AKADEMIA SZTABU GENERALNEGO

IM. GENERAŁA BRONI
KAROLA ŚWIERCZEWSKIEGO

Por. Janusz TRAWKA

OCHRONA SYSTEMÓW INFORMATYCZNYCH W ASPEKCIE FUNKCJI JEDNOSTEK RESORTU SPRAW WEWNĘTRZNYCH

Rozprawa doktorska

WARSZAWA 1989

AKADEMIA
SZTABU GENERALNEGO
IM. GENERAŁA BRONI
KAROLA ŚWIERCZEWSKIEGO

Por. Janusz TRAWKA

OCHRONA SYSTEMÓW INFORMATYCZNYCH W ASPEKCIE FUNKCJI JEDNOSTEK RESORTU SPRAW WEWNĘTRZNYCH

Rozprawa doktorska

WARSZAWA 1989

AKADEMIA SZTABU GENERALNEGO WOJSKA POLSKIEGO

im. GENERAŁA BRONI KAROLA ŚWIERCZEWSKIEGO

Janusz Trawka

OCHRONA SYSTEMÓW INFORMATYCZNYCH W ASPEKCIE FUNKCJI JEDNOSTEK RESORTU SPRAW WEWNĘTRZNYCH

(Rozprawa doktorska)

napisana pod kierownictwem naukowym
płk prof. dr hab. Władysława Filara

W A R S Z A W A 1988

S P I S T R E Ś C I

W S T Ę P

1. UZASADNIENIE TEMATU.

Ekspansja techniki komputerowej we wszystkich dziedzinach życia jest rownież źródlem wielu problemów. Komputeryzacja poza oczywistym postępem i optymalizacją działania pociąga za sobą również powstanie nowego typu zagrożeń w sferze funkcjonowania państwa, jego instytucji i organizacji. W aspekcie aktualnej sytuacji polityczno-gospodarczej, realizacji reform na wszystkich płaszczyznach oraz zachodzących przemian w przedsiębiorstwach i mentalności społecznej przewidywane perspektywy budzą szereg obaw. Dążenie do postępu jest powodem wzrostu liczby jednostek posiadających komputery , a jest ona juz rzędu dziesiątek tysięcy. Rośnie liczba producentów sprzętu i oprogramowania oraz oferentow różnych usług na tej płaszczyznie. Brak jest jednocześnie norm prawnych, schematów działania i postępowania i nikt w chwili obecnej nie kontroluje w żadnej dziedzinie tego problemu, jego rozmiarów i eskalacji oraz występujacych nieprawidłowości.

Obecne tendencje polityczno-społeczne wskazują na nieuchronną i błyskawiczną rekapitalizację naszego państwa. Wraz z tym procesem jest aktualnie implementowanych wiele rozwiązań, struktur i procesów. Jednocześnie wraz z pozytywnymi i stymulującymi do rozwoju zagadnieniami zaakceptować musimy występujące satelitarnie negatywy. Jednym z nich jest przestępczość. Niepodobną do tej jaką spotykamy w Polsce, jest to przestępczość doskonale zorganizowana, agresywna, kwalifikowana i posługująca się wszystkimi najnowszymi zdobyczami techniki. Społeczeństwo kapitalistyczne to społeczenstwo informatyczne, gdzie informacja w każdej dziedzinie życia i pracy jest dostępna i wykorzystywana do wszystkiego. Problemy przestępstw komputerowych znane są tam od dawna (1), a zyski bądź straty jakie te przestępstwa implikują sa niesamowicie wysokie (2).

Główną hipotezą pracy jest bezwzględna konieczność realizowania ochrony systemów informatycznych metodami wielowariantowymi, szczególnie w aspekcie funkcji jednostek resortu spraw wewnętrznych.

Nie wiadomym jest jak finalnie przedstawiała się będzie struktura resortu. Dla potrzeb niniejszej pracy założono, że

---

(1) Wśród dwudziestu udokumentowanych przestępstw komputerowych dokonanych w USA w latach 1966-1970 było siedem przypadków wandalizmu, cztery kradzieże, osiem defraudacji i dziewieć wypadków błędów.
Wg. "Computer Related Crimes", Journal of Forensic Sciences t.19, nr.9, 1974

(2) Amerykańscy eksperci szacują ewentualne straty wynikłe z możliwości załamania systemu informatycznego obsługujacego karty kredytowe na 30 miliardow dolarów.
por. "Bezpieczeństwo systemów komputerowych", Przegląd Techniczny.Wiadomości i propozycje. 1987 Nr.14

jako jednostki resortu spraw wenętrznych rozumieć będziemy wszystkie te jednostki, do zadań których należy neutralizacja (rozpoznanie, przeciwdziałanie i sciganie) przestępstw (w tym i wykroczeń) zagrażających bezpieczeństwu wewnętrznemu państwa i wszystkim jego podmiotom. W ich składzie należy w przyszłości uwzględnić struktury policyjne różnych szczebli i specjalności, służby specjalne realizujące szeroko pojęte czynności z zakresu kontrwywiadu (w tym przemysłowego i sabotażu) oraz inne wyspecjalizowane agencje (lub pojedyńcze osoby) realizujace te same cele. Ochrona systemow informatycznych w aspekcie jednostek resortu spraw wewnętrznych to neutralizacja przestępstw komputerowych przez wszystkich zainteresowanych i mogących to zadanie realizować. Celem niniejszej pracy jest możliwie wszechstronna analiza problemu oraz wskazanie ewentualnych rozwiązań do wykonania wcześniej wymienionego celu.

Ponadto postawiono szereg dodatkowych hipotez :
-ochrona systemów informatycznych bez wzgledu na to przez kogo i na jakim obszarze jest realizowana musi przebiegać równolegle przy pomocy metod formalnych i operacyjnych (3),
-znajomość metod i środków ochrony wraz z aktywną koordynacją bądź kontrolą jest i będzie bezwzglednie konieczna do zdobywania informacji zawartych w systemach informatycznych dla potrzeb wszystkich jednostek resortu, głównie dla czynności pozaprocesowych oraz dla służb specjalnych (4),
-stan ochrony istniejących systemów informatycznych jest conajmniej niezadawalający, a osoby odpowiedzialne charakteryzuje daleko posunięta niefrasobliwość,
-bieżące prognozy wskazują na lawinowy rozwój zastosowań i potezną ekspansję we wszystkie dziedziny życia mikrokomputerów a w związku z tym należy ze szczególną uwagą wyprzedzajaco uwzględnić tą problematykę w przyszłych zadaniach,
-implementacja rozwiazań technologicznych z Zachodu musi nieuchronnie doprowadzić do wystąpienia analogicznych problemów o zabarwieniu kryminogennym, jednocześnie pamietać należy o zagrożeniach wynikających z pobytu na terenie naszego kraju i ingerencji w polskie sprawy wysokokwalifikowanych specjalistów z wszystkich dziedzin,
-postepująca demokratyzacja w kraju oraz podmiotowa niezależność jednostek gospodarczo-organizacyjnych stanie sie źródłem utrudnienia w dotarciu do potrzebnych resortowi informacji (w tym jednostek policyjnych działających oficjalnie z poparciem społecznym),

---

(3) Zagadnienia z zakresu pracy operacyjnej zgodne są z wymogami instrukcji o pracy operacyjnej i pozycją Korepta L. Matula E. "Praca operacyjna Służby Bezpieczeństwa" Departament Szkolenia i Doskonalenia Zawodowego MSW, Warszawa 1984.

(4) Autor ma na myśli konieczność dostepu do pewnych informacji przechowywanych w systemie bez zwrócenia uwagi na fakt zainteresowania się nimi.

2. METODY BADAŃ.

W celu uzyskania jak najbardziej reprezentatywnej próbki badanej populacji systemów informatycznych posłużono się doborem świadomym. Przebadano 51 systemów informatycznych z czego 11 wyposażonych bylo w tak zwaną "ciezką informatyke", czyli duże komputery. Siedem wykorzystywało minikomputery, w jedenastu przygotowywano dane, a w czterdziestu jeden zainstalowane były mikrokomputery. Sieci mikrokomputerowe badane były w sześciu obiektach, w tym w jednym przypadku była to sieć z pełnym oprzyrządowaniem i oprogramowaniem. Wyłacznie mikrokomputery były wykorzystywane w osiemnastu obiektach badanych. Badania prowadzono na terenie trzech województw - katowickiego, krakowskiego i kieleckiego, a do badań dobrano możliwie najrożniejszych przedstawicieli. Badano zarówno wyspecjalizowane kombinaty informatyczne takie jak COIG (5), CIBEH, duże ośrodki informatyczne autonomiczne takie jak ZETO , ETOB, oraz ośrodki zakładowe duże (np.STAR Starachowice) czy tez pojedyncze stanowiska mikrokomputera zarówno w jednostkach gospodarczych, jednostkach budżetowych jak i szpitalach czy szkołach wyższych. Uwzględniono systemy pracujące w sieciach oraz pracujące w czasie rzeczywistym. W każdym punkcie zrealizowano ankietę, złożoną z odpowiednio dobranego zestawu pytań w zależności od stanowiska zajmowanego przez respondenta. Nie adresowano ankiety do osoby - była ona z założenia anonimowa - lecz kierowano ją do przedstawiciela konkretnej grupy respondentow (np.programistów). Anonimowość starano się osiągnąć poprzez dwuczęściowy układ ankiety, tak aby dane mogące zlokalizować osobę ankietowaną rozdzielić od zasadniczej części ankiety. Jednocześnie w każdym badanym obiekcie prowadzono wywiady oraz starano się osobiście zapoznać ze wszystkimi mającymi funkcjonować metodami ochrony.

Ponadto w piętnastu przypadkach przeprowadzono badania za pomocą metod opracyjnych wykorzystując wiedzę osobowych źrodeł informacji, konkretnie tajnych współpracowników.

Do podstawowych metod badawczych zastosowanych w niniejszej pracy zaliczyć należy analizę statystyczną, syntezę, analizę systemową i krytyczną ocenę literatury. Szczególną uwagę zwrócono na zastosowanie takich technik badawczych jak ankietowanie, wywiady i symulacje.

Ankieta złożona była z trzech części, pierwsza część to karta kwalifikacyjna ośrodka informatycznego, pozwalająca zorientować się w strukturze zakładu oraz zatrudnieniu. Własnie na jej podstawie przygotowywane były zestawy pytań dla poszczególnych stanowisk pracy. Cześć druga była identyczna dla każdego z ankietowanych, a dotyczyła jego podstawowych danych oraz stosunku do problemów ochrony. W części trzeciej, każdy z ankietowanych otrzymał od dwunastu do dwudziestu ośmiu pytań spośród

---

(5) Pełne brzmienie nazw badanych zakładow pracy zawiera załącznik "C".

dziewięćdziesięciu dziewięciu w zależności od zajmowanego stanowiska. Jak juz wspomniano obie te części były rozdzielone poniewaz ankieta była z założenia anonimowa, a cześć druga mogła posłużyć do zidentyfikowania respondenta. Wypełnienie ankiety każdorazowo było nadzorowane bądź osobiście przez autora bądź przez oficera obiektowego, aby uniknąć ewentualności podania wyników niezgodnych ze stanem faktycznym (autor osobiście natrafił na dwa takie przypadki na początku realizacji ankiety - oba zostały skorygowane) (6).

Wywiady prowadzono w każdym badanym systemie i z reguły połączone były z demonstracją metod ochrony, przedstawieniem potrzeb i problemów oraz analizą o wystepujących typach nieprawidłowości. Autorowi jako osobie niezatrudnionej bezpośrednio przy komputerze były bardzo przydatne.

Symulacja zagrozeń miała miejsce przy pomocy metod operacyjnych bądź nieformalnych. Miała na celu wykazanie słabości istniejących mechanizmów ochrony i niestety w większości przypadków próby "włamania się" do poddanych symulacji obiektów zakończyły się sukcesem. Wnioski z tej formy badań podobnie jak zresztą z przeprowadzonych wielu w tym temacie wywiadów zostały uwzględnione w pracy lecz z przyczyn technicznych nie ujęto ich szczegółowo. Nadawały by się one do zilustrowania problemów w książce a nie w pracy naukowej.

Nadmienić również należy, ze opracowanie zamieszczonych w załaczniku " A " badań jest skrótowe i niepełne. Właściwe było realizowane przy pomocy mikrokomputera , a uzyskiwane wyniki wykorzystane zostały w pracy. Podobnie miało miejsce z efektami wywiadów i symulacji. Rezultaty otrzymane w ich wyniku mają swoje odzwierciedlenie w kolejnych rozdziałach pracy . Wyniki badań ankietowych rozpoczynają się od omówienia obiektów badań, ich struktury, osób ankietowanych z uwzględnieniem wielu cech oraz wyciągnięciem wniosków. Nie przeprowadzano obliczeń statystycznych bowiem z uwagi na treść pracy oraz jej zakres nie było to zasadne.

3. USTOSUNKOWANIE SIĘ DO LITERATURY.

Dostępne publikacje, które ukazały się do chwili obecnej dotyczą wyłącznie ochrony systemów informatycznych w aspekcie problematyki cywilnej.

Zainteresowanie się problemem ochrony zainicjowała na szerszą skalę XXIV Konferencja Europejskiego Programu Badawczego Diebolda, ktora odbyła sie w marcu 1972 roku w Wiedniu. Swoiste credo stanowi wypowiedź przedstawiciela

---

(6) W obydwu przypadkach dyrektorzy zoobowiazali się do realizacji ankiety. W pierwszym dyrektor ośrodka wypelnił wszystkie ankiety wraz ze swoim zastepcą, w drugim, ponieważ miał je zebrać (wypełnili je pracownicy), polecił napisać ankietę jeszcze raz, ponownie ją powielić i sam ją wypełnił.

firmy IBM W.H.Murray'a. "Bezpieczeństwo to - zadania kierownictwa obejmujące dbanie o dokładność i nienaruszalność informacji potrzebnej do prowadzenia przedsiębiorstwa, o poufność i niedostępność wrażliwych danych, o ochronę instalacji obliczeniowej przed katastrofami, niewłaściwym użyciem itp., o ustrzeżenie pracowników przed pokusą, a kierownictwa przed nieprzezornością. Bezpieczeństwo musi zapewniać przetrwanie przez przedsiębiorstwo wszelkich katastrof i kontynuację realizacji zadań. Bezpieczeństwo musi współzawodniczyć z innymi zadaniami kierownictwa o zasoby i musi być osiągalne w ten sam sposób jak zysk. Należy więc patrzeć na nie jako na funkcję operacyjną, liniową a nie sztabową." W tym samym 1972 roku w maju w Szczecinie odbyło się Sympozjum Polskiej Grupy Doradczej d/s Współpracy z Europejskim Programem Badawczym Diebolda, poświęcone zagadnieniom ochrony zbiorów.

Ze względu na lawinową eskalację zastosowań informatyki wystąpiła potrzeba zapełnienia luki na odcinku ochrony systemów informatycznych. Wśród autorów którzy zajęli się tym problemem było wielu czołowych teoretyków i praktyków informatyki, takich jak E.Yourdon, J.Martin, D.van Tassel, i inni. Jednocześnie w prawie każdej pozycji z różnych działów informatyki pojawiły się rozdziały lub co najmniej akapity poświęcone problemowi ochrony. W maju 1976 roku we Wrocławiu odbyła się konferencja poswięcona prawnym problemom systemów informatycznych. W roku 1978 w Warszawie zorganizowana została przez TNOiK kursokonferencja na temat "Zapewnienie poufnosci informacji w procesie przetwarzania danych". Pierwszą pozycją ksiazkową, która ukazała się w Polsce była "Ochrona informacji w procesie przetwarzania" Andrzeja Idźkiewicza. W sposób w miarę kompleksowy autor ujął podstawowe założenia i tezy związane ze stosowaniem metod ochrony. Przetłumaczono również i wydano w roku 1982 ksiazkę Lance Hoffmana "Poufność w systemach informatycznych", która jest szczególnie cenną pozycją ze względu na swoją uniwersalność. Podkreślić należy szereg publikacji Andrzeja Dziurnikowskiego i Krzysztofa Marciniaka z MSW oraz Andrzeja Sokołowskiego z WAP. W 1987 roku ukazała się nakładem MON książka A.Sokołowskiego "Ochrona informacji komputerowych", szeroko ujmująca problematykę zagadnień ochrony. Inne wydawnictwa poswięcone informatyce rownież zwracają uwagę w coraz to większym stopniu na problematykę ochrony.

