastronomii hotelowej.

We wszystkich Systemach stosowane są:

- organizacyjne,
- sprzętowe,
- programowe

zabezpieczenia procesu przetwarzania danych.

Na zabezpieczenia organizacyjne, jednolite dla całego Ośrodka składają się:

1/ archiwum materiałów magnetycznych, wyposażone w szafę ogniotrwałą do przechowywania dysków i kaset magnetycznych z kopiami programów i zbiorów głównych,
2/ biblioteka kaset magnetycznych, wypożyczonych przez rejestratorki,
3/ biblioteka dysków magnetycznych, pobieranych przez operatorów.

Niestety nie udało się dotychczas uzgodnić ze Strażą Pożarną warunków dodatkowego zamknięcia całego zespołu pomieszczeń komputerowych oraz obsługi technicznej i operatorskiej.

Do zabezpieczeń sprzętowych należy przede wszystkim możliwość przetwarzania każdego systemu na obydwu minikomputerach NCR-8200 lub w przypadku poważnej awarii - na takich samych komputerach zainstalowanych poza Ośrodkiem.

W ramach każdego systemu stosowane są standardowo następujące zabezpieczenia programów:

1. kopie programów i zbiorów głównych,
2. trzy generacje wszystkich zbiorów dyskowych niezbędnych do powtórzenia trzech ostatnich przebiegów,

3. Kontrola numerów seryjnych nośników magnetycznych i numerów generacji zbiorów,
4. sumy kontrolne wszystkich dyskowych zbiorów sekwencyjnych.

Ponadto, w każdym Systemie wmontowane są dodatkowe zabezpieczenia programowe, zwiększające niezawodność i bezpieczeństwo przetwarzania.

Przykładowo:

1/ w Systemie rozliczeń zagranicznej turystyki indywidualnej przyjazdowej prowadzona jest rozwinięta kontrola całego przebiegu przetwarzania, obejmująca:
- kolejność wykonywanych programów,
- numery i daty zbiorów

oraz różne przekroje sum kontrolnych i bilansowych;

2/ w Systemie zautomatyzowanej wymiany walut przechowywane są szyfrowane numery kasjerów; wprowadzenie takiego numeru jest warunkiem startu Systemu na danym stanowisku kasowym; ponadto System rozróżnia numer kierownika zmiany, upoważnionego do wykonywania funkcji specjalnych;

3/ w zaprojektowanym do pracy on-line Systemie bilansowania miejsc noclegowych, osoba rozpoczynająca pracę w systemie musi każdorazowo wprowadzić swój kod, uprawniający ją do wykonywania określonych funkcji.

mgr inż.P.Brzezicki
Centrum Informatyki
Gospodarki Morskiej
Gdynia

ANALIZA ZABEZPIECZEŃ W SIECIACH TRANSMISJI DANYCH

1. Charakterystyka zagadnienia

W systemach o działaniu bezpośrednim użytkownik, wykorzystując odpowiednie środki techniczne i programowe, ma bieżący kontakt z systemem liczącym, a w szczególności dostęp do zbiorów przechowywanych w tym systemie. Może to być dostęp do danych i programów, możliwość inicjowania funkcji systemu operacyjnego, odczyt i modyfikacja danych.

W Ośrodkach Obliczeniowych realizujących tradycyjne przetwarzanie wsadowe typowe środki podejmowane w celu zapewnienia ochrony danych, poprawności wyników i zabezpieczenia przed ingerencją osób niepowołanych są niewystarczające w warunkach eksploatacji systemów pracujących na bieżąco.

W systemach o działaniu bezpośrednim:

- zdalne urządzenia końcowe ułatwiają dostęp do systemu liczącego osobom niepowołanym. Wszelkiego typu zabezpieczenia administracyjne i techniczne obowiązujące w Ośrodku Obliczeniowym nie mają zastosowania do użytkowników zdalnych;
- użytkownicy wprowadzając informacje na bieżąco przyjmują odpowiedzialność za poprawność używanych przez siebie zbiorów danych. Scentralizowana kontrola poprawności zbiorów przez porównywanie z dokumentami źródłowymi jest niemożliwa, gdy te nie istnieją, lub są niedostępne. Kontrola poprawności wyników przez personel Ośrodka Obliczeniowego zmienia charakter, gdy wyniki są wyprowadzane na żądanie przez użytkownika poza obrębem Ośrodka;
- charakter sieci ułatwia nieuprawniony dostęp do danych wzdłuż linii telotransmisyjnych.

Środki, które trzeba podjąć dla zapewnienia poufności i jednocześnie ochrony systemów przetwarzania przed niepowołanym dostępem zależą od charakteru systemu i klasy-

fikacji danych. Może być to ochrona fizyczna polegająca na: odpowiednich zarządzeniach administracyjnych narzucających określone normy postępowania i na zastosowaniu urządzeń o żądanych właściwościach.
Sposób funkcjonowania programów użytkowych i systemu operacyjnego będzie natomiast określał zakres ochrony logicznej.
Projekt systemu użytkowego musi określać wszystkie środki ochrony. Ochrona fizyczna i logiczna są ze sobą integralnie związane. Przykładowo: trzeba ustalić zasady postępowania użytkownika w razie przypadkowego wykrycia niepoprawnych danych i jednocześnie programowo umożliwić mu /lub nie!/ poprawienie błędnego rekordu.
Środki ochrony można także sklasyfikować w zależności od stopnia ogólności zastosowania od takich, których można użyć we wszystkich systemach o działaniu bezpośrednim do rozwiązań mających zastosowanie w specyficznych momentach działania systemu. Ten podział przyjęto poniżej.
W dalszej części przez tryb wielodostępny /time sharing/ rozumiany będzie taki sposób pracy użytkownika w którym współpracuje on z systemem operacyjnym, zaś przez tryb transakcyjny /transaction processing/ - współpracę z programem użytkowym. W pierwszym trybie użytkownik układa i wprowadza zadanie wykonywane na bieżąco pod kontrolą systemu operacyjnego, w drugim - inicjuje jedną z góry określonych funkcji zadania użytkowego obsługującego jego terminal.