Jednakże wymieniona literatura poswięcona jest w całosci tak zwanej "ciężkiej informatyce" i dotyczy systemów informatycznych, w ktorych eksploatowane sa duze komputery.

W sferze mikrokomputerów brak jest obecnie opracowań związanych z problemem ochrony, a ukazujące się pozycje ograniczają się do wzmianki o istnieniu zabezpieczenia w postaci identyfikatora i hasła. Wynika to głównie z faktu stosunkowo krótkiego czasu użytkowania tego typu sprzętu, niespotykanej skali i obszaru występowania oraz olbrzymiego postępu technicznego w tej dziedzinie. Pojedyńcze publikacje w formie artykułów o charakterze popularno-naukowym

rejestrują w zasadzie symptomy zjawisk bez uogólnień i bliższego ustosunkowania się (7).

Podkreślić należy, ze całość literatury i wszyscy autorzy zwracają uwagę na jeden fakt. Bez względu na koszty ilość i jakość, a także i zakres stosowanych środków i metod ochrony najsłabszym ogniwem ochrony zawsze pozostanie człowiek. Ochrona człowieka, jego praw i swobód to podstawowe zadanie resortu spraw wewnętrznych. Ochrona systemów informatycznych w aspekcie funkcji jednostek resortu spraw wewnętrznych to również ochrona człowieka będącego elementem, użytkownikiem, środkiem ochrony i zarazem zagrożeniem systemu informatycznego, ochrona człowieka przed nim samym.

Podkreślić należy, ze brak jest obecnie kompleksowego, systemowego ujęcia problematyki ochrony ze wskazaniem zadań i funkcji poszczególnych jednostek resortu spraw wewnetrznych oraz instytucji i organizacji cywilnych.

4. ZARYS PRACY.

W pracy znajduje się szeroki przegląd problematyki ochrony systemów informatycznych, głównie w aspekcie funkcji jednostek resortu spraw wewnętrznych. Praca składa się z czterech rozdziałów.

I. Pierwszy zawiera szczegółowy wykaz i omówienie występujących zagrożeń oraz zawiera klasyfikację przestępstw komputerowych, charakterystyki grup sprawców, a także analizę wymienionych problemów.
II. Drugi dotyczy poziomów ochrony z uwzględnieniem charakterystyk, punktów newralgicznych oraz zagrożeń.
III. W trzecim omowióne zostały metody ochrony zarówno pod kątem aktualnego stanu stosowania jak i występujacych potrzeb.
IV. Czwarty stanowi podsumowanie problemów ochrony. Zawarta jest w nim klasyfikacja istniejących systemów w aspekcie ich struktury, oceny aktualnego stanu ochrony oraz zadań na tej płaszczyźnie.

---

(7) Większość informacji dotyczących wystąpienia zagrożeń i przestępstw komputerowych publikowanych jest w popularnych nienaukowych czasopismach. Stwierdzają one jednakże fakty wystąpienia rzutując na ocenę zjawiska bez wzgledu na brak aspektu naukowego.

I. R O D Z A J E , I K L A S Y F I K A C J A Z A G R O Ż E Ń .

1. SABOTAŻ I ZAGROŻENIA NIEUMYŚLNE.

Oba pojęcia charakteryzuje występowanie szkody bez bezpośredniego materialnego lub informacyjnego zysku oraz zbieżny charakter wystepujących zagrożeń.

Możemy do nich zaliczyć :

- pożar,
- warunki atmosferyczne i klęski żywiołowe,
- awaria zasilania energetycznego,
- dezintegracja lub destrukcja informatyczna,
- fizyczne czynniki destrukcyjne,
- czynnik ludzki,

Rozpatrując powyższe jako zagrożenia o charakterze nieumyślnym nie bedą one podlegać zainteresowaniu jednostkom resortu spraw wewnętrznych. Jednak każde z nich może byc rozpatrywane z punktu widzenia sabotażu badź zaniedbania. Szkody wywołane przez zagrożenia nieumyślne z reguły są efektem braku przewidywania badź bezmyślności. Sabotaż rozpatrujemy jako umyślne niewypełnianie albo umyślne wypełnianie wadliwie swoich obowiazków w zamiarze wywołania dezorganizacji, strat i szkód. Zaniedbanie czyli nieumyślność w tym aspekcie implikuje brak zamiaru, jednak powinno się ono znaleźć w kregu zainteresowań jednostek resortu spraw wewnętrznych, głównie w sferze profilaktyki i rozpoznania zapobiegawczego. W odróżnieniu od zagrożeń nieumyślnych sabotaż należy rozpatrywać dwojako. Zagrożenie może byc związane z popełnieniem sabotażu, bądź może być potencjalną przesłanką jego wystąpienia. W pierwszym przypadku rozpatrywać należy sabotaż jako czynnik działania ludzkiego wystepującego w tym samym czasie co efekt finalny w postaci zaistniałego zagrożenia. W drugim mamy do czynienia z działaniem o charakterze perspektywicznym mogącym mieć skutki w przyszłości z reguły w konkretnych uwarunkowaniach. Gdy działania bedą inspirowane przez czynniki zewnętrzne (np.obcy wywiad) będziemy mieli wtedy do czynienia z dywersją.

Rozważmy w powyższym aspekcie nastepujące typy zagrożeń:

1.1. Pożar.

Może być zdarzeniem nieumyślnym, jednak należy wziąć pod uwagę potencjalny efekt sabotażu bądź zaniedbania. Problemem poza celowym podpaleniem jest objeciem sabotażem przepisów i srodków ochrony przeciwpożarowej. Z punktu widzenia funkcji jednostek resortu spraw wewnętrznych należy zwrócić uwagę na całokształt zabezpieczenia przeciwpożarowego pod kątem sabotażu. Obiektem ataku mogą być systemy wykrywania ognia, srodki gaśnicze i przeciwpożarowe, systemy wentylacyjne, a nawet w fazie projektowania i budowy lokalizacja i reżim norm budowlanych.

1.2. Warunki atmosferyczne i klęski żywiołowe.

Należą głównie do zagrożeń o charakterze nieumyślnym. Jednak w przypadku gdy powstają duze szkody trzeba również rozpatrzeć możliwość celowych lub przypadkowych zaniedbań, w zależności od charakteru wystepujących tego typu zagrożeń oraz możliwości ich przewidywania. Niewykluczone jest wykorzystanie prawdopodobieństwa lub cykliczności ich wystąpienia jako środka sabotażowego.

1.3. Awaria zasilania energetycznego.

Ten rodzaj zagrożenia wiąże się z koniecznością pracy systemów informatycznych w skonczonych okresach czasu lub w czasie rzeczywistym oraz ich fizyczną wrażliwością. Trywialne są problemy konieczności awaryjnego zasilania w przypadku dużych komputerów . Lecz w tym przypadku również pojawić się może sabotaż lub zaniedbanie w postaci niesprawnego awaryjnego generatora , nie działającego przy odcięciu zewnetrznego zasilania. Poważnym zagrożeniem jest natomiast brak zasilania w przypadku mikrokomputerów, gdzie istnieją co prawda urządzenia podtrzymujące pracę systemu, lecz są one drogie, rzadko stosowane i w przypadku pracującej sieci trudne do jednoczesnego stosowania. Prowadzone badania wykazały, że w niewielu wypadkach przewidziano awaryjne zasilanie dla mikrokomputerów, a tam gdzie urządzenia takie zakupiono nie były one podłączone z różnych przyczyn.

1.4. Dezintegracja lub destrukcja informatyczna.

Systemy i pakiety użytkowe muszą pracować w konkretnym otoczeniu programowym. Programy i dane są przechowywane w pamięciach stałych lub na zewnętrznych nośnikach informacji. Na atak sabotażowy narażone są zatem programy oraz zbiory i to nie tylko jako całość, ale również w postaci zainstalowanych podprogramów, procedur lub instrukcji dezorganizujacych pracę systemu lub powodujących procesy destrukcyjne z autodestrukcją systemu włącznie. Wystąpienie tego typu akcji sabotażowych należy rozważyć w fazie projektowania i programowania systemu czy pakietu oraz podczas eksploatacji czy dokonywaniu zmian. Może on przybrać postać swoistej "software'owej miny" rezydującej lub założonej np.podczas wprowadzania danych. Szczególnie na tego typu zagrozenia podatne są systemy wielodostepne lub mikrokomputery pracujące w sieciach. Jako przykład posłużyc może szeroko omawiany w publikatorach "wirus" komputerowy atakujący mikrokomputery głównie standardu IBM. Poza tym, że powoduje on zniszczenie zbiorów zarówno na dyskietkach jak i na dysku sztywnym, dezorganizuje podstawowe funkcje mikroprocesorów i systemów operacyjnych to przenosi się z komputera na komputer przy przenoszeniu danych lub programów. Charakteryzuje go również okres utajony, podczas którego "zaraża" on wszystkie dostepne mu miejsca w systemie i w jego otoczeniu, by w dogodnym dla siebie momencie

uaktywnić swoje niszczycielskie mozliwości (8).

1.5. Fizyczne czynniki destrukcyjne.

Zaliczymy do nich to wszystko, co w sposób fizyczny, materialny może doprowadzić do wystąpienia zniszczeń w systemie informatycznym. Stanowią one jedno z najpoważniejszych zagrożeń. Zastosowanie ich może doprowadzić do nieodwracalnego fizycznego zniszczenia sprzętu (np. ładunek wybuchowy) lub nieodwracalnej utraty programów lub zbiorów. Jako przykład może posłużyć specjalna dyskietka, która po włożeniu do napędu dyskowego mikrokomputera IBM powoduje destrukcję systemu.

1.6. Czynnik ludzki.

W przypadku sabotażu człowiek jest sprawcą wymienionych zagrożeń, ale również jego działalność poza wymienionymi może stanowić odrebne zagrożenie. Wymienić tu należy celowe lub przypadkowe złe wypełnianie obowiązków w każdym ogniwie funkcjonowania systemu informacyjnego, spowalnianie lub odmowę pracy, strajk lub bunt.

Akcje sabotażowe stanowią poważny problem w zagadnieniach ochrony ze względu na ich bezwzględność i pozorną irracjonalność. Sabotazysta działa w zamiarze uszkodzenia sprzętu lub oprogramowania. Motywy jego działania mogą być polityczne, ekologiczne, ekonomiczne bądź osobiste. Sabotaż może przybierać różnorodne formy techniczne, jednak sprawca musi mieć dostęp do urządzeń by móc je uszkodzić w sposób bezpośredni. Jeżeli posiada wiadomości z dziedziny informatyki może uszkodzić urządzenie drogą pośrednią lub zadziałać perspektywicznie zewnetrznie. Najczęściej ma on kontakty osobiste z użytkownikami urzadzenia lub sam jest pracownikiem danej instytucji. Takie osoby mają ułatwione zadanie - łatwy dostęp, znajomość procedur wewnętrznych, a poza tym brak wzbudzania podejrzeń. Utrudnia to wykrycie szkody i sprawcy.

2. INFILTRACJA BIERNA I CZYNNA.

Wszystkie elementy systemu informatycznego są narażone na infiltrację (9). W odróżnieniu od sabotażu, działania infiltracyjne związane są z osiągnięciem przez sprawcę konkretnego zysku. Istnieją trzy rodzaje infiltracji : przypadkowa, bierna i czynna. Pierwsza , biorąc pod uwagę rozbudowane moduły kontroli wewnętrznej oraz postęp w dziedzinie rozwoju systemów operacyjnych jest w zasadzie

---

(8) Por. Majewski Władysław , "Wirusowa goraczka", Komputer 1988 Nr. 11

(9) Infiltracja - to działanie osób nieupoważnionych mające na celu przenikanie do różnych punktów w systemach informatycznych w celu zdobycia informacji przy pomocy różnych sposobów i środków.

problemem szczątkowym. Do poważnych zagrożeń zaliczyć należy infiltrację bierną i czynną.

2.1. Infiltracja bierna.

Można ją porównać do podsłuchu, który może wystąpić jako wewnętrzny lub zewnętrzny. Ogólnie infiltracja bierna to śledzenie informacji w pewnym punkcie jej obiegu. Do metod infiltracji biernej należą :

- przechwytywanie elektromagnetyczne,
- dołączanie się do linii transmisji danych,
- badanie i kopiowanie zbiorów niezabezpieczonych,
- analiza makulatury bądź pozostałości na nośnikach,
- ukryte nadajniki,

2.1.1. Przechwytywanie elektromagnetyczne.

Może mieć charakter lokalny. Występuje wówczas, gdy istnieje możliwość dostępu do połączeń pomiedzy jednostką centralną a peryferyjnymi urządzeniami lub terminalami pracującymi w sieci. Możliwe jest także techniczne rozwiązanie polegające na kierunkowej emisji promieniowania i analizie sygnału odbitego od promieniującego komputera. Zasięg tego typu urządzenia oceniany jest obecnie około jednego kilometra (10).

2.1.2. Dołączanie się do linii transmisji danych.

Pozwala na śledzenie przepływającej informacji. Przybiera niepokojące rozmiary w przypadku rozpowszechnienia modemów pracujących na ogólnie dostępnych sieciach telekomunikacyjnych. Możliwe jest również przechwytywanie sygnałów przekazywanych drogą radiową.

2.1.3. Badanie i kopiowanie zbiorów niezabezpieczonych.

Występuje z reguły wtedy, gdy użytkownik ma dostęp do programów i danych, może przeglądać ich zawartość lub kopiować je dla własnych potrzeb. Problem ten występuje najczęściej jako tzw. "piractwo komputerowe", w Polsce obecnie występuje w skali masowej (11).

2.1.4. Analiza makulatury bądź pozostałości na nośnikach informacji.

Ma miejsce w przypadku możliwości dostępu do tabulogramów, wydruków lub używanych uprzednio nośników

---

(10) Zob. Blatchford C.W. "Computer Crime, the need for data Security", Management Services, 1986 Nr 9
Jóźwin M. "Komputer przestepca" , Nowator 1986, Nr 12

(11) Zob. Tomaszewski T. "Kryminalistyczna problematyka przestępczości komputerowej", Problemy kryminalistyki 1980 Nr 143.

informacji. Niefrasobliwość w gospodarce makulatura jest w ośrodkach obliczeniowych nagminna i nawet obcej osobie z zewnątrz nie stwarza żadnego poważniejszego problemu uzyskanie informacji tą drogą. Może wystąpić ze względu na przewidziane normami technologiczne zużycie, ewentualność zakupu nośnika np. dyskietki, na której znajdują się używane wcześniej programy lub zbiory. Wiąże się to z lekceważeniem funkcji zerowania (12). Najczęściej usuwa się zapisane zbiory nie biorąc pod uwagę faktu, że są one możliwa do odzyskania.

2.1.5. Ukryte nadajniki.

To zagadnienie wiąże się z infiltracją pasywną i aktywną. Umieszczony w jakimś punkcie systemu informatycznego nadajnik bądź procedura komunikacyjna może być źródłem uzyskiwania efektów pracy systemu.

2.2. Infiltracja czynna.

To najbardziej niebezpieczne i w największym stopniu mogące zdezorganizować proces przetwarzania danych zagrożenie. Polega głównie na uzyskaniu świadomego dostępu do systemu celem ingerencji w najbardziej wrażliwe i najistotniejsze funkcje. O ile infiltracja pasywna ogranicza się do śledzenia informacji i w zasadzie związane z tym są ogromne nakłady pracy wynikające z przypadkowości uzyskanej informacji, to infiltracja aktywna pozwala na dostanie się do konkretnego miejsca w systemie. Poza tym uzyskanie dostępu do interesującego adresu jest związane z reguły z możliwością dokonania zmian lub wykasowaniem.

Infiltracja aktywna może przybrać następujące formy :

- łamanie zabezpieczeń,
- ingerencja w struktury systemu operacyjnego,
- legalny dostęp do informacji, bez posiadania uprawnienia,
- programy i procedury dodatkowe,
- fizyczne aspekty infiltracji aktywnej,

2.2.1. Łamanie zabezpieczeń.

To zespół czynności wykonywanych w celu dostępu do dowolnego miejsca w systemie informatycznym, pozwalający na ominięcie zabezpieczeń zastosowanych przez legalnego użytkownika systemu. Zagrożenie to może wystąpić zarówno w stosunku do systemu operacyjnego, pamięci, zbiorów jak i nośników informacji.

Wyróżnić możemy w tej grupie :

- dotarcie do macierzy upoważnień lub rejestru zabezpieczeń,
- programowa i sprzętowa analiza zawartości programu lub nośnika,
- stosowanie specjalnych programów narzędziowych,

Łamanie zabezpieczeń popularnie nazywane hackingiem jest

---

(12) Zob. Idźkiewicz A. "Ochrona informacji w procesie przetwarzania", PWE Warszawa 1979.

obecnie zjawiskiem masowo występującym na całym świecie. Zalegalizowane w naszym kraju moralnie z jednej strony przyspiesza rozwój stosowania informatyki, z drugiej pociąga za sobą wykształcenie u poszczególnych osób wysokich kwalifikacji w tej dziedzinie. Szacuje się, że obecnie wszystkie dostępne na zachodzie, najlepiej chronione programy są po upływie już dwóch tygodni odbezpieczone i dostępne w Polsce jako kopie użytkowe (13).

2.2.2. Ingerencja w struktury systemu operacyjnego.

Właściwa jest dla wysokokwalifikowanych informatyków, z reguły projektantów i programistów systemowych. Pozwala na dokładne penetrowanie całego systemu operacyjnego i na dowolne manipulowanie informacją. Wykorzystuje się z reguły typowe słabości systemów operacyjnych i ich błędy funkcjonalne.

2.2.3. Legalny dostęp do informacji, do której nie ma się uprawnienia.

W tym przypadku wykorzystuje się legalne połączenie programowe bądź sprzętowe z komputerem przy użyciu właściwego klucza identyfikacyjnego lub stosownej procedury. Może mieć postać "podszycia się" pod uprawnionego użytkownika.

2.2.4. Programy i procedury dodatkowe.

W infiltracji aktywnej są one najczęściej wykorzystywane do popełniania przestępstw. Umieszczone z reguły w fazie programowania bądź dopisywane w trakcie eksploatacji mogą spowodować załamanie niezawisłości systemu i stosowane są celem osiągnięcia ściśle zamierzonego efektu. Ze względu na możliwość autodestrukcji trudne są do wykrycia i mogą powodować niewyobrażalne wręcz następstwa.

2.2.5. Fizyczne aspekty infiltracji.

Związane są z działalnością intruza w systemie informatycznym, z reguły poza kradzieżą sprzętu, nierozerwalnie dotyczą innych wymienionych form infiltracji aktywnej lub sabotażu.

---

(13) Celem potwierdzenia niniejszego faktu wystarczy sprawdzić dowolną ofertę większej firmy sprzedającej software w naszym kraju. Autor tego typu próby przeprowadzał kilkakrotnie i ani razu nie zawiódł się na krajowym rynku oprogramowania. Interesującym jest fakt, że działalność ta obejmowała dowolne typy programów (od gier do systemów operacyjnych) na wszystkie znane autorowi typy komputerów. Dominowało oczywiście oprogramowanie profesjonalne na mikrokomputery typu IBM.
Por. "Komputerowe piractwo", Słowo Ludu 1987 Nr 5.

3. PRZESTĘPSTWA KOMPUTEROWE.

Termin "przestępczość komputerowa" jest tematem wielu polemik i jest różnie definiowany (14). Zgodnie z definicją N.Visura (15) przyjmijmy, że przestępczosc komputerowa obejmuje wszystkie formy działalności przestępczej, które mają jakikolwiek związek z komputerem. Upraszczając można ten rodzaj przestępczosci podzielić według sposobu popełniania na pośrednią i bezpośrednią przestępczość komputerową.

3.1. Przestępczość komputerowa bezpośrednia.

Celem sprawcy jest sam komputer (rozumiemy pod tym pojęciem zarówno sprzęt jak i software wraz z ideą techniczną). Dokonanie tego typu przestępstwa obejmuje różne czynności, do których zaliczyć należy :

- nieuzasadniony zakup,
- zakup z osiągnieciem nieuzasadnionych korzyści,
- kradzież oprogramowania (kopiowanie),
- kradzież myśli technicznej,
- kradzież informacji,
- kradzież sprzętu,
- kradzież czasu pracy maszyny,
- przemyt,
- sabotaż i dywersja sprzętowo-programowa.

3.1.1. Nieuzasadniony zakup.

Zakwalifikowanie tego rodzaju działalności do grupy przestępstw gospodarczych (Art.217 KK) budzi szereg wątpliwości. Problem występuje głównie w sferze nabywania przez jednostki gospodarcze i administracyjne mikrokomputerów. Na fali mody na mikrokomputery, wyznacznikiem prestiżu nabywcy staje się klasa posiadanego sprzętu, często nieadekwatnego do występujacych w danej jednostce potrzeb. Angażowane są w tym przypadku znaczne kwoty ze społecznych funduszy. Przeprowadzone badania wykazały, że szacunkowo w 16% badanych systemow mikrokomputerowych zakupiona konfiguracja zdecydowanie wykraczała poza zakres potrzeb użytkownika, natomiast w kolejnych 33% zestawy mikrokomputerowe lub pojedyńcze urządzenia zakupione zostały na wyrost. Należy zwrócić uwagę na wykorzystanie nieświadomości decydentów zakupu przez informatyków i ekspertów realizujących bezwzględnie swoje osobiste z reguły finansowe cele i zamierzenia. Kwestia

---

(14) Rozprawa nie obejmuje dyskusji dotyczących problematyki definicji. Zob. Tomaszewski T. "Kryminalistyczna problematyka przestępczosci komputerowej", Problemy kryminalistyki 1980 Nr 143; Kalinowska H. "Terminologia bezpieczeństwa systemów", Prasa Techniczna, 1986 Nr 3.

(15) VISURA L. : Die Computerkriminallitat, "Der Organisator", I. 1987. Szwajcaria.

ewentualnego przeciwdziałania w tej kategorii przestępstw ze względu na znaczne trudności w udowodnieniu winy ciąży na czynnościach profilaktyczno-operacyjnych. Rownoległym problemem jest niewykorzystywanie posiadanego sprzętu, zakupionego dla samego faktu posiadania, z jednoczesnym w konsekwencji dostępem nielicznego grona z bezpośredniego otoczenia decydenta zakupu (18% badanych przypadków).

3.1.2. Zakup z osiągnięciem nieuzasadnionych korzyści.

Ten typ przestępstwa podlega pod artykuł 239 KK, a jest głównie wynikiem występowania silnej konkurencji wśród firm oferujących sprzęt mikrokomputerowy. Ze względu na fakt, że dystrybucją sprzętu w większości zajmują się organizacje z kapitałem zagranicznym lub różnego rodzaju spółki akcyjne rozpowszechnione jest przy zakupie udzielanie decydentowi lub pośrednikowi swoistej prowizji o znacznej wartości, proporcjonalnej z reguły do wartości kontraktu (przyp. autora). Równolegle występuje przypadek oddziaływania na decydentów zakupu sprzętu poprzez osoby na wysokich stanowiskach powiązane z dystrybutorami sprzętu, np. bedącymi akcjonariuszami firm lub spółek. W tej grupie rownież czynniki procesowe są bardzo trudne do zrealizowania i cały ciężar zapobiegania i neutralizacji w zasadzie spoczywa na pionie operacyjnym jednostek resortu spraw wewnętrznych.

3.1.3. Kradzież oprogramowania.

Przestępstwo to, jest jednym z niewielu zjawisk w Polsce usankcjonowanym prawnie, a dotyczy jedynie nielicznych pakietów programowych producentów krajowych (np.CSK). Bezprawne kopiowanie programów, słabość mechanizmów ochronnych implikuje znaczne społeczne zagrożenie jakim jest hamowanie rozwoju rodzimej myśli twórczej w zakresie konstruowania oprogramowania. Plaga "piractwa komputerowego" winna być rozpatrzona w sferze ustawodawstwa i następnie po zakwalifikowaniu prawnym ścigana z urzędu poprzez pion śledczy (16).

3.1.4. Kradzież myśli technicznej.

Rozwój techniki informatycznej w kraju w stosunku do zachodu stoi na stosunkowo niskim poziomie. Tym bardziej nieliczne rozwiązania z tego zakresu podlegać powinny szczególnej ochronie operacyjnej. Tematykę tą obejmują artykuły XIX Rozdziału KK i działania operacyjne wyspecjalizowanych jednostek ochrony przemysłu oraz kontrwywiadu. Prawdopodobna jest ingerencja w środowisko systemów informatycznych wyspecjalizowanych agend wywiadu przemysłowego .

---

(16) HEARNDEN K.:Computer Crime Multi-million Pound Problem "Long Range Planning", X.1986, nr.5 Wlk. Brytania

3.1.5. Kradzież informacji.

Należy ją rozpatrywać jako kradzież dla osiągnięcia osobistych korzyści lub działania na szkodę podstawowych interesów Polski. W pierwszym przypadku zdobyta informacja jest punktem wyjsciowym do zrealizowania innych czynów przestępczych (szantaż, oszustwo, kradzież i.t.p), w drugiej z reguły ma formę szpiegostwa i podlega pod Art.124 KK. Perspektywicznie należy rownież rozpatrzeć mozliwość kradzieży informacji na tle konkurencji miedzy jednostkami gospodarczymi.

3.1.5. Kradzież sprzetu.

Bardzo intratna i opłacalna, głownie ze względu na istniejące mechanizmy rynkowe. Duża liczba jednostek gospodarczych zajmujących się skupem i rozprowadzaniem sprzętu na terenie całego kraju stwarza warunki do eskalacji tego zjawiska. Nie bez znaczenia jest fakt, że przy niewielkich gabarytach i wadze osiąga się znaczne zyski, legalnie sprzedając skradziony sprzęt rozmontowany na części. Daje się zauważyć dobrą orientację przestępców kradnących jednostki centralne, karty i pakiety użytkowe, napędy dyskowe co uniemożliwia praktycznie ich odnalezienie po zainstalowaniu w innych mikrokomputerach. Przykładowo cena sztywnego dysku wielkości kasety video o pojemności 20 MB wynosi około 3 mln zł, a o pojemności 40 MB już około 6 mln zł. Jako forma kradzieży może również wystąpić kidnaping komputerowy (17).

3.1.7. Kradzież czasu pracy komputera.

Przestępstwo to było problemem zasadniczym podczas pracy w dużych ośrodkach obliczeniowych, obecnie zaczyna nabierać coraz większego znaczenia przy wykorzystywaniu mikrokomputerów w zakładach pracy do wykonywania innego typu prac.

3.1.8. Przemyt.

Obejmuje zakres aktualnych zagadnień związanych z przywozem zza granicy całych systemów mikrokomputerowych lub ich części składowych. W przypadku pojedyńczych osób może jedynie wystąpić naruszenie przepisów celno-dewizowych. Jednak liberalna polityka państwa w tym zakresie oraz kolosalne zyski powodują, że cła płacone są z reguły skrupulatnie i powstaje jedynie zagrożenie natury moralnej. Najjaskrawiej przestępstwo przemytu przejawia się przy organizowaniu tego procederu na szeroką skalę poprzez osoby

---

(17) Z banku informacji w poblizu uniwersyteckiego miasta Louvain skradziono 12 płyt pamięci elektronicznej unikatowego komputera COMPEX, za których zwrot złodzieje zażądali 3.5 mln frankow okupu. Por. "Kontrowersje", W Służbie Narodu, 1986 Nr 49.

podstawione lub firmy wysyłkowe. Zysk w tym przypadku jest z reguły sześciokrotny. Przestępstwo to ujmuje Art.135 KK.

3.1.9. Sabotaż i dywersja sprzętowo-programowa.

Biorąc pod uwagę lawinową informatyzację wszystkich dziedzin życia w kraju oraz niefrasobliwość i ignorancję w zakresie ochrony głównie wrażliwych danych stanowi jedno z najbardziej niebezpiecznych przestępstw. Potencjalnie może wystąpić wszędzie, a ze względu na postępujące uzależnianie się pracy bieżącej jednostek od działania informatyki sabotaż bądź dywersja jest w stanie sparaliżować wszystkie, obecnie tak optymistycznie informatyzujące się przedsiębiorstwa i organizacje. Konieczne do zwrócenia szczególnej uwagi, ścigane w ramach Art.127 KK. W tej grupie należy także rozważyc także tło gospodarcze, ekologiczne i osobiste.

3.2. Pośrednia przestępczość komputerowa.

W pośredniej przestępczości komputerowej przestepca wzbogaca się za pomocą komputera lub wykorzystuje go jako środek do działalności przestępczej.

W tej grupie wyróżnimy :

- oszustwa komputerowe,
- wykorzystanie informacji komputerowych,
- symulacja i planowanie działań przestępczych,
- komputer narzędziem porozumiewania się,
- przestępcze systemy informatyczne,

3.2.1. Oszustwo komputerowe.

Dotyczy przypadków gdy sprawca posługując się komputerem aktywnie ingeruje w proces przetwarzania danych celem osiągnięcia nienależnego mu zysku (18). Występuje to z reguły manipulacja informacją rezydującą wewnątrz systemu informatycznego. Na zachodzie problematyka ta występuje w skali masowej, w naszym kraju jest niedostrzegana. Jednak biorąc pod uwagę rozmiary i tempo instalowania systemów informatycznych najbliższą przyszłość może doprowadzić do licznego wystąpienia tego typu przestępstwa. Oszustwa mogą być popełniane przy wprowadzaniu danych do systemu informatycznego dotyczących rachunków, stanu zapasów, komputerowych bądź dane wyjściowe mogą być wykorzystane

---

(18) Przykłady oszustw znaleźć można w pozycjach :
Computerkriminalitat, Kriminalistik, 1984, Nr 12;
Computerkriminalitat : Weniger Falle - Bacher Schaden Kriminalistik, 1984, Nr 1;
Wymann J.J. EDV - Sicherheit in Klein und Mittelbetrieben, Der Organisator, 1987, Nr 1;
HEARNDEN K. Computer Crime Multi - million Pound Problem "Long Range Planning", X.1986, Nr 5

transferow itp. Może mieć miejsce fałszowanie programów niezgodnie z przeznaczeniem. Np. kradzież czekow, niszczenie not itp.

3.2.2. Wykorzystanie informacji komputerowych.

Przy pomocy komputera sprawca może przygotować inne formy przestepstw podobnie jak przy kradzieży informacji, jednak różnica wystepuje w czasokresie trwania. Kradzież z reguły jest przestępstwem jednorazowym, natomiast w przypadku ingerencji w oprogramowanie mamy do czynienia z uzyskiwaniem lub manipulacją w dłuższym okresie czasu i co z tym się wiąże z przestępstwem ciągłym. Istotny jest także aspekt wykorzystania informacji do celów szpiegowskich.

3.2.3. Symulacja i planowanie działań przestępczych.

Może wystąpić przy wykorzystaniu komputera do planowanego przestępstwa, optymalizacji i symulacji działania oraz jego przygotowania. Ujęte w Art.14 KK.