2. Środki ochrony

W eksploatacji systemu o działaniu bezpośrednim trzeba zastosować takie rozwiązania, które zabezpiecza kompletność, poprawność i poufność informacji. Rozwiązania te można podzielić na:

- zabezpieczenie przed skutkami awarii sprzętu komputerowego,
- zabezpieczenie przed nieprawidłowymi /zamierzonymi lub przypadkowymi/ działaniami ludzi mającymi kontakt z systemem przetwarzania.

Pierwsza grupa zabezpieczeń sprowadza się do opracowania i wdrożenia procedur restartu systemu i odtwarzania uszko-

kadzonych zbiorów danych, jak również zasad postępowania w trakcie awarii i nie będzie tutaj omawiana. Pominięto także opis środków ochrony grupy drugiej, mających zastosowanie w obrębie Ośrodka Obliczeniowego.
Ochrona przed nieprawidłowymi działaniami ludzi może dotyczyć:
- sieci teletransmisyjnej,
- urządzeń zdalnych.

2.1. Ochrona sieci transmisji danych

Fakt, że komunikacja użytkownika z zestawem liczącym odbywa się poprzez linię telefoniczną /lub telegraficzną/ może zostać wykorzystany przez osobę niepowołaną do uzyskania lub wprowadzenia informacji na odcinku łącza między urządzeniem zdalnym a komputerem.
Dostępne środki ochrony, to:

2.1.1. Utrudnienie dostępu do łącz teletransmisyjnych.

Najłatwiej podłączyć się do linii w obrębie budynku użytkownika. Z tego względu głowica rozdzielcza powinna znajdować się w pomieszczeniu zamykanym, a przewody telefoniczne powinny być niedostępne /prowadzone w ścianach/. Poza budynkiem identyfikacja przewodów używanych do transmisji danych w kablu wieloprzewodowym jest bez odpowiedniej dokumentacji bardzo trudne.

2.1.2. Szyfrowanie

Zastosowanie efektywnego szyfru może praktycznie uniemożliwić nieuprawnione uzyskanie informacji. Przykładowo koszt "złamania" /za pomocą odpowiedniej maszyny cyfrowej/ projektowanego standardowego szyfru do transmisji danych NBS-DES oceniany jest na około 20 - 200 mln $. Decydując się na użycie szyfru projektant musi uwzględnić ograniczenia protokółu transmisji /zastrzeżone znaki sterujące/ i ewentualnie zapewnić odpowiednie urządzenia techniczne.

2.2. Ochrona urządzeń zdalnych

Stosowane są tu zarówno zabezpieczenia fizyczne, jak i logiczne:

2.2.1. Zabezpieczenia fizyczne

Zdalne urządzenia końcowe mogą zostać wyposażone w czytnik kart identyfikacyjnych, lub zamek mechaniczny. Uprawniony użytkownik musi wówczas posiadać odpowiednią kartę /z zapisem magnetycznym, rzadziej - optycznym/ lub klucz. Ograniczać można także dostęp do pomieszczenia, w którym znajduje się urządzenie zdalne. Urządzenie może być wyposażone w układ identyfikujący je przy łączności z komputerem centralnym.

2.2.2. Podstawowe zabezpieczenia logiczne

Zabezpieczenia te realizowane są przez hasła stanowiące"klucze dostępu" i/lub identyfikujące użytkownika. Sposób wprowadzenia hasła powinien uniemożliwiać poznanie go przez osoby postronne. Hasła powinny być okresowo zmieniane. Sposób zmianirozprowadzania haseł wśród użytkowników powinien uniemożliwiać zapoznanie się z nimi przez osoby trzecie. Można zastosować także zasadę pytań użytkownika o fakty tylko jemu znane. Uporczywe próby ominięcia hasła powinny być rejestrowane i sygnalizowane.

2.2.3. Zabezpieczenia logiczne w trybie wielodostępnym

System operacyjny musi posiadać właściwości umożliwiające przypisanie zbiorów /danych i programów/ poszczególnym użytkownikom i zakazujące dostępu do "cudzych" zbiorów bez zgody "właściciela". Zgoda ta może zezwalać jedynie na odczyt, zapis lub wykonanie programu. Mogą być stosowane klucze dostępu do poszczególnych zbiorów. Zadania inicjowane z urządzenia zdalnego nie powinny mieć wpływu na przebieg innych prac. Zakres funkcji dostępnych z urządzenia zdalnego należy w razie potrzeby ograniczyć do niezbędnego minimum.

2.2.4. Zabezpieczenia logiczne w trybie transakcyjnym

Zabezpieczenia te dotyczą:

- typu transakcji,
- ochrony danych przed niepowołanym odczytem,
- kontroli poprawności danych przy wprowadzaniu

2.2.4.1. Typ transakcji

Należy rozważyć jakie kategorie użytkowników współdziałają z systemem transakcyjnym i w jakim stopniu są oni upoważnieni do zapisu/odczytu danych. Transakcje służące do wprowadzania/wyprowadzania danych, które nie powinny być dostępne dla ogółu użytkowników należy poprzedzić dodatkowym hasłem. Niezależnie od zakresu przyjętej identyfikacji użytkownika /patrz 2.2.2./ istotne transakcje wejściowe powinny być autoryzowane.

Zasady autoryzacji muszą wykluczyć możliwość "podobieństwa podpisu".

2.2.4.2. Ochrona przed niepowołanym odczytem

Niezależnie od środków opisanych powyżej należy rozważyć ewentualną konieczność zakazu wyprowadzenia danych określonej treści. W takim przypadku system użytkowy musiałby badać zawartość rekordu przed wysłaniem go do urządzenia zdalnego i w razie negatywnego wyNiku - informować użytkownika o niemożliwości wyprowadzenia tej informacji.