3.2.4. Komputer narzędziem porozumiewania się.

Powszechna informatyzacja oraz coraz liczniejsze grono użytkowników mikrokomputerów domowych stanowi zagrożenie podobnie jak w przypadku symulacji działań przestępczych, bowiem komputer może być środkiem przesyłania informacji. Mogą być one zapisane na nośniku magnetycznym lub przesłane jako modulowany sygnał drogą radiową lub poprzez sieć telefoniczną. Poważne zagrożenie stanowi takie użycie mikrokomputera w przypadku szpiegostwa lub działań antypaństwowych. Zarejestrowano takie przypadki w naszym kraju. Uwagę należy zwrócić również na możliwość wyprowadzenia informacji z dowolnego obiektu siecią telefoniczną w postaci modulowanego sygnału dźwiękowego komputera.

3.2.5. Przestępcze systemy informatyczne.

To potencjalne niebezpieczenstwo może wystąpić z upowszechnieniem się i coraz łatwiejszym dostępem do mikrokomputerów w przypadku grup przestępczych. Aktualnie takie systemy pracują na użytek hackerów, są wykorzystywane do analizy przechwyconego promieniowania komputera śledzonego i mogą być używane do innych celów.

Przestępstwa komputerowe wyróżniają się kilkoma zasadniczymi cechami :

- przestępca nie zawsze musi być obecny na miejscu przestępstwa aby dokonać zaplanowanego czynu,
- kradzież informacji nie pozostawia żadnego materialnego sladu na miejscu przestępstwa,
- dostepność programów narzędziowych oraz skomplikowana struktura pakietów użytkowych uniemożliwia wręcz

udowodnienie kradzieży programu lub danych,
- brak jest przepisów prawnych związanych ze szczegółowym zakwalifikowaniem (19),
- nie istnieją granice przestępstw komputerowych w przypadku popełniania ich w sieci (20),
- upadek systemu lub zniszczenie danych poza z reguły niemożnością dokładnego ich odtworzenia pociąga za soba brak śladów,

4. CHARAKTERYSTYKA GRUP SPRAWCÓW.

Analizie należy poddać grupy sprawców zagrożeń wystepujących w problematyce ochrony systemów informatycznych (21).

4.1. Sprawca kradzieży sprzętu.

Poza wandalem jedyny typ sprawcy, który nie musi być związany z techniką komputerową. Chociaż i w tym przypadku praktyka wykazuje, ze łupem kradzieży rzadko padają cale systemy, natomiast najintratniejszą i najbezpieczniejszą jest kradzież wartościowych podzespołów i części. Do cech pozytywnych dla sprawcy takiej kradzieży zaliczyć należy anonimowość, małe gabaryty i wysoką cenę. Sprawca działa tradycyjnymi metodami stosowanymi przez włamywaczy. Skradzione rzeczy zbywane są na bazarach, giełdach bądź wyspecjalizowanym dystrybutorom sprzętu, którzy elementy montują w kompletnych zestawach mikrokomputerowych przeznaczonych do legalnej sprzedaży. Należy wziąć tu również pod uwagę mozliwość działania przestępczego na zlecenie. Ze względu na skalę i powszechność zjawiska komputeryzacji na terenie całego kraju odnalezienie i odzyskanie skradzionych rzeczy jest wręcz niemożliwe, a wytypowanie i schwytanie sprawcy bardzo trudne. Wspomniano również o ewentualności komputerowego kidnapingu jako szczególnej formie kradzieży komputerowej, w takim przypadku będziemy mieli do czynienia ze złodziejem - kidnaperem.

---

(19) Pierwszą w swiecie Ustawę o Danych wydano w Szwecji w 1973 roku. W niej wprowadzono pojęcie przestępstwa przeciwko danym (data trespass). W 1976 uchwalono w RFN federalną ustawę o ochronie danych.
Zob. Tomaszewski T. op. cit.,

(20) W roku 1985 miały miejsce : włamanie do komputera VAX japonskiego Panstwowego Instytutu Fizyki Wysokich Energii liniami telefonicznymi z terenu RFN oraz kradzież planów konstrukcji najnowocześniejszego silnika do superszybkich pociągów expresowych umieszczonych rownież w pamięci komputerowej przez CIA z terenu Hawaii.
Zob. "Włamanie do japonskiego banku...", Express Wieczorny 1987, Nr 43.

(21) HEARNDEN K. Computer Crime Multi - million Pound Problem "Long Range Planning", X.1986, Nr 5

4.2. Wandal.

Występuje rzadko, jego działalność jest uboczna, gdy wyładowywuje się na jego zdaniem bezwartościowym sprzęcie. Gdy agresje celowo kierunkuje na komputer, motywem z reguły są frustracje i chęć rozładowania się wynikające najczęściej z kompleksu wobec rozwiniętej techniki oraz własnego niedowartościowania. Uwzględnić także należy możliwość sabotażu lub motywy bedące pochodnymi bezrobocia (zwolnienie z pracy).

4.3. Sabotażysta.

Musi mieć dostęp do komputera drogą pośrednią lub bezpośrednią. Działa bez zamiaru osiągniecia materialnego lub informacyjnego zysku na miejscu popełnienia czynu (sabotaż w tzw. "czystej postaci"). Jednak moze działać na zlecenie bądź kierować się pobudkami wyższego rzedu. Należy go szukać wśród politycznych, ekologicznych lub ekonomicznych wrogów systemu. Szczególnie niebezpieczny gdy motywacje jego działania są natury osobistej lub wywodzi się z grona fachowcow sprzetowo-programowych.

4.4. Przemytnik.

Motywacje głownie ekonomiczne. W stosunku do pojedyńczych osób obecnie problem ten występuje na skalę masową. Zakwalifikowanie go do grupy przestępczej bardzo trudne ze wzgledu na opłacalność procederu nawet przy uregulowaniu opłat celnych. Przemyt występuje jako czynność złożoną. W pierwszej fazie inny towar (lub i sprzęt komputerowy) zostaje wywieziony za granicę, tam odsprzedany z zyskiem (z reguły kraje demokraji ludowej), następnie za nabyte tam waluty wymienialne przywożony zostaje sprzęt komputerowy głównie z Tajwanu, Singapuru lub RFN. Często ma również miejsce wysyłanie paczek lub korzystanie z usług firm wysyłkowych. Największe zagrożenie może wystąpić w postaci sprawstwa kierowniczego, przy zorganizowanej na szeroką skalę grupie przemytniczej wykorzystującej osoby podstawione. Może mieć pozory legalności pod szyldem spółki lub firmy skupującej sprzęt.

4.5. Hacker.

Jego zadaniem jest znalezienie sposobu na nieuprawnione wejście do systemu zarówno w sferze sprzętu jak i oprogramowania (22). Początkowo hackerzy nie mieli złych intencji, traktując swoje działanie jako sport lub test na inteligencję, a przestępstwa wynikające z ich działalności miały charakter nieumyślny. Obecnie hacking ma podłoże

---

(22) Hack - to w języku angielskim znęcanie się nad klawiaturą instrumentów w muzyce pop lub na terminalu komputera. Zob. Computerkriminalitat, Kriminalistik, 1984 , Nr 12.

głównie ekonomiczne, ale moze wystąpić przy sabotażu i szpiegostwie w sferze software'u. W Polsce występuje na skalę masową, jest do chwili obecnej zalegalizowany przez państwo - wypożyczalnie programów, firmy świadczące poradnictwo i usługi software'owe. Sprawcę charakteryzuje duża wiedza i praktyka z dziedziny informatyki. Ma dostęp do sprzetu i bogatego oprogramowania narzędziowego (np. programy typu "Super-Hacker", "Hacker-King", monitory dyskowe itp.). Może byc hacker również narzędziem w innych rękach. Pożądane byłoby kwalifikowanie jego działalności jako swoistej formy włamania (23).

4.6. Oszust komputerowy.

Większość tego typu sprawców to pracownicy przedsiębiorstw. Można nawet pokusić się o powiązanie rodzajów przestępstw z rodzajem zatrudnienia. Przestępstwa użytkowników (urzędników, nadzoru i kierowników) polegają prawie wyłącznie na manipulowaniu danymi wejściowymi. Specjaliści komputerowi mają najwiekszą możliwość niewłaściwego wykorzystania komputerów, swoisty monopol fałszowania programów lub danych i popełniaja oni w związku z tym najczęściej przestępstwa związane z danymi wyjściowymi.

4.7. Szpieg.

Z reguły o wysokich kwalifikacjach, wyposażony w doskonały sprzęt możliwy do wszechstronnego wykorzystania. Pole jego działania nieograniczone, realizowane czynności nie pozostawiają śladów. Może atakować systemy w każdym punkcie (24).

Problematyka sprawców przestępstw komputerowych dotyczy dwóch kategorii osób. Pierwsza grupa to ludzie niezwiązani z informatyką, dla których komputer jest bądź przedmiotem przestępstwa, bądź urządzeniem, przy pomocy którego osiągają oni zyski podając mu sfałszowane dane wejsciowe. Druga grupa sprawców to ludzie znający problemy informatyki. Mają oni największe możliwości i największą swobodę działania. Liczne źródła (25), (26) apologizują środowisko informatyków,

---

(23) Jako przykład posłużyć może działalność Klubu CHAOS z RFN. Zob. "19-letni uczeń postrachem producentów komputerów", Echo Dnia, 1988, Nr 54; "Przeniknęli nawet do NASA. Piractwo komputerowe Klubu Chaos z RFN", Echo Dnia, 1988, Nr 53; Safuta Jacek "Komputery, miny i piraci", Slowo Ludu, 1988, Nr 79.

(24) Por. zamieszczone wcześniej wzmianki o kradzieżach na odległość mające miejsce w Japonii, będące faktami szpiegostwa przemysłowego.

(25) Kurt Keidel : Das Informationssystem der Polizei im den USA. "Kriminalistik", nr.12 1969

(26) Braver H.: Forms of Computer Abuse "Revija za kriminalistiko in kriminologijo", nr.2 1982

zaprzeczając możliwości popełnienia przestępstwa wśród tej grupy zawodowej. Jest to stanowisko nieracjonalne i nie mające pokrycia w zaistniałych faktach. Udział w czynach przestępczych osób pracujących przy komputerze wg ankiety prowadzonej przez znany brytyjski koncern komputerowy ICL oceniany jest na 75%. Struktura sprawców przestępstw ulega w chwili obecnej kolosalnym zmianom. W okresie dominacji dużych osrodków obliczeniowych i stosunkowo nielicznej kadry wyspecjalizowanych informatyków popełnianie przestępstw komputerowych nie miało charakteru masowego, a typowanie sprawcy ograniczało się do niewielkiego kregu osób. Rozpowszechnienie mikrokomputerów poza rozproszeniem danych i swobodnym dostępem do sprzetu i oprogramowania doprowadziło do powstania społeczenstwa informatycznego. To co niegdyś było zastrzeżone dla wąskiej grupy osób stało sie udziałem szerokich mas. Na wagę problemu rzutuje również coraz niżej spadająca granica wieku osób bedących perfekcjonistami w sprawach komputeryzacji oraz związane z tym perspektywy na przyszłość. Juz kilkunastoletnie dzieci są sprawcami komputerowych przestępstw, a ich ewentualne dokonania w przyszłości muszą budzić poważne obawy.

5. PODSUMOWANIE.

Zagrożenia, przestępstwa komputerowe i problematyka ich sprawców to zagadnienia nurtujace wszystkich użytkowników komputerów. W miarę rozpowszechniania się i rozrastania obszarów zastosowań systemów informatycznych rośnie równolegle potrzeba na przeciwdziałanie zagrożeniom i przestępstwom komputerowym (27). Przy kompleksowym podejściu do ochrony systemów informatycznych (szczególnie w aspekcie funkcji jednostek resortu spraw wewnętrznych) należy rozważyc system prawodawstwa w tym zakresie oraz charakterystykę grup ewentualnych sprawców (28).

Aby działania w tym zakresie były skuteczne i systemy informatyczne mogły być chronione na wszystkich swoich poziomach istotna jest wiedza o potencjalnych zagrożeniach, o czynach mogących być przestępstwami oraz o osobach je popełniających. W przyszłości mogą powstać jeszcze innego rodzaju przestępstwa komputerowe, pojawić się mogą inne zagrożenia i inni sprawcy mogą byc brani pod uwagę. Mogą być one specyficzne dla poszczególnych państw czy grup użytkowników. Od wiedzy na ich temat będzie zależała ich penalizacja i sposoby ich zwalczania.

W niniejszym rozdziale podjęto próbę w miarę szczegółowego omówienia zzagrożeń i przestępstw, aby utworzyć bazę do dalszych zagadnień związanych z ochroną sysemów informatycznych.

---

(27) Wymann J. J. "EDV - Sicherheit in Klein und Mittelbetrieben", Der Organisator, 1987, Nr 1.

(28) Tomaszewski T. "Kryminalistyczna problematyka przestępczosci komputerowej", Problemy kryminalistyki, 1980, Nr 143.

II. P O Z I O M Y O C H R O N Y .

Rozpatrując ochronę systemów informatycznych w aspekcie funkcji jednostek resortu spraw wewnętrznych należy dokonać analizy na poszczególnych poziomach ochrony.

Rozważmy następujące poziomy ochrony :

- użytkownicy,
- urządzenia zewnętrzne komputera,
- nośniki informacji,
- urządzenia transmisji danych,
- bazy danych,
- systemy operacyjne,

Każdy z nich rozpatrzmy w aspekcie funkcji rozpoznawczych, zapobiegawczych i wykrywczych realizowanych zarówno przez jednostki policyjne jak i jednostki służb specjalnych.

1. UŻYTKOWNICY.

Podział użytkowników systemów informatycznych można przeprowadzić według ich udziału w procesie przetwarzania na pośrednich i bezpośrednich oraz według kwalifikacji informatycznych na biernych i czynnych. Bierni to użytkownicy korzystający z usług systemu lecz nie potrafiący dokonywać zmian, czynni to specjaliści, którym nieobca jest ingerencja do wewnątrz systemu. Newralgiczne miejsca poziomu ochrony jakim są użytkownicy to przede wszystkim motywacje zachowań odrębnych od przyjętych za normalne. Rozpatrzeć należy :

- możliwość osiągnięcia korzyści materialnych,
  - bezpośrednio przy pomocy komputera,
  - pośrednio, jako wynagrodzenie za zrealizowane czynności,
- działanie pod presją, szantażu,
- działanie na podłożu "sportowym",
- działanie na tle politycznym lub ekologicznym,
- działania na tle osobistym,

Użytkownik pośredni to użytkownik, który korzysta z usług komputera bez bezpośredniego dostępu do niego. Zwrócić należy uwagę jedynie na możliwość manipulacji przygotowywanymi danymi wejściowymi. Użytkownik bezpośredni ma kontakt osobisty z komputerem, stąd zawsze należy domniemywać, że jest jednocześnie użytkownikiem czynnym i może stać się potencjalnym intruzem systemu. Specyficzną i konieczną do poddania analizie grupą użytkowników jest personel obsługujący komputer. Omówmy obsadę typowego ośrodka informatyki (29) na poszczególnych stanowiskach w aspekcie ochrony systemów informatycznych według następujących grup tematycznych :

---

(29) Informatyka - poradnik dla ekonomistów. Pod redakcją E. Niedzielskiej. PWE Warszawa 1977

Aspekt operacyjno-rozpoznawczy;
a.- dostęp do poszczególnych punktów systemu,
b.- możliwość wywołania zagrożenia,
c.- ocena potencjalnie posiadanej wiedzy (30),
d.- ocena przydatności w charakterze osobowego źródła informacji,
e.- ocena przydatności jako konsultanta i biegłego,
Aspekt dochodzeniowo-śledczy;
f.- możliwość popełnienia przestępstwa,
g.- kwalifikacja pod kątem grup sprawców,
h.- ocena przydatności w charakterze świadka,
Uwagi w aspekcie zadań służb specjalnych;
i.- konieczność objęcia ochroną operacyjną (31),

Wybrane stanowiska w ośrodku obliczeniowym :

1.1. Członek kierownictwa.

a. Dostęp praktycznie do każdego punktu systemu i wszystkich parametrów uzbrajających. W zależności od specjalności zawodowej i rodzaju pracy możliwość ingerencji do wnętrza systemu .
b. Każde zagrożenie potencjalnie możliwe do wywołania, łącznie z ukrywaniem jego wystąpienia. Poza tym możliwość manipulacji decyzją, tak aby przy zachowaniu legalności i uzasadnionych podstawach można było osiągnąć zamierzony skutek. Bezpośrednia ingerencja wewnątrz maszyny mało prawdopodobna ze względu na możliwość zwrócenia na siebie uwagi. Natomiast optymalne sprawstwo kierownicze jako sterownika poczynań innych.
c. Wiedza w zależności od wykształcenia, jednak dodatkowo możliwość skorzystania z wiedzy podległych pracowników bez podania im w takim przypadku motywów.
d. Niewygodny jako osobowe źródło informacji zarówno po pionie policyjnym jak i służb specjalnych.
e. Jako konsultant bezwartościowy głównie z uwagi na fakt konieczności ochrony własnego interesu. Jako biegły również nie zalecany z uwagi na fakt zbyt rozproszonej, konkretnej wiedzy.
f. Należy zwrócić szczególną uwagę na nieuzasadniony zakup, zakup z osiągnięciem nieuzasadnionych korzyści i oszustwo komputerowe.
g. Potencjalne działanie w charakterze oszusta komputerowego z uwzględnieniem możliwości sprawcy kierowniczego.
h. Jako świadek nieobiektywny z uwagi na ochronę własnego interesu oraz tendencje do zbyt pozytywnego przedstawiania ogólnego obrazu kierowanej przez siebie placówki.

---

(30) Konieczne jest zwrócenie uwagi zarówno na wiedzę teoretyczną, (wyuczoną) jak i praktyczną, pozwalającą na wykonywanie różnych nieoczekiwanych czynności n.p. dostęp do systemu operacyjnego itp.
(31) Oczywiście w zależnosci od konkretnych potrzeb i stopnia wrażliwości systemu informatycznego.

i. Ochrona operacyjna musi być wielopłaszczyznowa celem uzyskania pełnego obrazu sylwetki moralno-zawodowej i ewentualnego oddziaływania operacyjnego. Ze względu na mozliwości wyjazdów za granicę i - szerokie kontakty osobiste ewentualność ochrony o charakterze kontrwywiadowczym z uwzględnieniem ochrony przed szpiegostwem gospodarczym.

1.2. Programista systemowy.

a. Ze względu na olbrzymią z reguły wiedzę, praktykę i dostęp do systemu operacyjnego ma możliwość pasywnego uzyskiwania każdej informacji oraz możliwość aktywnych zmian pracy czynności systemowych.
b. Główne zagrożenie to zneutralizowanie zabezpieczeń, dopisanie wejść lub ujawnienie zabezpieczeń. Jego działania są niewykrywalne i mogą być zrealizowane w dowolnym czasie pracy systemu.
c. W temacie funkcjonowania systemu informatycznego wiedza olbrzymia a potencjalne jej wykorzystanie zależne od praktyki.
d. Jako osobowe zródlo informacji nieoceniony, głównie ze względu na aspekt operacyjnego korzystania z usług systemu oraz zdobycia parametrow uzbrajających lub konkretnych danych.
e. Z uwagi na rozległą wiedzę pożądany i przydatny jako konsultant i biegły.
f. Potencjalny sprawca kradzieży wszystkich składowych software'u, wszystkich form sabotażu i oszustwa komputerowego.
g. Doskonały hacker, sabotażysta software'owy oraz oszust komputerowy.
h. Ze względu na wysoką specjalizację z reguły mało komunikatywny i trudny do przesłuchania. Żyje poza swiatem rzeczywistym stąd konieczność ostrożnego oceniania jego relacji.
i. Ochrona operacyjna bezwzględnie konieczna głównie pod kątem psychiki i akceptowalności warunków w jakich pracuje.

1.3. Operator.

a. Dostęp do większości zadań systemowych, utrudniony w przypadku rejestracji czynności. Wiedza o większości parametrów uzbrajających oraz kontakt z danymi wyjściowymi.
b. Manipulacja systemem operacyjnym lub pakietami, ujawnienie zabezpieczeń . Manipulacja informacją w wiekszości punktów procesu przetwarzania.
c. W zaleznosci od wykształcenia i przeszłej praktyki, jednak z reguły wiedza nie za wielka.
d. Z punktu widzenia ochrony systemów informatycznych zasadność pozyskania go w charakterze osobowego źródła informacji przeciętna.
e. Jako konsultant i biegły nieprzydatny.

f. Może wystąpić przy kradzieży oprogramowania lub informacji, a także przy oszustwie komputerowym wykorzystując znane mu dane wyjściowe.
g. Może być sabotażystą lub oszustem.
h. Jako świadek posiada rozeznanie o pracy bieżącej systemu i ewentualnych odchyleniach od normalnej procedury.
i. Objęcie ochroną operacyjną jedynie w przypadku obsługi wrażliwych systemów.

1.4. Konserwator.

a. Tak zwana "szara eminencja" systemu. W aktualnych warunkach w naszym kraju jedyny człowiek o wszechstronnym dostępie i możliwościach zarówno w aspekcie sprzętowym jak i z reguły programowym. Badania wykazały, że 76% konserwatorow to osoby mogące zrealizować wszystkie zamierzenia w stosunku do systemu.
b. Zagrożenia to wyłaczenie urządzeń ochrony, użycie niewspółdzialajacych z systemem programów pomocniczych i urzadzeń realizujacych dodatkowe procesy współbieżne.
c. Z reguły bez względu na wykształcenie ogromna wiedza oparta na praktyce.
d. Pożądany jako osobowe źródło informacji, szczególnie w przypadku ewentualności zastosowania techniki operacyjnej i operacyjnego dotarcia do konkretnych punktów systemu.
e. Doskonały jako konsultant i biegły.
f. Może skraść każdy z elementów systemu łacznie ze sprzętem bez zwrócenia szczególnej uwagi.
g. Moze wystąpić jako hacker, oszust i sabotażysta.
h. Jako swiadek szczególnie przydatny z uwagi na doskonałą, znajomość praktyczną wszystkich punktów systemu.
i. Bezwzględnie konieczna ochrona operacyjna ze szczególnym uwzględnieniem możliwości dotarcia do systemów w innych ośrodkach. Należy wziąć pod uwagę ewentualność "zaminowania" systemu oraz w koniecznych przypadkach objąć zainteresowaniem operacyjnym.

1.5. Projektant i programista.

a. Dostęp swobodny nieco ograniczony, ale przy znajomości struktur systemowych potencjalna mozliwość rozbicia blokad i swobodnego "buszowania" po systemie. Naturalna programowa ingerencja w system.
b. Subtelne modyfikacje oprogramowania, możliwość manipulacji danymi i dużymi sektorami pracy systemu. Ewentualność programowego "zaminowania" systemu.
c. Z reguły spora ale wyspecjalizowana w dosyć wąskim zakresie.
d. Biorąc pod uwagę wyspecjalizowanie w pracy niespecjalnie pożądany jako osobowe źródlo informacji.
e. Jako konsultant lub biegły nadaje się jedynie w wąskim przez siebie opanowanym zakresie.
f. Może popełnić programowe oszustwo komputerowe oraz sabotaż np. w postaci "miny software'owej".

g. Potencjalny hacker, oszust i sabotażysta programowy.
h. Jako świadek przydatny przy wyjaśnianiu zawiłości progamowych.
i. Bez specjalnego typowania ochrona operacyjna niekonieczna.

1.6. Pracownik we/wy komputera i administracji.

a. Dostęp do systemu wąski, ograniczony, brak możliwości ingerencji w niezawisłość.
b. Moze wystąpić celowe przekłamanie lub falszowanie danych wprowadzanych, wykorzystanie niezgodnie z przeznaczeniem danych wyjściowych, oraz celowe ukrycie innych, szerszych z punktu widzenia informatycznego umiejętności. W takim przypadku może mieć charakter intruza przypadkowego lub podszywającego się.
c. W normalnych warunkach wiedza o systemie szczątkowa.
d. Jako osobowe źródło informacji mało przydatne.
e. Bezzasadne rozpatrywanie jako konsultanta lub biegłego.
f. Może wystąpić oszustwo komputerowe głównie na bazie manipulacji danymi wejściowymi lub wykorzystaniu wyjściowymi oraz sabotaż.
g. Konsekwentnie może byc oszustem lub sabotażystą.
h. Jako świadek na normalnych zasadach.
i. Ochrona operacyjna bezzasadna.

1.7. Personel mikrokomputera.

Odrębne podejście do problemu użytkownika-personelu pojawia się w sferze wykorzystania systemów mikrokomputerowych. Personel jest w zasadzie kilkuosobowy, a prawie każdy użytkownik (rozpatrujemy personel kwalifikowany) jest specjalistą, mogącym być wyposażonym w bardzo wyrafinowane narzędzia (32). Według podanych grup tematycznych ocena jest nastepująca :

a. Osoby odpowiedzialne za prace systemu mikrokomputerowego ze względu na znajomość tematu i zakres oraz skuteczność programów narzędziowych mają w zasadzie dostęp do każdego bitu informacji i do każdej danej.
b. Może wystąpić każde z zagrożeń, od kradzieży sprzętu połaczonej z zamianą poprzez ingerencje w pakiety i programy do swobodnego manipulowania informacją. Efekt zagrożenia w większości przypadków może pozostać niezauważony.
c. Wiedza różnorodna, jednak istotne jest to, że przy współczesnych programach narzędziowych i łatwosci ich obsługi głęboka wiedza informatyczna nie jest konieczna.
d. Jako osobowe źródlo informacji pożądane, szczególnie

---

(32) Kleiber M. Szuniewicz R. "Komputer osobisty typu IBM PC. Możliwości zastosowań profesjonalnych", PWN Warszawa 1988;
Madej D. Marasek K. Kurylowicz K. "Komputery osobiste", WKiŁ Warszawa 1987.

w przypadku konieczności infiltracji systemu przez stosowne jednostki resortu spraw wewnętrznych.

e. W charakterze konsultanta lub biegłego przydatny w zależności od stopnia opanowania wiedzy i posiadanej praktyki.

f. Wszystkie typy przestępstwa możliwe do popełnienia, przy nieuzasadnionym zakupie lub zakupie z osiągnięciem nieuzasadnionych korzyści z reguły rola konsultanta zasadności zakupu.

g. Możliwość zakwalifikowania do każdej grupy sprawców przestępstw.

h. Podczas przesłuchania w charakterze świadka należy zwrócić uwagę na osobisty stosunek do systemu oraz udział własny w tworzeniu oprogramowania i funkcjonowanie systemu - może to implikować duży stopień subiektywizmu w składanych zeznaniach.

i. Pozyskanie w charakterze osobowego źródła informacji pożądane lub konieczne w zależności od potrzeb.

2. URZĄDZENIA ZEWNĘTRZNE KOMPUTERA.

Do urządzeń zewnętrznych komputera (33) w systemach informatycznych zaliczymy :

› Urządzenia wejścia przygotowywujące dla potrzeb procesu przetwarzania danych informacje w postaci zrozumiałej przez komputer :
  - dziurkarki i czytniki taśm i kart perforowanych,
  - zestawy wprowadzania danych na nośnik magnetyczny,
  - rejestratory sygnałów,

› Urządzenia wyjścia przedstawiające informacje wynikową w formie czytelnej dla użytkownika :
  - drukarki,
  - plotery,
  - sterowniki,

› Urządzenia będące zewnętrznymi pamięciami komputera :
  - o dostępie sekwencyjnym - przewijaki taśm,
    - magnetofony kasetowe,
    - streamery,
  - o dostępie swobodnym - pamięci dyskowe,
    - pamięci bębnowe,
    - napędy dysków stałych,
    - napędy dysków miekkich,
    - inne pamieci (np.optyczne),

› Urządzenia konwersacji stanowiące bezpośrednią komunikację z komputerem :

  - stanowisko operatora,

---

(33) Por. Flores I. "Urządzenia zewnętrzne komputerów", WNT Warszawa 1979.

- terminale,
- monitory,
- urządzenia specjalne (klawiatura, mysz, joystick itp.)

) Gniazda – mikrokomputera wraz z software'owym lub hardware'owym interfejsem :

- szeregowe,
- równolegle,
- specjalne,

Rozważmy wymienione grupy według następujących problemów :

A. Charakterystyka.
B. Punkty newralgiczne.
C. Zagrożenia.

2.1. Urządzenia wejscia.

A. Charakteryzuje je jednokierunkowy przepływ informacji od dokumentu źródłowego poprzez nośnik informacji do komputera. Dokumentem źródłowym może być grupa danych spisanych z faktury, kwestionariusza itp., program w dowolnym języku lub ciąg impulsów charakteryzujących wielkość parametrów rejestrowanych przez komputer.

B. Punktami newralgicznymi są :
- dane na wejściu urządzenia,
- proces przetwarzania na urządzeniu,
- nośniki,
- linie przesyłu informacji,

C. Zagrożenie jakie głównie może wystąpić to sfałszowanie danych przed wprowadzeniem ich lub w trakcie transponowania na postać przeznaczoną dla komputera. Może mieć formę bierną – podanie nieprawdziwego obrazu rzeczywistości lub formę czynną, będącą ingerencją w oprogramowanie celem ugodzenia w niezawisłość systemu. Należy również uwzględnić potencjalne zaminowanie systemu w tych punktach, podsłuch lub przeglądanie danych z możliwością sporządzenia kopii.

2.2. Urządzenia wyjścia.

A. Podobnie jak omówione wyżej charakteryzują się jednostronnym przepływem informacji, tym razem z komputera na zewnątrz.

B. Punkty newralgiczne to :
- informacja wynikowa,
- sterowniki wykonujące polecenia komputera,

C. Zagrożenia w tym przypadku są następujące :
- możliwość zamiany wynikowych danych bądź na

przygotowane wcześniej bądź w formie korekty, w celu przedstawienia fałszywego obrazu rzeczywistości i osiągnięcia innych, wcześniej zamierzonych celów,
- atak na informacje wyjściową, sterującą pracującymi z reguły w czasie rzeczywistym i regulującymi wartości sterowników oraz uruchamiającymi konkretne akcje (np. system ochrony przeciwpożarowej itp.),

2.3. Pamięci zewnętrzne.

A. Są to urządzenia do gromadzenia informacji i programów potrzebnych w procesie przetwarzania. Charakteryzuje je z reguły wymienny nośnik informacji.

B. Punkty newralgiczne :
- nośnik,
- podzespoły elektroniczne,

C. W przypadku pamięci mikrokomputerowych stają się one często ze względu na ich dużą wartość przedmiotem kradzieży, poza tym ich podzespoły elektroniczne są doskonałym miejscem do zainstalowania urządzenia podsłuchowego lub miny hardware'owej.

2.4. Urządzenia konwersacji.

A. Są to urządzenia do kontaktowania się i konwersacji z komputerem. Składają się one z reguły z klawiatury alfanumerycznej lub wyspecjalizowanej i sprzętu przekazującego komunikaty komputera (drukarka lub częściej monitor ekranowy). Główną cechą jest bezpośredni, dwustronny kontakt z komputerem i dostęp do jego programów i zasobów. W przypadku mikrokomputera klawiatura, jednostka centralna i monitor stanowią z reguły integralną całość.

B. Jako punkt newralgiczny należy wziąć pod uwagę całe urządzenie, a jego zdolność do komunikacji bezpośredniej komputerem i jego zasobami predystynuje go do miana najwrażliwszych elementów systemu.

C. Zagrożenia.
- kradzież fizyczna (klawiatura i mikroprocesor),
- podsłuch i przeglądanie,
- infiltracja aktywna celem uzyskania dostępu do danych lub ingerencji w struktury programowe,
- zaminowanie,

Urządzenia specjalne są formą urządzeń konwersacyjnych, bezpieczniejszymi z uwagi na ograniczoność kontaktu z komputerem.

2.5. Gniazda mikrokomputera.

A. Są to miejsca dostępu do systemu informatycznego jakim jest mikrokomputer. W większości to łącza aktywne czyli

wysyłające i przyjmujące informacje. Najpopularniejsze to : - łącze szeregowe RS -232,
- łącze równolegle Centronics,

B. Same w sobie są miejscem newralgicznym ze względu na potencjalny dostęp do wnętrza systemu będący atakiem niestandartowym.