2.2.4.3. Kontrola poprawności przy wprowadzaniu

Należy w jak najszerszym stopniu stosować standardowe techniki kontroli zawartości poszczególnych pól, a także - w miarę możliwości - badać na niesprzeczność z dotychczas istniejącymi zbiorami.

3. Konkluzja

Postulat zabezpieczenia poprawności, kompletności i poufności danych musi zostać uwzględniony na wszystkich etapach prac związanych z systemem o działaniu bezpośrednim, w sposób racjonalny i przemyślany. Nadmierne zabezpieczenie systemu utrudnia jego prawidłowe funkcjonowanie i podraża koszty, niedostateczne - może narazić użytkownika na poważne straty.
W ramach prac projektowych należy zatem:

- przeprowadzić analizę przetwarzanych danych i funkcji systemu:
  - określić, kto i w jakim zakresie powinien mieć do nich dostęp i kto ma być odpowiedzialny za poprawność zbiorów,
  - ocenić skutki zniszczenia danych, błędnej aktualizacji nieuprawnionego odczytu,
  - określić przepuszczalne cele i prawdopodobieństwo nieprawidłowego wykorzystania systemu i dokonać podziału danych określając wymagany stopień zabezpieczenia,
- przeprowadzić analizę struktury sieci transmisji danych:
  - określić najbardziej prawdopodobne sposoby nielegalnej ingerencji w działanie systemu,
  - przeanalizować dostępne środki ochrony - fizyczne i logiczne i określić sposób zabezpieczenia systemu.

Po wdrożeniu należy okresowo weryfikować celowość i skuteczność zastosowanych środków ochrony.

Piotr Pawlak

kmdr Henryk Paciorek
Centrum Informatyki
Gospodarki Morskiej
w Gdyni

Zabezpieczenie systemów i zbiorów informacji

I. Zasady ogólne

1. Uwzględniając fakt, że informatyka szerokim frontem wkracza we wszystkie dziedziny życia gospodarczego - powstaje konieczność wprowadzenia niezawodnych metod ochrony systemów i zbiorów informacji.
2. Aby ochrona była skuteczna i stosowna do posiadanych urządzeń i wykonywanych prac, winna opierać się na wnikliwej analizie istniejącego stanu w Ośrodku Informatyki i wprowadzeniu takich środków ochrony, które będą odpowiadały faktycznym potrzebom.
   Do potrzeb zalicza się nie tylko sprawy /materiały/ posiadające odpowiedni stopień poufności i tajności, lecz również potrzebę wdrożenia nawyków przestrzegania ustalonego reżimu pracy przez personel, celem przygotowania go do podjęcia w każdej chwili prac tajnych oraz umiejętnej ochrony zbiorów i systemów przed zagrożeniem ich zniszczenia lub utraty.
3. Pod pojęciem zagrożenia zbiorów i systemów należy rozumieć:
   - wypadki, błędy w pracy powodujące nieumyślne zniszczenie zbiorów lub ich pojedynczych elementów,
   - niekontrolowany dostęp do zbiorów i systemów, przez co istnieje ryzyko kradzieży lub umyślnych zniszczeń,
   - samowalny dostęp w nadzwyczajnych okolicznościach np. w czasie pożaru, awarii urządzeń, powodzi itp.,
   - świadome zagrożenie ze strony nieupoważnionych pracowników w wyniku:
     - niezbyt jasno sprecyzowanych kryteriów dopuszczania do zbiorów,
     - nadmiernego zaufania do pracowników,
     - nierejestrowanie każdego dojścia pracownika do zbiorów, przez co istnieje bezkarność w działaniu,
   - zagrożenie środowiska naturalnego /pożar, powódź, awaria elektryczna itp./ i świadome akcje niszczące przez pra-

cowników lub osoby obce,
- świadome penetracje przez osoby obce, posiadające jednak niezbędną wiedzę techniczną.

4. Przedmiotem ochrony zbiorów i systemów powinny być następujące środki informatyczne:
- maszynowe nośniki informacji, a w tym:
- taśmy magnetyczne,
- dyski magnetyczne,
- taśmy kasetowe,
- karty perforowane,
- taśmy perforowane,
- linie teletransmisyjne,
- dokumenty źródłowe i wynikowe,
- korespondencja,
- dokumentacja systemów,
- instrukcje systemowe, a w tym:
  - operatorskie i użytkownika,
- personel,
- sprzęt informatyczny.

5. Uwzględniając przedmiot ochrony oraz formy zagrożenia, należy stosować następujące rodzaje ochrony systemów i zbiorów:
- ochrona fizyczno-techniczna,
- logiczna ochrona informatyki /zabezpieczenie dostępności do prac informatycznych/.

Oba wymienione rodzaje ochrony winny posiadać należyty system kontroli skuteczności ich działania.

II. Ochrona fizyczno-techniczna

1. Ochrona fizyczno-techniczna zawiera w sobie następujące metody zabezpieczenia zbiorów informacji:
- fizyczne /zamknięcia/,
- organizacyjne,
- techniczne /zabezpieczające przed przypadkowym zniszczeniem zbiorów przez żywioł/.

Możliwości dostępu do zbiorów, zarówno przez personel ośrodka jak i przez użytkowników, winny być ograniczone dla niezbędnej ilości osób i ściśle kontrolowane.

2. Przy wejściu do budynku winna znajdować się stała służba dozoru /portier/, posiadająca jasno sprecyzowane w odpowiedniej instrukcji, zasady: kogo i w jakich okolicznościach wolno wpuszczać do budynku.
3. Organizacja pracy w Ośrodku winna być taka, aby sprzyjała ochronie zbiorów informacji. W tym celu:
   - dział kadr pracowniczych winien mieć należyte rozeznanie w wartościach moralnych zatrudnionych pracowników,
   - dyrektorzy Ośrodków winni ponosić pełną odpowiedzialność, za:
     - wydanie odpowiednich instrukcji zabezpieczających zbiory informacji,
     - ruch osobowy wewnątrz zakładu pracy,
     - egzekwowanie przestrzegania wydanych instrukcji,
     - przestrzeganie zasady, że pracownik Ośrodka ma dostęp wyłącznie do tych materiałów, które opracowuje,
     - kierownik pionu technicznego winien tak zorganizować obsługę techniczną sprzętu, aby w pełni były zachowane potrzeby ochrony zbiorów. W tym celu:
       - ustalić wykaz osób, które mogą wchodzić do sali EMC, oraz w jakim celu,
       - wprowadzać współczesne urządzenia zamykające wejścia do budynku i pomieszczeń.

   Skuteczność ochrony zbiorów winna być okresowo kontrolowana przez kierownictwo Ośrodka.

   Kontrole mogą być planowe, kompleksowe, doraźne i wyrywkowe. Wyniki kontroli winny służyć wniesieniu poprawek w posiadanych instrukcjach ochrony zbiorów informacji.
4. Metoda technicznej ochrony winna zabezpieczyć zbiory przed przypadkowym zniszczeniem przez żywioł /pożar, zalanie wodą/. Niezależnie od tego, że ośrodki obliczeniowe, a szczególnie sale EMC, winny zajmować budynki o najwyższej klasie odporności ogniowej, stosuje się szereg urządzeń technicznych wykrywających dym, ogień i wodę, sygnalizujących wykryte zjawisko oraz automatycznie uruchamiające środki gaśnicze, lub odcinające dopływ wody. W celu zwiększenia zabezpieczenia technicznego należy również stosować telewizję przemysłową z takim rozmieszczeniem kamer, aby wszystkie najbardziej zagrożone pomieszczenia znajdowały się pod ciągłą obserwacją.

Stała obserwacja wybranych pomieszczeń zwiększa również dyscyplinę zachowania się pracowników, oraz utrudnia wszelkie zabronione działania.
Wybrane pomieszczenia /np.sala EMC, biblioteka itp./ winny być wyposażone w odpowiednie zamki, umożliwiające wejście za pomocą klucza - przepustki z szyfrem.

III. Ochrona zbiorów na etapie projektowania

Każdy ośrodek obliczeniowy posiada określony standard zabezpieczenia zbiorów informacji, wynikających z warunków lokalowych, organizacyjnych i aktualnych potrzeb. Szczegółowe określenie w projekcie systemu stopnia zabezpieczenia informacji konieczne jest w przypadku, gdy wymagania systemu, określone przez użytkownika są odmienne od istniejącego standardu.

Ochrona zbiorów na etapie projektowania polega na odpowiedniem zakwalifkowaniu systemu /jawne, poufne, tajne, tajne specjalnego znaczenia/ i zabezpieczeniu przed zniszczeniem lub utratą.
Kryteria dotyczące w/w spraw ustalają wspólnie projektant z użytkownikiem, uwzględniając następujące pojęcia rodzajów środków informatycznych podlegających ochronie na tym etapie:
- założenia projektowe systemu użytkowego,
- projekt wstępny systemu użytkowego,
- projekt techniczny systemu użytkowego,
- biblioteka programów systemu,
- dokumenty źródłowe,
- zestawienia wynikowe,
- pliki z danymi systemu na nośniku magnetycznym,
- instrukcje operatorskie,
- korespondencja dotycząca systemu,
- EMC z urządzeniami peryferyjnymi,
- urządzenia przygotowania danych,
- środki transmisji danych.

Użytkownik może wprowadzić ograniczenia dostępności do wszystkich w/w środków informatycznych lub też tylko w stosunku do niektórych, wymienionych w umowie.

W celu ujednolicenia pojęć stosowanych w umowach z użytkownikiem, należy stosować następującą terminologię w zakresie:

1. Sposobów zabezpieczenia przed odczytem środka informatycznego:
   - brak zabezpieczenia,
   - zaszyfrowanie,
   - dostęp tylko dla określonej grupy pracowników,
   - dostęp możliwy po podaniu hasła,
   - dostęp możliwy po okazaniu żetonu,
   - dostęp możliwy tylko po podaniu hasła /zabezpieczenie programowe/,
   - dostęp możliwy tylko po okazaniu żetonu /zabezpieczenie programowe/,
   - zamknięcie w szafie metalowej,
   - zamknięcie w kancelarii tajnej,
   - zamknięcie w ogniotrwałej szafie pancernej,
   - zabezpieczenie przez obróbkę w pomieszczeniu, które spełnia warunki takie jak do pracy z dokumentami tajnymi,
   - likwidacja przez pocięcie po przekazaniu wyników użytkownikowi,
   - zamykanie w kasecie na czas transportu,
   - zabezpieczenie przez rozczłonkowanie kompletu całej informacji na części "wzdłuż" - tj. poszczególne cechy opisujące podmiot są gromadzone w odrębnych tomach,
   - zabezpieczenie przez rozczłonkowanie kompletu całej informacji na części "w poprzek" /"wszerz"/, tj. cały zbiór pocięty jest na części zapisane w odrębnych tomach.
2. Sposobów zabezpieczenia przed zniszczeniem lub utratą
   - brak zabezpieczenia,
   - dodatkowa kopia przechowywana w lokalu ośrodka obliczeniowego,
   - dodatkowa kopia przechowywana poza ośrodkiem obliczeniowym /odległość około 4 km/,
   - przechowywanie w zwykłej szafie z zamkiem patentowym,
   - przechowywanie w szafie metalowej z zamkiem patentowym,
   - transportowanie w zamykanej kasecie metalowej,
   - przechowywanie w kancelarii tajnej,
   - obróbka w specjalnym pomieszczeniu zamkniętym,
   - przechowywanie u użytkownika.
3. Grup pracowników upoważnionych do dostępu do środka informatycznego:

- dowolne osoby,
- operatorzy EMC:
  operatorzy EMC danej zmiany,
  kierownik działu EMC,
- pracownicy biblioteki nośników informacji w ośrodku obliczeniowym,
  pracownicy biblioteki nośników informacji danej zmiany,
- obsługa techniczna,
  obsługa techniczna danej zmiany,
- projektant systemu,
  projektant danego systemu,
  programista systemu,
  programista danego systemu,
  konserwator systemu,
- dyrekcja zakładu,
  dyrekcja Ośrodka Obliczeniowego,
  dyrekcja danego Ośrodka Obliczeniowego,
  dyrekcja pionu projektowania,
  kierownictwo działu projektowego,
  kierownik danego działu projektowego,
- pracownicy stacji przygotowania danych,
- przedstawiciel użytkownika.