C. Zagrożeniem jest wykorzystanie gniazda do aktywnej ingerencji w strukturę systemu, zmianę jego wewnętrznej funkcji oraz dostęp do przetwarzanych programów i danych.

Analogicznie należy rozpatrzeć gniazda kart mikrokomputerowych.

3. NOŚNIKI INFORMACJI.

Będą z reguły efektem wynikowej pracy urządzeń pamięci zewnętrznych komputera lub integralnymi zespołami elektronicznymi (34). Można je podzielić na :
- nośniki z dostępem sekwencyjnym :
  - taśmy magnetyczne,
  - kasete magnetofonowe,
  - kasety streamera,
- nośniki z dostępem swobodnym :
  - pakiety dyskowe,
  - dyskietki,
  - wymienne sztywne dyski,
  - karty,

Nośniki informacji mogą stać się przedmiotem kradzieży fizycznej lub obiektem manipulacji. Można je z reguły bez większego problemu skopiować i to poza ich właściwym systemem komputerowym, głównie ze względu na ich niewielkie rozmiary i ogólna typizacje. Ponadto po rozbrojeniu wewnętrznych zabezpieczeń można penetrować zapisane na nich dane oraz nanieść inne godzące w niezawisłość (35) macierzystego systemu. Mogą również służyć jako pomoc przy ataku na system informatyczny zawierając programy destrukcyjne lub narzędziowe. W przypadku kart możliwe jest zastosowanie dodatkowych, wypełniających specjalne funkcje urządzeń elektronicznych. Jako przykład mogą posłużyć software'owe i hardware'owe wirusy komputerowe (36).

---

(34) Nowak E. Sawicki Z. "Pamięci maszyn cyfrowych" WNT Warszawa 1987.

(35) Przez niezawisłość systemu w niniejszej rozprawie rozumieć będziemy realizacje przez system tylko tych funkcji , których realizacja przez niego jest oczekiwana bez żadnych innych dodatkowych nie zaplanowanych przez uprawnionego do korzystania z systemu użytkownika.

(36) Majewski Władysław : "Wirusowa gorączka" Komputer 1988 Nr 11.

4. URZĄDZENIA TRANSMISJI DANYCH.

Transmisja danych to dział telekomunikacji, obejmujący przekazywanie odpowiednich sygnałów elektrycznych (informacji) od maszyny do maszyny jako aparatów przetwórczych (37). Elementami składowymi konfiguracji systemów transmisji danych będą :

- urządzenia sterowania transmisją,
- linie telekomunikacyjne,
- teledatory,

4.1. Urządzenia sterowania transmisją.

Zapewniają realizację transmisji w dowolnej wymaganej chwili oraz umożliwiają zwielokrotnienie kanału, przez który dane są wprowadzane do komputera. Zaliczymy do nich multipleksery, selektory i procesory komunikacyjne (np.karty sieciowe). Funkcje multipleksorów i selektorów są podobne i polegają na sterowaniu operacjami wejścia i wyjścia oraz na transmisji danych między teledatorami i pamięcią operacyjną komputera. Zadaniem procesora telekomunikacyjnego jest odciążenie procesora centralnego od funkcji związanych ze sterowaniem transmisją i przyjmowaniem komunikatów od wielu odległych urządzeń. Zagrożenia jakie mogą się pojawić

w urządzeniach sterowania transmisją to przede wszystkim manipulacja parametrami sterowania, podłączenie nieupoważnionego kanału celem podsłuchu lub aktywnej ingerencji w system informatyczny, a także podłączenie się do linii transmisji tak aby można było wprowadzać fałszywe lub wyprowadzać pożądane dane.

4.2. Linie telekomunikacyjne.

Realizacja procesu transmisji odbywa się w linii telekomunikacyjnej, określanej również mianem łącza transmisji danych.

Składa się ona z nadajnika, łącza telekomunikacyjnego i odbiornika , przy czym nadajnik i odbiornik mogą być fizycznie tym samym urządzeniem. Atak może nastąpić na każdym odcinku linii telekomunikacyjnej. Może on mieć formę podsłuchu, przesłuchu, detekcji promieniowania oraz ingerencji elektronicznej polegającej na zamontowaniu dodatkowych urządzeń w odbiorniku lub nadajniku. Może wystąpić podłączenie się do linii celem zamarkowania uprawnionej końcówki lub próby aktywnego wdarcia się do systemu. Należy rozpatrzeć również fakt, że łącze telekomunikacyjne może być łączem radiowym.

---

(37) Informatyka – poradnik dla ekonomistów. Pod redakcją E. Niedzielskiej. PWE Warszawa 1977.
Baran Z. "Problemy transmisji danych" WKiŁ Warszawa 1977.

4.3. Teledatory.

Tym pojęciem określa się szeroki wachlarz urządzeń końcowych, które służą do wprowadzania i wyprowadzania danych u użytkownika. Mogą być nimi autonomiczne systemy informatyczne lub urządzenia omawiane już w punkcie 4.2. Ważne jest zwrócenie uwagi na fakt, że teledatorem może być mikrokomputer.

Godnym zwrócenia uwagi jest fakt, że coraz częściej rolę sieci transmisji danych pełnią linie telefoniczne i telegraficzne, co wzmaga zagrożenie na odcinku ewentualnego dostępu i ingerencji.

5. BAZY DANYCH.

5.1. Charakterystyka.

Bazę danych można zdefiniować jako zbiór wzajemnie powiązanych danych pamiętanych bez zbędnej redundacji, służących jednemu lub wielu zastosowaniom w sposób optymalny. Dane pamiętane są w taki sposób, że są niezależne od programów, które z nich korzystają. Przy dołączaniu i modyfikacji oraz wyszukiwaniu danych stosuje się wspólną metodę umożliwiającą sprawdzenie poprawności wykonywanych operacji. System zawiera zbiór baz danych, jeśli są one całkowicie rozłączne pod względem struktury (38).

Wśród wielu rodzajów baz danych wymienić należy : kartotekowe, relacyjne, hierarchiczne, sieciowe i inne. W aspekcie ochrony systemów informatycznych analizą objąć należy trzy czynniki :

- usytuowanie bazy danych,
- dostęp do bazy danych,
- możliwość manipulacji jej zawartością,

5.1.1. Usytuowanie bazy danych.

Związane jest z fizycznym przechowywaniem jej na nośnikach informacji i to z reguły w postaci co najmniej zdublowanej. W przypadku dużych komputerów mamy do czynienia z bazą danych rezydującą na pakietach dyskowych z rezerwowym zbiorem na taśmie magnetycznej. Bazy danych wykorzystywane przez mikrokomputer ulokowane są najczęściej na dysku sztywnym z rezerwą na dyskietkach lub taśmie magnetycznej

---

(38) Martin J. "Organizacja baz danych", PWN Warszawa 1983.
Date C. J. "Wprowadzenie do baz danych", WNT Warszawa 1981.
Olesinski J. Staniszkis W. "Projektowanie baz danych" PWE Warszawa 1984.
Yourdon E. "Projektowanie systemów o działaniu bezpośrednim", WNT Warszawa 1976.

przewijaka lub streamera.

5.1.2. Dostęp do bazy danych.

Przede wszystkim to dostęp za pośrednictwem systemu operacyjnego komputera, ktory daną bazę danych obsługuje i wykorzystuje. Jednakże istnieje również manualny, fizyczny dostęp do nośników informacji, na których bazy danych są przechowywane.

5.1.3. Możliwosc manipulacji zawartością bazy danych.

Warunkuje ją w zasadzie system operacyjny podczas realizacji standartowych funkcji. Możliwa jest rownież ingerencja w zbiory bazy danych przechowywane na nośnikach. W przypadku mikrokomputera mogą wystąpić autonomiczne bazy danych z pełna ofertą manipulacji lub wykreowane pod programem narzędziowym bazy wymagające do zmian rezydującego programu narzędziowego.

5.2. Punkty newralgiczne baz danych.

Zaliczyć do nich możemy :

- komunikacja z systemem operacyjnym,
- nośnik informacji, szczególnie kopia awaryjna,
- organizacja bazy danych,

5.3. Zagrożenia.

Do najważniejszych należą :

- kradzież bazy danych wraz z nośnikiem na którym jest zapisana, bądź przekopiowanie jej na inny nośnik,
- ewentualność zniszczenia,
- infiltracja aktywna po złamaniu zabezpieczeń lub zmiania parametrów macierzy dostępu, z reguły poprzez system operacyjny,

5.4. Zasady ochrony baz danych.

Wymieńmy podstawowe zasady ochrony baz danych, które powinny obowiązywac powszechnie :
- informacje (dane) należy traktować jako potrzebne do określonego celu i nie można ich używać do celów innych bez odpowiedniego zezwolenia,
- dostęp do informacji (danych) powinien byc ograniczony do osób upoważnionych do ich posiadania w celu w którym je zgromadzono,
- zakres zebranej i przechowywanej informacji należy ograniczyć do niezbędnego minimum, koniecznego do zaspokojenia określonej potrzeby,
- w projektach i programach systemów informatycznych przetwarzających informacje powinny być zawarte właściwe zabezpieczenia dla oddzielenia informacji osobowych

(wrażliwych) od reszty danych,
- są potrzebne zarządzenia na mocy których osoba (organizacja) mogłaby być zapoznawana z dotyczącą jej informacją,
- istniejące w systemie środki ochrony powinny być wcześniej określone przez użytkownika i powinny obejmować metody zapobiegające rozmyślnemu nadużyciu lub niewłaściwemu użyciu informacji,
- należy przewidzieć system sygnalizowania ułatwiający wykrywanie dowolnego naruszania systemu ochrony,
- w projektowaniu systemów informatycznych należy podać okres, poza którym informacja nie powinna być przechowywana,
- dane powinny być ścisłe (poprawne), należy przewidzieć mechanizm korygowania i uaktualniania informacji,
- szczególna uwagę należy zwrócić na kodowanie (szyfrowanie) danych szczególnie wrażliwych (39),

6. SYSTEMY OPERACYJNE.

Termin system operacyjny oznacza te moduły programowe w obrębie systemu informatycznego, które rządzą sterowaniem zasobami sprzętowymi takimi jak procesory, pamięć operacyjna, pamięć zewnętrzna, urządzenia wejścia/wyjścia oraz plikami. Moduły te rozstrzygają konflikty, próbują optymalizować działania i upraszczają efektywne wykorzystanie systemu oraz tworzą łącze między programami użytkownika a sprzętem fizycznym komputera (40).

Z powyższej definicji wynika, że system operacyjny to zespół programów (algorytmów) przeznaczonych do zarządzania zasobami systemu, a mianowicie pamięcią, procesorami, urządzeniami i informacją, (programami i danymi). Wszystkie z zasobów są cenne i zadaniem systemu operacyjnego jest dążenie do efektywnego ich wykorzystania, jak również rozwiązywania konfliktów wynikających ze współzawodnictwa między różnymi użytkownikami.

System operacyjny musi śledzić stan każdego zasobu, decydować o tym, który proces powinien otrzymać zasób (ile i kiedy), przydzielić go i ewentualnie żądać jego zwrotu.

Rozpatrując system operacyjny jako zarządcę zasobów stwierdzamy, że musi on :

- śledzić zasoby systemu,
- narzucać strategię, która określa odbiorcę, rodzaj zasobu, moment przydziału i ilość zasobu,
- przydzielać zasób,
- odzyskiwać zasób,
- chronić zasób,

Systemy operacyjne to owoc wieloletniej pracy

---

(39) Por. Naur P. "Zarys metod informatyki", WNT Warszawa 1979.

(40) Madnick S.E. Donowan J.J. "Systemy operacyjne" PWN Warszawa 1983.

wieloosobowych zespołów wysokokwalifikowanych specjalistów. Z reguły wszystkie posiadają mniej czy bardziej rozbudowane mechanizmy ochrony (41), a problematyka ich błędów funkcjonalnych czy miejsc newralgicznych wykracza poza ramy niniejszej pracy (42).

7.PODSUMOWANIE

Perspektywy dalszego rozwoju stosowania systemów informatycznych wskazuja na olbrzymią powszechność i życzliwość w stosunku do każdego użytkownika. Postęp techniczny w dziedzinie informatyki jest olbrzymi. Pojawianie się nowych rozwiązań zarówno w obszarze software'u jak i hardware'u implikuje uaktualnianie wiedzy na bieżąco. By można było dbać o ochronę systemów informatycznych szczególnie w aspekcie funkcji jednostek resortu spraw wewnętrznych należy bezwzględnie rozpatrzeć wszystkie możliwie poziomy ochrony zarówno pod kątem ich architektury jak i mogących wystąpić zagrożeń. Dużą uwagę należy poswięcić także najważniejszemu a zarazem najsłabszemu ogniwu systemu ochrony jakim jest człowiek. Biorąc pod uwagę stale zmieniające się elementy systemu informatycznego w niniejszym rozdziale dokonano przeglądu większości poziomów ochrony co może stanowić bazę do stosowania metod i przedsięwzięcia stosownych środków ochrony.

---

(41) Głowacki M. "Systemy operacyjne DOS i OS" WNT Warszawa 1982.
Hansen P.B. "Podstawy systemów operacyjnych" WNT Warszawa 1979.
Liebiediew W.N. Sokołow A.P. "System operacyjny OS JS. Podstawy użytkowania." PWE Warszawa 1982.
Shaw A.C. "Projektowanie logiczne systemów operacyjnych", WNT Warszawa 1980.
Borak S. Klaczak J. "System operacyjny George 3" WNT Warszawa 1981.
Piotrowski A. "Ukryte gwiazdy - systemy operacyjne", Mikroklan 1986 Nr 2.
(42) Hofman L.J. "Poufność w systemach informatycznych" WNT Warszawa 1982.

III. METODY OCHRONY.

Metoda to zespół czynności i środków użytych dla osiągnięcia celu. W niniejszym przypadku to stosowanie zabezpieczeń i wykonywanie czynności ochronnych w celu zapobieżenia lub zminimalizowania skutków zagrożeń godzących w niezawisłość systemu. Wielu autorów stosuje sztuczne podziały uzależnione od różnego rodzaju konkretnych rozwiązań technicznych i organizacyjnych. Jest to nieuzasadnione, głównie ze względu na lawinowo postępujący rozwój techniki oraz upowszechnianie się różnego rodzaju wariantów rozwiązań. Niniejsza próba klasyfikacji jest także umowna, głównie ze względu na fakt, że metody prawie nigdy nie występują w czystej formie. Poszczególne zabezpieczenia można zaliczyć do kilku metod naraz, niemniej w niniejszej pracy podjęto próbę zaakcetowania pewnej cechy dominującej w tych metodach.

1. METODY FIZYCZNE.

Przez metody fizyczne będziemy rozumieć stosowanie urządzeń i układów technicznych oraz procedur postępowania w sferze środków fizycznych mających możliwość skutecznego działania przeciwko ingerencji w niezawisłość systemu informatycznego, a także chroniących przed przypadkami zagrożeń. Metody fizyczne rozpatrzmy w trzech grupach :

- identyfikujacej,
- zabezpieczajacej,
- alarmujacej,

trzeba rownież zwrócić uwagę na aspekt operacyjny.

1.1. Metody fizyczne identyfikacyjne.

Mają na celu w sposób selektywny ograniczyć dostęp ludzi i urzadzeń tylko do tych punktów systemu, do których dostęp ten jest uzasadniony, oraz ograniczyć możliwości dostepu nieupoważnionego (43). Sposoby identyfikacji sprowadzają się do trzech podstawowych klas :

- można wykorzystać pewną wiedzę (hasło, numer w zamku elektronicznym),
- zidentyfikować pewną cechę charakterystyczną (kod terminala, obraz siatkowki oka),
- sprawdzić posiadany identyfikator (legitymacja,klucz),

Z pojęciem identyfikacji powiązane jest ściśle uwierzytelnianie i upoważnianie wchodzące z reguły w skład metod programowych.

1.2. Metody fizyczne zabezpieczające.

Są one z reguły nierozerwalnie związane z metodami

---

(43) Por. Curvey C.E. Eaton C.E. "Identyfication of IBM Keypunch Machines by their Printed Products", Journal of Forensic Sciences, 1976 Nr 4.

identyfikacyjnymi, stanowią barierę ograniczającą dostęp do systemów informatycznych i dopuszczają do korzystania z systemu po identyfikacji i uwierzytelnieniu zgodnie z posiadanym upoważnieniem.

1.3. Metody fizyczne alarmujące.

Są one i powinny być uzupełnieniem powyżej wspomnianych metod. W przypadku gdy naruszona zostanie bariera identyfikacyjna, uwierzytelnienia lub upoważnienia metody fizyczne alarmujące uruchamiają stosowne czynności i wszczynają alarm dla zapewnienia bezpieczeństwa.

Do metod fizycznych możemy zaliczyć :

- strażnicy i dozorcy,
- specjalne zamki w drzwiach i urządzeniach,
- szafy pancerne,
- plomby,
- systemy alarmowe,
- system telewizji przemysłowej,
- fotokomorki,
- czujniki,
- urządzenia rozpoznające (np. głos, linie papilarne itp.),
- przeciwpodsłuchowe generatory szumów,
- urządzenia kryptograficzne,
- inne (44),

1.4. Aspekt operacyjny.

Zastosowanie metod fizycznych wiąże się z reguły z kosztami, w taki sposób, że ich ilość oraz jakość zależy od wrażliwości danych przetwarzanych przez system. Poza samokontrolą sprawdzanie ich jest konieczne, bowiem z reguły ich funkcjonowanie utrudnia codzienne czynności i występują tendencje do ich omijania. Dla celów operacyjnych metody ochrony fizycznej są doskonałym punktem wyjścia do własnej infiltracji systemu (45). Ewentualna kontrola ich funkcjonowania w ramach szeroko pojętej profilaktyki to baza do zrealizowania własnych celów łącznie z założeniem

---

(44) "Antyszpiegowske okna" , Nauka i Technika" Serwis Zagraniczny PAP. Nr 1453 1988.

(45) Autor ma na myśli fakt, że coraz większa ilość informacji jest lokowana w masowych pamięciach komputerowych. Wiele z tych informacji jest lub będzie niezbędnych dla realizacji rutynowych czynności jednostek resortu spraw wewnętrznych, a ujawnienie faktu o zainteresowaniu nimi może skomplikować lub wręcz udaremnić proces dochodzenia lub śledztwa. Aby uzyskać owe informacje przechowywane przez system drogą operacyjną (np. wykorzystując np. osobowe źródła informacji) niezbędna jest znajomość metod ochrony.

podsłuchu. Obszary stosowania metod fizycznych to najczęściej jedyne miejsca, gdzie wystąpić mogą ślady włamania do systemu bądź innych form infiltracji. Szczególnie ważne jest ich zabezpieczenie w przypadku podejrzenia "ataku" na system.

2. METODY ORGANIZACYJNE.

Metody organizacyjne to określone postępowanie lub zespół czynnosci wykonywanych przez osoby obsługujace i użytkujące system informatyczny w celu jego ochrony. Realizowane są poprzez instrukcje, zarządzenia, rejestry, wykazy, listy, polecenia, przepisy, ewidencje, zakazy itp. W sposób całościowy od wejścia informacji do jej udostępnienia czy reakcji wejściowej ujmują w normy zasady postępowania. Sa w zasadzie powiązane z konkretnym systemem niemniej szereg z nich ma charakter uniwersalny. Do ich zalet należy zaliczyć szeroki zakres oddziaływania, stosunkowo niskie koszty, możliwość szybkiego ich wprowadzenia oraz dużą elastyczność. Wady to mała skuteczność wynikająca z realizacji przez ludzi oraz konieczność okresowego angażowania części personelu.

Metody organizacyjne nierozerwalnie związane są z pojęciem odpowiedzialności. Można wyodrębnić trzy podstawowe reguły : przydział odpowiedzialności, jej podział i rotacja (46).

2.1. Przydział odpowiedzialności.

Odpowiedzialność na każdym etapie przetwarzania danych musi być przydzielana w sposób jednoznaczny, a osoby którym powierzono stosowne zadania winny być swiadome ich realizacji oraz konsekwencji w przypadku zaniedbania obowiązków.

2.2. Podział odpowiedzialności.

Bezwzględnie należy stosować zasadę, ze odpowiedzialność kluczowa zawsze jest ponoszona przez więcej niż jedną osobę lub jednostkę organizacyjną. W tym względzie należy kierować się następujacymi wskazówkami :

- żadnej osobie bez względu na jej kwalifikacje i znaną uczciwość nie wolno powierzać wyłącznej odpowiedzialności za opracowanie większego systemu, w szczególności nikt nie powinien odpowiadać
- nie należy obarczać żadnej osoby (bez nadzoru) odpowiedzialnością za wprowadzenie zmian lub aktualizacją programów,
- operator nie powinien mieć dostępu bezpośredniego do programów lub zbiorów z biblioteki lub katalogu,

---

(46) Idźkiewicz A. : "Ochrona informacji w procesie przetwarzania". PWE Warszawa 1979.

- parametry uzbrajajace metody ochrony software'owej powinny być niedostępne dla osób znajacych kompleksowo architekturę systemu,
- nie powinna mieć w żadnych okolicznościach dostępu do systemu informatycznego jedna osoba,
- system przed eksploatacją powinien zostać poddany badaniu przez kogoś niezaangażowanego w jego opracowanie,
- inspekcja powinna wyrywkowo dokonywać sprawdzania wybranych przez siebie systemów,

2.3. Rotacja odpowiedzialności.

Powinno przestrzegać się nastepujących zasad :
- żaden programista ani projektant nie powinien stale pracować nad tym samym typem prac,
- żaden operator nie powinien regularnie obsługiwac tych samych systemów,
- urlopy powinny być wykorzystane w z góry ustalonych terminach,

Poza powyższym w zakresie metod organizacyjnych należy uwzględnić lad i porządek w systemie informatycznym, prawidłowy obieg dokumentacji, nośników i makulatury, składowanie i wszystko to co jest zwiazane z organizacyjną stroną systemu informatycznego.

Na dzień dzisiejszy metody organizacyjne stanowią najwiekszy procent stosowanych zabezpieczeń. A. Sokołowski podaje (47), że 46% , jednak rozpatruje on systemy informatyczne bez uwzględnienia mikrokomputerów. Szacunkowo należy na podstawie przeprowadzonych badań ocenić stosowanie metod organizacyjnych na 57%. Istotne jest, że w wyniku badań okazało się, że w 32% przewidzianych metod organizacyjnych były one ignorowane z różnych przyczyn. Wyniki uzyskane drogą operacyjną wskazują na lekceważenie bądź celowe pomijanie ich w 68%.

3. METODY KADROWE.

W większości opracowań sa one pomijane lub traktowane marginalnie. Przyjmuje się, ze pracownicy i użytkownicy systemów informatycznych to ludzie uczciwi, ze strony których zagrożenie jest znikome. Polityka kadrowa jako metoda ochrony leży głównie w sferze zainteresowań i kompetencji decydentow systemów informatycznych, polityka kadrowa w naszym kraju od dawna była źródłem wielu problemów. Środowisko ludzi profesjonalnie trudniących się informatyką jest bardzo specyficzne. W większości są to osoby o realnej, wysokiej ocenie własnej wartości, mający w otaczającym środowisku uznanie i o szerokim światopoglądzie. Podczas prowadzonych badań stwierdzono w 72% fascynację zachodem. Równolegle do techniki występował swoisty kult dla kultury. Większość, bo 68% informatyków

---

(47) Zob. Sokołowski Andrzej "Ochrona informacji komputerowych", MON Warszawa 1987.

(łacznie z kadrą kierownicza) była na zachodzie i krytycznie jest nastawiona do innej, jakiejkolwiek rzeczywistości niż tamta. Ludzi informatyki cechuje "komputerowe" podejście do rzeczywistości, powoduje ono odrzucanie kompromisów i całkowita wręcz negacja niekompetencji. Charakterystyczne jest, ze radykalne postawy (chociaż z reguły nie wrogie) są proporcjonalne do fachowości i kategorii danego człowieka. Profesjonaliści informatycy sa z reguły endodynamikami, rzadziej statykami. Egzodynamicy trafiają się stosunkowo rzadko (48). Polityka kadrowa w tego rodzaju społeczności nie jest rzecza najprostszą.

Do metod ochrony w aspekcie kadrowym zaliczymy :
- aktualną wiedzę o nastrojach i stosunkach między pracownikami wraz z natychmiastową reakcją w przypadku jakichkolwiek zaburzeń,
- obsadzanie stanowisk zgodnie z posiadanym wykształceniem, stażem oraz doświadczeniem w aspekcie pracy w zespole,
- prowadzenie w ramach zakładu oceny okresowej pracownika,
- realne rozeznanie w obszarze posiadanej wiedzy i możliwości,
- wiedza o ewentualnych specjalnych predyspozycjach,
- szczegółowa ocena realizacji zleconych zadań,

Aktualne rozpowszechnianie się postaw konsumpcyjnych i pogoni za zyskiem nie ominęło również środowiska informatycznego. Ceny usług w tej sferze sa wysokie i stąd częste przypadki pracy na kilku etatach lub przyjmowanie prac zleconych. Tolerancja przez państwo wielu moralnie zalegalizowanych przestępstw komputerowych (hacking, piractwo) wytwarza niepożądane nawyki mogące niekorzystnie zaowocować w niedalekiej już przyszłości.

Co prawda cały konglomerat problemów polityki kadrowej leży w gestii macierzystej jednostki decydenckiej dla systemu informatycznego lecz w przypadku zaistnienia przestępstwa w tym środowisku lub powstania zagrożeń odpowiednie jednostki resortu spraw wewnetrznych będą musiały wziąć je pod uwagę w realizacji czynności operacyjno-rozpoznawczych lub dochodzeniowo-śledczych.

4. METODY PROGRAMOWE.

To programy, podprogramy, segmenty programów lub etykiety specjalnie opracowane w celu ochrony dostępu do systemu informatycznego przed osobami i urządzeniami nieupoważnionymi oraz nierozważnym postępowaniem personelu lub samych użytkowników. Podobnie jak metody fizyczne rozpatrywać je będziemy w trzech grupach : identyfikacji, uwierzytelnienia i upoważnienia.

---

(48) Por. Białek T. "Cybernetyczny model taktyki wykrywania przestepstw", Departament Szkolenia i Doskonalenia Zawodowego MSW Warszawa 1984

4.1. Ochrona na poziomie systemu operacyjnego.

Metody programowe będą starały się zapobiec zagrożeniom w punktach newralgicznych systemu operacyjnego. Ponieważ system operacyjny jest głównym dysponentem w systemie informatycznym jego zadania w kwestii ochrony są najistotniejsze. Poprzez niego następuje identyfikacja zarówno użytkowników jak i urządzeń zewnętrznych. On uwierzytelnia je i przydziela upoważnienia. Rozwiązania techniczne wykraczają poza zakres niniejszej pracy będąc szczegółowo omowionymi w literaturze (49). Nie mniej wbrew propoagowanym zasadom badania wykazały, ze w 92% osrodków istnieją osoby (z reguły więcej niż jedna) znające architekturę systemów operacyjnych i potrafiące spenetrować dokładnie każdy jego punkt. Zazwyczaj byli to programiści systemowi, konserwatorzy i projektanci. Problem nawarstwia się w przypadku mikrokomputerów, gdzie pojęcie systemu operacyjnego jest raczej umowne, a krąg osób znających dokładnie mapę pamięci mikroprocesora jest zbliżony do 70% użytkowników (profesjonalnie zajmujących się programowaniem mikrokomputerów). Najbardziej wrażliwym miejscem z punktu widzenia metod ochrony programowej jest lokacja i utajnienie parametrów uzbrajających, z reguły mających postać macierzy dostępu. Jako rozwiązanie proponuje się np. w przypadku mikrokomputerów zastosowanie blokady na jednostce użytkowej w celu niemożnosci wprowadzania programów narzędziowych, w przypadku dużych systemów niemożności badania zawartości pamięci.

4.2. Ochrona na poziomie programów.

Podobnie jak w przypadku systemu operacyjnego musi nastapić identyfikacja użytkownika, urządzeń i danych, uwierzytelnienie i upoważnienie. Powinno sie dążyc do autonomii w tym zakresie, to znaczy do doprowadzenia, aby poza ochroną na szczeblu systemu operacyjnego poszczególne programy miały swoje zabezpieczenia, niezależnie od systemu. Pozwoli to na zabezpieczenie się przed włamaniem do programu i danych przez system operacyjny. Należy w tym punkcie zwrócić uwagę na dogodną i stosunkowo mało kłopotliwą metodę programową jaką jest szyfrowanie. Programy szyfrujące mogą znajdować się w systemie operacyjnym, jednak umieszczając je w programach użytkowych uwalniamy się od zagrożeń ze strony systemu.

4.3. Ochrona informacji na nośnikach.

Jedynym optymalnym rozwiązaniem jest magazynowanie informacji w postaci zaszyfrowanej. Stosuje się również rozłączne bazy danych, gdzie dane powiązane są ze sobą identyfikatorami. Obecny rozwój techniki pozwala na penetrację całego nośnika bez względu na jego rodzaj i jawne zapisanie zbioru jest równoznaczne z bezproblemowa

---

(49) Por. przypis (41) w niniejszej rozprawie.

możliwościa jego odczytu (50).

4.4. Ochrona informacji w teletransmisji.

Rownież jedyną metodą, stosowaną powszechnie jest szyfrowanie przesyłanych informacji. Tym bardziej, że komputer jest doskonałym narzędziem do tego celu. W przypadku wielodostępu i sieci stosuje się często sprzężenie zwrotne ze zwielokrotnionym uwierzytelnieniem.

Ogólną zasadę programowej metody ochrony ilustruje schemat blokowy umieszczony na rysunku 1 (51). Dodatkowo można uwzględnić zablokowanie końcówki lub pracę symulowaną na błędnych danych w celu ewentualnego ujęcia sprawcy albo jego dezinformacji.

Wspomnieć także należy o programach - szczepionkach zwalczających lub zapobiegających wirusom komputerowym, jest to rownież forma metody ochrony programowej.