Uwaga: Jeśli nie zastrzeżono inaczej, upoważnienie pracownika do dostępu do określonej informacji automatycznie oznacza, że dostęp posiadają również jego przełożeni. Reguła ta nie ma zastosowania w przypadku dostępu na podstawie hasła, żetonu lub upoważnienia imiennego.

4. Dla każdego stopnia zakwalifkowania zbiorów /jawne, poufne, tajne i tajne specjalnego znaczenia/ należy opracować wyczerpujące zakresy zabezpieczenia informacji.

IV. Ochrona zbiorów i wyników na etapie przetwarzania

Zabezpieczenie zbiorów i wyników w całym procesie przetwarzania winno posiadać doskonale zorganizowaną kontrolę WE/WY, odnoszącą się do systemów użytkowych i testowania.

W odniesieniu do systemów użytkowych:

- prowadzenie rejestru zdarzeń zaistaniałych w całym procesie przetwarzania /spływ dokumentów, przekazanie do obliczeń, korekty, sytuacje nieprzewidziane itp./,
- ewidencjonowanie archiwalnie dokumentów /zbiorów WE/,
- analiza wszystkich dokumentów, wyjściowych /tabulogramów/ otrzymanych z obliczeń. Selekcja wydruków do całkowitego zniszczenia lub na makulaturę.

W zakresie testowania:

- rejestracja każdej pracy złożonej do testowania,
- przygotowywanie wsadów do przetwarzania,
- analiza rezultatów testowania. Selekcja wydruków do zniszczenia lub na makulaturę.

Podstawowym okresem na tym etapie jest przetwarzanie na EMC i w tym czasie należy przewidywać:

1. Z zakresu wymagań ogólnych:
   1.1. niedopuszczanie do obsługi urządzeń, manipulowania danymi wejściowymi oraz tabulogramami osób postronnych,
   1.2. wykonywanie jedynie tych prac, które zostały przygotowano przez kontrolę WE/WY,
   1.3. dopilnowywanie codziennej konserwacji sprzętu oraz czyszczenia przestrzeni międzypodłogowej,
   1.4. wprowadzenie komisyjnych egzaminów weryfikujących umiejętności operatorów szczególnie nowo zatrudnionych.
2. W zakresie przetwarzania systemów i testowań.
   2.1. Rejestracja zdarzeń powstałych na etapie obliczeń,
   2.2. Przekazywanie wszystkich dokumentów wyjściowych do kontroli WE/WY,
   2.3. współpraca przy przygotowaniu przez kontrolę wsadów obliczeń.
3. W obsłudze taśm magnetycznych
   3.1. Zdejmowanie pierścienia zapisu każdej taśmy etykietowanej,
   3.2. zakaz zmian nazw taśmy bez specjalnego zlecenia kontroli,
   3.3. przestrzeganie właściwego numerowania taśm,
   3.4. przekazywanie do biblioteki taśm wykazujących błędy z krótkim opisem ich typu.
4. W obsłudze dysków magnetycznych
   4.1. przekazywanie do biblioteki pakietów wykazujących błędy z krótkim opisem ich typu,

4.2. uważne i właściwe manipulowanie pakietami dyskowymi na sali EMC.

Dostęp do procesu przetwarzania winien być zorganizowany na zasadach podobnych do etapu projektowania, a ponadto:

1. Dostęp na salę EMC mają jedynie operatorzy i obsługa techniczna z tym że, w czasie wykonywania prac tajnych lub tajnych specjalnego znaczenia osoby te muszą posiadać specjalne dopuszczenie do prac tajnych.
2. Wstęp na salę innym osobom jest możliwy jedynie po uzyskaniu zgody dyrektora oddziału i to w towarzystwie osoby uprawnionej do przebywania na sali EMC.
3. Celowym byłoby wyposażenie pracowników uprawnionych do przebywania na sali EMC w odpowiednie plakietki rozpoznawcze, o innym kolorze aniżeli plakietki wszystkich pracowników przebywających na terenie Ośrodka Obliczeniowego.
4. W okresie wykonywania prac z zakresu obronności kraju prowadzić ścisły rejestr osób wchodzących na salę EMC.

V. Biblioteka nośników magnetycznych

Osoby zatrudnione w bibliotece winny odpowiadać wymaganiom i spełniać warunki określone dla osób dopuszczonych do prac z dokumentami tajnymi, zawsze wtedy, gdy prowadzone prace posiadają klauzulę tajną lub tajną specjalnego znaczenia.

Ewidencja przechowywania oraz wydawania tych zbiorów winna być zgodna z przepisami o obchodzeniu się z dokumentami stanowiącymi tajemnicę państwową lub służbową.

A ponadto, należy dokonywać następujących czynności w pracach z:

1. Taśmami magnetycznymi:
   1.1. prowadzenie kartoteki zdarzeń dla każdej taśmy oddzielnie /błędy, obcięcia, zmiana znacznika itp./,
   1.2. kontrola stanu zużycia oraz uszkodzeń mechanicznych taśm i ich kaset,
   1.3. zakładanie pierścieni zapisu taśmami oddawanymi do zerowania,
   1.4. niedopuszczanie do produkcji taśm po wystąpieniu na nich błędu typu FAIL,

1.5. wydawanie taśm do produkcji poprzez rejestr zmianowego obrotu taśmami,

1.6. dopilnowanie odpowiedniego przygotowania przed produkcją taśm nowych /przewinięcia/,

1.7. zabezpieczenie zbiorów szczególnej wagi w kopiach przechowywanych w innym ośrodku obliczeniowym/w odległości około 4 km/.

2. Dyskami magnetycznymi

2.1. prowadzenie kartoteki zdarzeń dla każdego dysku oddzielnie,

2.2. niedopuszczanie do produkcji pakietów po błędach typu FAIL oraz SCA,

2.3. kwalifikacja pakietów dyskowych do użycia oraz czyszczenie filtrów,

2.4. wydawanie pakietów do produkcji jedynie poprzez rejestr zmianowy.

Specjalista d/s wojskowych
Henryk Paciorek

mgr Eugeniusz KUBICA
Katowickie Przedsiębiorstwo
Informatyki Przemysłu Budowlanego "ETOB"

K O M U N I K A T

Zabezpieczenie zbiorów w Katowickim Przedsiębiorstwie Informatyki P.B. "ETOB"

---

1. Zabezpieczenie organizacyjne informacji w procesie przetwarzania oraz przed dostępem osób nieupoważnionych.

2. Zabezpieczenie maksymalnej informacji o zaszłościach użytkownika na TM i DM /celem umożliwienia wykonania opracowań za dowolny okres obliczeniowy/.

3. Zabezpieczenie zbiorów taśmowych i dyskowych przed ew. zniszczeniem /fizycznym, ew. z powodu awarii maszyny/.

4. Zabezpieczenie systemowych TM i DM.

5. Zabezpieczenie systemowe przed zniszczeniem zbiorów na TM i DM.

1. Zabezpieczenie organizacyjne informacji w procesie przetwarzania oraz przed dostępem osób nieupoważnionych

W celu właściwego zabezpieczenia informacji przed dostępem osób nieupoważnionych należy wprowadzić odpowiednią organizację i technologię przetwarzania od momentu przyjęcia dokumentów źródłowych poprzez przygotowanie maszynowych nośników informacji, przetwarzanie na komputerze i wysłanie opracowań wynikowych.

Poprawna technologia przetwarzania powinna uwzględniać na wszystkich etapach odpowiednie punkty kontrolne, odpowiednie opisanie danych, właściwą rejestrację otrzymanych i przekazanych danych z uwzględnieniem ilości, daty, nazwy, stopnia tajności, osób upoważnionych itp. cech wszystkich ogniw przetwarzania.

Spełnienie wymogu odpowiedniej organizacji jest pierwszym stopniem zabezpieczenia zbiorów i jest stosowane w KPIPB ETOB. Prócz tego należy przestrzegać wymogów dotyczących odpowiedniego zamknięcia wszystkich dokumentów, danych i opracowań wynikowych oraz jasnego określenia czynności i odpowiedzialności przez właściwe zakresy.

Wymienione aspekty są przestrzegane w KPIPB "ETOB" i prócz tego pozwalają na sprawne wykonywanie zadań, zabezpieczają zachowanie tajemnicy służbowej.

Pierwszym etapem przetwarzania jest przygotowanie dokumentu źródłowego. Czynności te sprowadzają się do:

- zarejestrowania nadesłanej partii dowodów źródłowych
- sprawdzenie zgodności ze specyfikacją
- sprawdzenie formalne i merytoryczne danej partii materiału
- ustalenie dokładnej liczby ilości pozycji
- wystawienie tzw. "zlecenia perforacji" dla danej partii materiału, określającego cechy oraz ilość
- przekazanie danej partii danych do perforacji wraz ze "zleceniem perforacji"
- kompletacja całości dokumentów źródłowych po zakończeniu przetwarzania.

Wyżej wymienione czynności są niezbędne dla zabezpieczenia danych. Dokumenty źródłowe są przechowywane w zamykanych szafach i pomieszczeniach. Dostęp do nich mają tylko i wyłącznie osoby upoważnione.

Drugim etapem jest tworzenie maszynowych nośników informacji, którego ogniwami właściwego zabezpieczenia są:

- przyjęcie dowodów zgodnych ze "zleceniem perforacji" i przekazanie kopii zlecenia do sekcji sprawdzarek
- wypełnienie karty obiegowej dla danej paczki dokumentów
- zarejestrowanie w karcie przerobu pracownika
- zarejestrowanie w zleceniu perforacji numeru pracownika
- przyjęcie wyperforowanych danych od pracownika
- przekazanie do sprawdzenia partii materiału
- powtórne wypełnienie karty obiegowej

- rejestracja w karcie przerobu sprawdzarki
- wystawienie, dla pliku, karty pilotującej
- przekazanie dokumentów źródłowych do sekcji kontroli wejścia.

Następnie dane wędrują do zespołu kompletacji, gdzie następuje:

- uzgadnianie ilościowe oraz kompletowanie danych wg "zlecenia perforacji" dla danego systemu epd
- nanoszenie ilości danych wejściowych na tzw. - karty operacji
- przyjęcie i rejestracja kart operacji
- przygotowanie taśm magnetycznych lub dysków, określonych kartą operacji
- przekazanie danych łącznie z taśmami i kartami operacji do przetwarzania kierownikowi zmiany emc lub mla.

Elektroniczne przetwarzanie danych realizowane jest na podstawie dobowego planu obciążenia oraz w oparciu o przygotowane dane, karty operacji oraz zbiory. Dobowy plan obciążenia sporządzany jest przez dyspozytora przy współpracy z operatorem systemu i po zatwierdzeniu przez kierownika przetwarzania, przekazywany jest do realizacji. Kartę operacji wypełnia operator systemu z zaznaczeniem właściwych zbiorów TM do wzięcia.

Karty perforowane na emc są przechowywane w pomieszczeniu zamykanym, natomiast technika mla nie umożliwia zamykania danych po zakończonym cyklu przetwarzania, stanowiąc zagrożenie zaginięcia dokumentów.

Jak wynika z opisu technologii obiegu dokumentów źródłowych są one ściśle rejestrowane na każdym etapie przetwarzania od momentu przyjęcia w Kontroli Wejścia aż do momentu powrotu dokumentów do Kontroli, skąd następuje ścisłe rozliczenie z użytkownikiem.

Taśmy magnetyczne oraz dyski przechowywane są w obrębie sal emc oraz w specjalnie wyznaczonym do tego celu pomieszczeniu, znajdującym się poza salą /tzw. archiwum TM/. Pomieszczenia te są stale zamknięte w czasie nieobecności w nich bibliotekarza.

Sprawę prawidłowego funkcjonowania biblioteki i archiwum taśm magnetycznych reguluje Instrukcja Nr 1/76 wprowadzona w życie zarządzeniem Dyrektora KPIPB "ETOB".

Do prowadzenia gospodarki taśmami magnetycznymi i dyskami powołany jest na każdej zmianie bibliotekarz, którego obowiązkiem jest:

- zabezpieczenie zbiorów przed zniszczeniem oraz dostępem do nich osób nieupoważnionych
- prowadzenie dokumentów, zgodnie z instrukcją - księgi inwent. oraz kart ewidencyjnych TM
- wydawanie TM tylko i wyłącznie ujętych w kartach operacji.

Taśmy specjalnego znaczenia /zbiory, programy/ znajdują się poza salą emc w specjalnych metalowych szafach. Klucze do tych szaf przechowywane są w odpowiedniej zaplombowanej gablotce wiszącej w bibliotece TM. Dostęp jest możliwy za zgodą Dyrektora lub Kierownika przetwarzania. Drugi komplet kluczy

umieszczony w zalakowanej kopercie, jest zdeponowany w kasie pancernej i może być wydany jedynie za zgodą Dyrektora. Fakt dostępu do archiwum winien być odnotowany w specjalnym zeszycie.

Wyniki obliczeń przekazywane są natychmiast po wykonaniu do sekcji kontroli, skąd po sprawdzeniu i zarejestrowaniu są wysyłane do użytkownika. Wszelkie poprawki są wykonywane po zgłoszeniu ich zaistnienia dyspozytorowi i operatorowi systemu.

Jak z powyższego opisu wynika, Zbiory Taśmowe i dyskowe są ściśle ewidencjonowane i wydawane tylko osobom upoważnionym, a więc nie ma możliwości wydania Zbioru osobie postronnej. Można stwierdzić, że przebieg procesu przetwarzania z jednoczesną rejestracją informacji o zbiorach i dokumentach w dużej mierze spełnia wymogi ochrony informacji. Dlatego też jasno sprecyzowana została odpowiedzialność osobista w każdym punkcie cyklu przetwarzania i obiegu informacji jak również ścisłe zasady przekazywania danych jednej osobie przez drugą.

Słabym ogniwem w procesie obiegu dokumentów źródłowych i maszynowych nośników informacji jest ich transport i ze względu na rozrzucenie komórek przetwarzania po całym budynku KPIPB "ETOB" należałoby rozważyć zmianę usytuowania poszczególnych komórek epd celem zachowania ciągu technologicznego. Zastosowanie urządzeń do zapisu danych na TM częściowo zmniejszy długość obiegu dokumentów.

Największe zagrożenie stanowi możliwość zaginięcia mni na MLA oraz na R-32 z racji usytuowania regałów odstawczych na korytarzu. Niezbędnym się staje wydzielenie pomieszczenia do tego

celu szczególnie do przechowywania kart związanych z przetwarzaniem na R-32.

2. Zabezpieczenie na TM i DM maksymalnej informacji o zaszłościach użytkownika

Zabezpieczenie to ma na celu umożliwienie wykonania opracowań w ramach danego systemu za dowolny okres obliczeniowy. W tym celu /np. w systemie SGM/ nagrywane są na taśmie zaszłości za kolejne miesiące obliczeniowe a zbiory zachowywane są narastająco w danym roku obliczeniowym. Umożliwia to wykonanie dowolnych /na życzenie użytkownika/ opracowań. Równocześnie zwalnia ośrodek od konieczności przechowywanie dokumentów źródłowych oraz maszynowych nośników informacji, co byłoby nawet niemożliwe, gdyż liczba kart sięga ok. 15 mln rocznie. Informacja o zaszłościach przedsiębiorstw, raz wprowadzona do zbiorów, jest przechowywana przez długi okres czasu a postać przechowywanej informacji jest zgodna z dokumentami źródłowymi.

3. Zabezpieczenie zbiorów przed ewentualnym zniszczeniem

Zabezpieczenie powinno uwzględniać:

- ochronę zapisów niemożliwych do odtworzenia
- niedopuszczanie do większych strat czasu emc w przypadkach awaryjnych
- ochronę zbiorów przed zniszczeniem na pierwszym szczeblu ich tworzenia
- organizacyjne poziomy ochrony zbiorów poprzez stosowanie dublerów

- zapewnienie pełnego zabezpieczenia funkcjonalności systemu epd
- odpowiednie warunki klimatyzacyjne, czystość itp.
- okresowe czyszczenie nośników magnetycznych
- chronienie przed ogniem, wodą i źródłami energii magnetycznej
- badanie losowe tzw. taśm kontrolnych.

Aby spełnić takie zabezpieczenie wprowadzono dla poszczególnych systemów, z uwzględnieniem ich specyfiki oraz doświadczeń eksploatacyjnych, odpowiednią ilość egzemplarzy szczególnie ważnych zbiorów.

Ochrona zapisów jest ściśle związana z określeniem odpowiedniego stopnia ważności. Zapisy na TM i DM są oceniane i kwalifikowane do jednego ze stopni. Według tego następuje określenie miejsca przechowywania oraz upoważnień do eksploatacji.

Rozróżnia się następujące stopnie ważności:

Stopień 0 - obejmuje zapisy o specjalnym znaczeniu ze względu na tajemnicę państwową, służbową /archiwum poza salą/;

Stopień I - obejmuje zapisy niezbędne dla wykonania zadań przeds., nie dające się odtworzyć lub których odtworzenie jest bardzo pracochłonne /wszystkie TM w archiwum poza salą/;

Stopień II - obejmuje zapisy ważne, które dają się z trudem lub dużym kosztem odtworzyć bez krytycznego opóźnienia jakiegokolwiek zasadniczego zadania systemu informatycznego;

Stopień III - obejmuje zapisy, których utrata może sprawić kłopot, ale które można szybko zestawić bez większych strat czasowych;

Stopień IV - obejmuje taśmy robocze itp.

Taśmy stopnia 0 i I /strefa II/ przechowywane są w archiwum z odpowiednią ilością dublerów i to w specjalnym pomieszczeniu. Taśmy stopnia II, III, IV /strefa I/ znajdują się w bibliotece taśm. Zakwalifikowanie nośników magnetycznych do odpowiedniego stopnia ważności dokonywane jest na bieżąco na wniosek Kierownika przetwarzania po zatwierdzeniu przez Dyrektora d/s eksploatacji.

Dostęp do tego rodzaju zbiorów jest możliwy dla ścisłego grona osób i dlatego taka organizacja zabezpiecza prawie w 100% dane dla użytkownika. Niemniej zabezpieczenie takie pociąga za sobą wyższe koszty przetwarzania. Niezależnie od powyższego dane każdorazowo są sprawdzane pod względem jakości zapisu na nośniku magnetycznym.

Zabezpieczenie zapisów w pierwszej strefie użytkowania polega na stosowaniu dublerów /oznaczonych stopniem II, III i przechowywanych w bibliotece/, zgodnie z dokumentacją eksploatacyjną danego systemu przy uwzględnieniu doświadczeń eksploatacyjnych. W związku z tym wprowadzono zasadę kopiowania dublera przed użyciem go w przypadku zniszczenia oryginału. Takie zabezpieczenie ma na celu niedopuszczenie do nadmiernych strat czasu emc oraz chroni dodatkowo strefę II-gą /archiwum - taśmy stopnia 0 i I/.

Taśmy przechowywane poza salą emc, oznaczone stopniem 0 i I, posiadają zabezpieczenie w postaci kilku egzemplarzy aktualizowanych w trakcie procesu przetwarzania lub zmiany programów. Również tutaj obowiązuje zasada wykonania kopii w przypadku zniszczenia 1 egz. przed użyciem oryginału w procesie przetwarzania.

4. Zabezpieczenie taśm magnetycznych i dysków systemowych

Niezależnie od opisanego w pkt. 4 zabezpieczenia taśm systemowych /stopień ważności 0/, w celu zapewnienia prawidłowego i bezawaryjnego funkcjonowania systemów oraz zachowania tajemnicy służbowej należy wprowadzić obowiązek ścisłej rejestracji wszelkich zmian dokonywanych w programach eksploatowanych systemów.

Rejestr Działu Program powinien zawierać prócz innych danych, szczegółowy opis zmian dokonanych oraz nr krążka ze zmianami. Po nagraniu zmian należy przekazać opis zmian w aneksie i nagraną taśmę operatorowi systemu. Operator systemu powinien zarejestrować zmiany oraz skopiować nową taśmę systemową i przekazać ją do archiwum taśm. Ewentualne zmiany muszą objąć również kartę operacji i załączonych schematów przetwarzania.

Tak więc należy dopracować zasady wprowadzania zmian w systemach eksploatowanych w KPIPB "ETOB".

5. Zabezpieczenie systemowe przed zniszczeniem zbiorów TM i DM

Niezależnie od ogólnych poczynań zabezpieczających fizycznie i organizacyjnie całą działalność przedsiębiorstwa, każdy z działających systemów epd powinien mieć specyficzne cechy ochronne.

Sprawy te powinny znaleźć swoje miejsce już na etapie projektowania systemu. Wprowadzanie środków zabezpieczających do systemu już pracującego może być znacznie trudniejsze.

Faktyczny sposób zabezpieczenia, aby niewłaściwy dysk, taśma nie zostały wzięte do przetwarzania polega na stosowaniu na początku i na końcu zbioru etykiet, o znormalizowanym formacie, zawierających informacje dla identyfikacji zbioru, określenie daty ważności itp.

W eksploatowanych systemach epd w KPIPB "ETOB" na R-32 następuje dopuszczenie zbioru do obliczeń na podstawie karty parametrycznej. Błąd w karcie parametrycznej ew. złe podłożenie taśmy powoduje wstrzymanie obliczeń. Niemniej w niektórych systemach taśmy posiadają te same oznaczenia i powodują zniszczenie zbioru w niewłaściwej kolejności użyte przez operatora.

Należałoby opracować wytyczne do programowego zabezpieczenia zbiorów na tyle, aby jakakolwiek pomyłka operatora nie spowodowała zniszczenia zbioru, tzn. aby system nie dopuścił do obliczeń. Należy zaznaczyć, że R-32 umożliwia programowe metody ochrony zbiorów za pomocą etykiet. Ochrona ta może zabezpieczać przed użyciem do obliczeń niewłaściwego zbioru lub też przed dopuszczeniem do systemu nieupoważnionej osoby /klucz dostępu, hasło/ po sprawdzeniu upoważnienia.

Należy zaznaczyć, że stosowane metody ochrony w KPIPB ETOB są aktualnie wystarczające /za wyjątkiem ochrony kart na MLA/. Niemniej należy rozwiązać zabezpieczenie programowe, szczególnie dla systemów opracowywanych na R-32, ze względu na wprowadzenie zdalnego dostępu, aby zabezpieczyć zbiory informacji również w czasie samego przetwarzania na komputerze.