Do zalet metody programowej należy zaliczyć :

- łatwość konstrukcji, także we własnym zakresie,
- małe nakłady finansowe, realizacja przez komputer,
- stosunkowo wysoka niezawodność,
- mozliwość rejestrowania przypadków nieupoważnionego dostepu do zbioru,
- brak oznak zewnetrznych o stosowaniu,
- nieskomplikowanie procesu przetwarzania,

Wady są nastepujące :

- wydłużenie procesu przetwarzania,
- niebezpieczeństwo "złamania systemu, w przypadku ujawnienia parametrów uzbrajających,

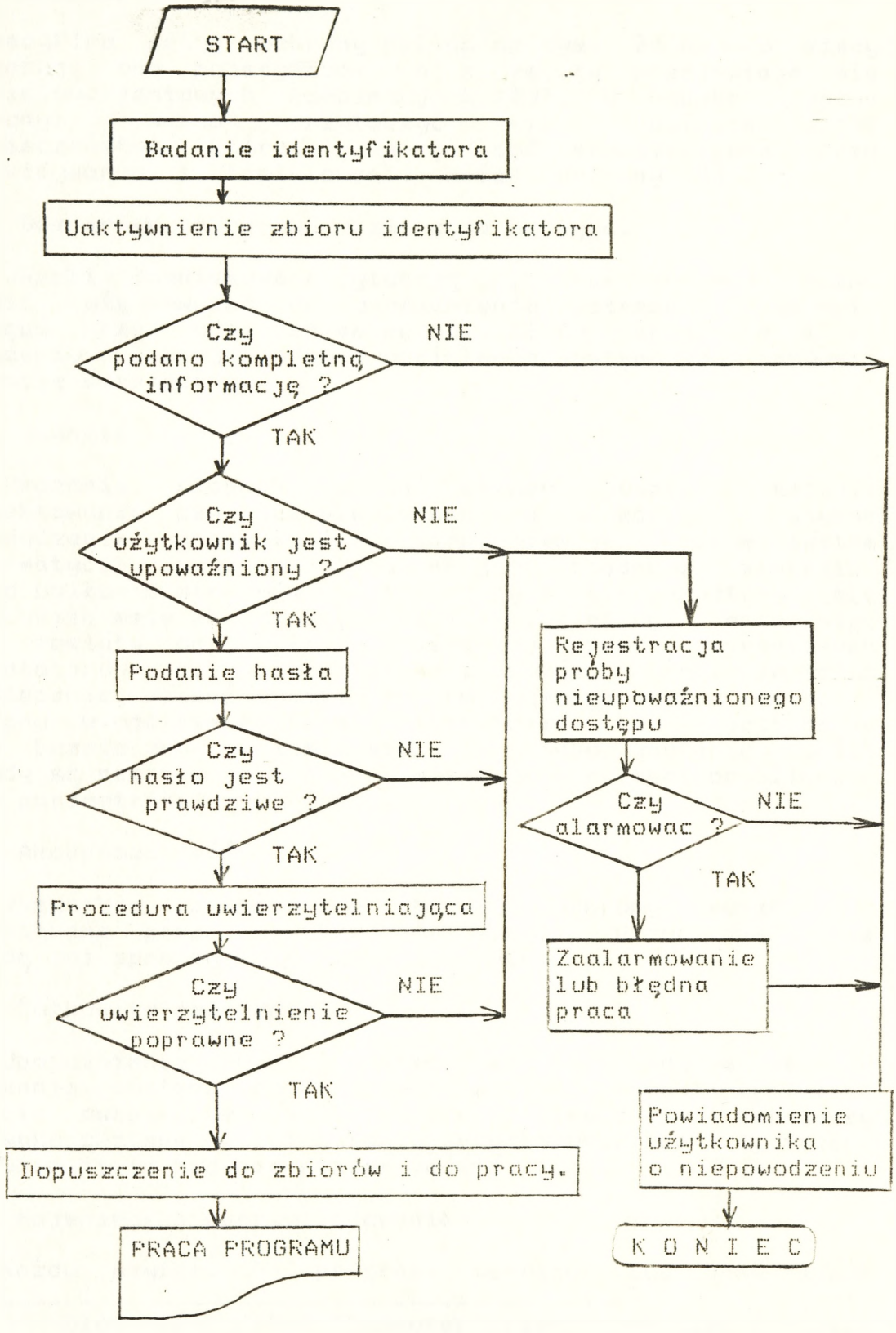
4.5. Aspekt operacyjny.

Programowe metody ochrony w chwili obecnej są stosowane głównie w postaci haseł (78% badanych systemów). Istotna jest wiedza o przechowywaniu parametrów uzbrajających i ich ulokowaniu. Możliwe jest poprzez osobowe źródła informacji umiejscowione przy komputerze dotarcie do wszystkich zbiorów systemu, gdy znane będą hasła. Stosowanie techniki operacyjnej rownież wymagało będzie rozpoznania w tym zakresie. Ponadto dla celów dochodzeniowo-śledczych w przypadku włamania się do systemu metody programowe mogą ujawnić wiele istotnych czynników.

---

(50) proponowane są rownież inne techniczne rozwiązania jednak ich stosowanie nie jest ekonomiczne por. Kroh J. " Zabezpieczenie programów", Mikroklan 1987 Nr 11-12.

(51) Sokołowski Andrzej: "Ochrona informacji komputerowej" MON Warszawa 1987.



Rys.1. Ogólny schemat działania programowej metody ochrony.

5. PODSUMOWANIE METOD.

Specyfika metod ochrony polega na tym, że rzadko kiedy występują one pojedyńczo, a z reguły przejawiają się w wielowariantowych kombinacjach (52). W aspekcie metod ochrony, warto przytoczyć kilka ważnych zasad bezpieczeństwa, które powinny być przestrzegane przy przewidywaniu i instalowaniu metod ochrony (53).

5.1. Domniemywana odmowa udzielenia dostępu.

Jezeli domniemywaną sytuacją jest brak dostepu, można zmusić użytkownika do uzasadnienia potrzeby uzyskania dostępu przed udzieleniem mu go. Błędy w projekcie i we wdrożeniu powodują odmowę udzielenia dostępu co zapewnia sytuację bezpieczną.

5.2. Jawność metody.

Ukazanie słabych stron metody jeszcze podczas projektowania czy tez planowania ułatwi zdolnym krytykom wprowadzenie poprawek przed wdrożeniem jej, zanim system informatyczny zacznie polegać na jej (błędnym) działaniu. Można usiłować utrzymywać w tajemnicy stosowane metody, ale na dłuższą metę znajdą się w nich jakieś błędy. Lepiej więc aby zostały one wykryte wczesniej przez zaproszonych komentatorow, niż później przez intruzów. Jeżeli nie można bezpiecznie opisać systemu informatycznego wraz z metodami ochrony w ogólnie dostępnej literaturze, to nie jest on na tyle bezpieczny by można mieć do niego zaufanie. Jeśli metody są rzeczywiście dobre, można je w całosci opublikować poza parametrami uzbrajającymi.

5.3. Akceptowalność.

Wszystkie zastosowane metody ochrony muszą być akceptowane przez użytkowników, gdyż w przeciwnym razie znajdą oni sposoby na to aby je obejść.

5.4. Całkowite pośredniczenie.

Upoważnienie musi być sprawdzane przy każdym zadaniu uzyskania dostępu do każdego obiektu. Zasada ta wymaga by w razie ewentualnej zmiany poziomu upoważnienia nie mogły być wykorzystane wyniki badania upoważnienia, lecz by trzeba ponownie takie badanie przeprowadzić.

5.5. Najmniejsze uprzywilejowanie.

Każdy uzytkownik, program, terminal lub inny zasób

---

(52) Blatchford C.W. "Computer crime - the need for data security", Management Services, IX.1986.

(53) Hofman L.J. "Poufność w systemach informatycznych" WNT Warszawa 1982.

powinien korzystać tylko z tych przywilejów, które są niezbędne do wykonania zadania.

5.6. Ekonomiczność mechanizmu.

Projekt metod ochrony i sama ochrona powinny być tak proste i małe jak tylko to możliwe.

5.7. Oddzielenie przywilejów.

Dwa oddzielne zabezpieczenia stanowią zawsze lepszą i elastyczniejszą ochronę niż jeden. Kiedy mechanizm jest zamknięty, dwa klucze do niego mogą byc fizycznie oddzielone i oddane pod opiekę różnym programom, organizacjom lub ludziom.

5.8. Najmniejszy wspólny mechanizm.

Każdy wspólny mechanizm reprezentuje potencjalną ścieżkę przepływu informacji między użytkownikami, a więc wielodostepność powinna być minimalizowana.

6. METODY OCHRONY W ASPEKCIE FUNKCJI JEDNOSTEK RESORTU SPRAW WEWNĘTRZNYCH.

Zdefiniowano metodę jako zespół czynności i środków użytych dla osiągnięcia celu. Celem metod ochrony jest stosowanie zabezpieczeń w celu zapobieżenia zagrożeniom godzącym w niezawisłość systemu. Omówiono podstawowe typy metod ochrony, które powinny obowiązywać na poziomie samego systemu. Przeprowadzona analiza pozostaje w ścisłym związku z metodami ochrony rozpatrywanymi na poziomie jednostek resortu spraw wewnętrznych. Podstawowym celem resortu jest organizowanie i doskonalenie metod i form działań rozpoznawczych, zapobiegawczych i wykrywczych w celu zwalczania przestępstw oraz wykroczeń, jak również innych czynów i zjawisk zagrażających bezpieczeństwu państwa i porządkowi publicznemu. Rozważmy zatem metody - czynności i środki, które winny być użyte w celu zapobieżenia zagrożeniom godzącym w niezawisłość systemu.

Jednostki resortu spraw wewnętrznych wykonują czynności operacyjno-rozpoznawcze przejawiające się w ramach szeroko pojętej profilaktyki oraz dochodzeniowo-śledcze, które są przedsięwzięciami procesowymi, podejmowanymi w ramach prowadzonego postępowania przygotowawczego (dochodzenia lub śledztwa) na podstawie przepisów postepowania karnego.

W aspekcie powyższego rozpatrzmy następujące problemy :

- zakres czynności operacyjno-rozpoznawczych w ramach ochrony systemów,
- czynności dochodzeniowo-śledcze w przypadku naruszenia systemu ochrony i stwierdzenia przestępstwa komputerowego,
- dobór, kwalifikacje oraz szkolenie pracowników resortu pod kątem fachowości w omawianym zagadnieniu.
- rozmieszczenie i właściwe eksploatowanie sieci osobowych

źródeł informacji,
- rola i znaczenie konsultantow i biegłych,
- mozliwość zastosowania srodkow techniki operacyjnej w ochronie systemow informatycznych,

6.1. Zakres czynności operacyjno-rozpoznawczych w ramach ochrony systemów.

Czynności operacyjno-rozpoznawcze to działania pozaprocesowe o charakterze jawnym i niejawnym. Czynnościami operacyjnymi są czynności nieoficjalne (tajne, poufne) podejmowane w celu uzyskania określonych informacji, ich sprawdzenia lub uzupełnienia. W ramach czynności operacyjno-rozpoznawczych informacje zdobywane mogą być poprzez osobowe źródła informacji lub przez prowadzenie rozmów nieformalnych bądź dokonywanie okresowych kontroli. Uzależnione jest to od występujących potrzeb i możliwości. Podczas typowania osób do mających być przeprowadzonych rozmów lub potencjalnych kandydatów na osobowe źródła informacji należy wziąć pod uwagę omówienie w niniejszej pracy poziomu ochrony jakim są użytkownicy , a podczas przygotowania scenariusza rozmowy przydatne może byc omowienie metod ochrony w bieżącym rozdziale. Poza profilaktycznym aspektem omawianych czynności, bardzo istotnym jest stworzenie zaplecza do potwierdzenia, poszerzenia lub uzupełnienia informacji uzyskiwanych i potrzebnych dla realizacji czynności dochodzeniowo-śledczych realizowanych w przypadku naruszenia niezawisłości systemu.

6.2. Czynności dochodzeniowo-śledcze w przypadku naruszenia systemu ochrony.

Problem ten należy do tych problemów, które wymagają jak najszybszej i w miarę najpełniejszej realizacji. W przypadku zaistnienia przestępstwa związanego ze złamaniem systemu ochrony, gdy nastąpi naruszenie prawa w postaci infiltracji, manipulacji bądź zniszczenia należy posłużyć się przewidzianym i ujętym w normy instrukcyjne tokiem postępowania przy zabezpieczaniu śladów celem ich procesowego wykorzystania.

Występuje tutaj kilka zagadnień :

Przybyli na miejsce zdarzenia pracownicy resortu winni wiedzieć co zabezpieczyć. W przypadku całej gamy przestępstw komputerowych większość z nich charakteryzuje się tym, że brak jest wyraźnych śladów, brak jest odcisków linii papilarnych odprysków szkła czy innych mikrośladów. Prawie wszystkie ślady zawarte są najczęściej we wnętrzu komputera, ewentualnie na nośnikach informacji. Ważne jest zatem, aby przynajmniej na szczeblu wojewódzkim znajdował się pracownik, który będzie wiedział co i jak zabezpieczyć. Jak odtworzyć interesujący okres pracy systemu, które nośniki zabezpieczyć celem dalszych badań, jak niedopuścić do utraty tych informacji, które mogą ujawnić sprawcę, a mogą zniknąć bezpowrotnie, np. przy

wyłączeniu maszyny. Jakie dokumenty zwykłe i maszynowe w obiegu informacyjnym ośrodka będą konieczne do zobrazowania rzeczywistego stanu rzeczy. Ponadto ważna jest również forma ich zabezpieczenia oraz dalsza obróbka celem zebrania stosownych materiałów dla potrzeb procesowych. Istotna jest wiarygodność dla sądu. Uwypukla się w tym momencie również rola konsultanta, który po wstępnej analizie może orzec o przydatności zabezpieczonych materiałów, o niedoborach wśród nich oraz o ewentualnie występujących innych potrzebach.
Biorąc pod uwagę trendy światowe w praktyce popełniania przestępstw komputerowych oraz obecny w naszym kraju stan przyszłościowy naszej rodzimej bazy informatycznej i mikrokomputerowej, jak również jej wykorzystanie trzeba poważnie podejść do tego problemu i w jak najszybszym tempie wprowadzić stosowne przepisy w tym zakresie.
Charakterystycznym staje się fakt, że większość przedsiębiorstw zmienia swoją administrację i księgowość na formę obsługi przy użyciu komputera. Ponieważ wiąże się to z redukcją personelu oraz optymalizacją działania wymusi to na pracownikach resortu, którzy będą zmuszeni do wykorzystywania tych informacji w realizacji swoich czynności konieczność znajomości zapisu tych informacji w komputerze. Ponadto będą musieli potrafić zabezpieczyć je dla potrzeb sądu, tak by uniknąć wieloznaczności a także umieć odpowiednio je wykorzystać. Głównie dotyczy to pionu przestępstw gospodarczych.

6.3. Dobór, kwalifikacje oraz szkolenie pracowników resortu pod kątem fachowości w omawianym zagadnieniu.

Szkolenie pracowników jednostek resortu spraw wewnętrznych powinno przebiegać wieloszczeblowo. Podczas szkolenia podstawowego u szeregowych pracowników najistotniejszym byłoby zwrócenie ich uwagi na konieczność stosowania się do instrukcji omawiającej postępowanie przy obecności na miejscu zdarzenia komputera. Instrukcji analogicznych do tych które określają zachowanie podczas zabezpieczenia innych miejsc zdarzenia. Zakres przekazywanej na tym szczeblu wiedzy powinien dotyczyć najprostszych manualnych czynności niezbędnych dla niezatarcia śladów itp. Wiedza przekazywana na szkołach resortowych w zakresie informatyki obejmuje problemy zbędne i nie porusza istotnych (54). Na całym świecie rezygnuje się z nauczania informatyki na bazie konstrukcji komputera i na poziomie języków programowania. Stan komputeryzacji, jej wykorzystanie oraz ogólnoświatowe trendy dążą do nauki obsługi komputera w ramach pracy z poszczególnymi gotowymi pakietami (typu edytor tekstu, arkusz kalkulacyjny itp.). Osoby przeznaczone do realizacji czynności operacyjno-

---

(54) Przykładowo por. Rosiak H. "Organizacyjne ujęcie procesu dydaktycznego WSO MSW w Legionowie z wykorzystaniem komputera", Zeszyty Naukowe WSO 1987 Nr 2 - 3.

rozpoznawczych powinny ogólnie być zapoznane ze specyfiką środowiska informatyków oraz z metodami zdobycia informacji, bez szczegółowego dotarcia do konkretnych danych. Pracownicy pionu przestępstw gospodarczych muszą być przygotowani jeżeli nie do samodzielnego dotarcia do potrzebnych im danych to przynajmniej do zabezpieczenia ich dla celów procesowych tak aby mogły być przekazane do dalszej obróbki specjalistom. Przedostatni szczebel szkolenia to na szczeblu centralnym, a w przyszłosci na szczeblu wojewódzkim specjaliści lub grupy specjalistów informatyków wyposażonych w sprzęt i oprogramowanie narzędziowe by można było na zasadach pionu kryminalistyki sporządzac ekspertyzy z dziedziny i obszaru informatyki dla potrzeb procesowych. Szczebel najwyższy to wyspecjalizowana jednostka na szczeblu centralnym (55) mogąca realizować wszystkie zadania z omawianej dziedziny oraz konstruująca własne pakiety programowe (np. badające księgowość prowadzoną przez system mikrokomputerowy) dla potrzeb niższych szczebli. Powinien tu wystąpić proces samokształcenia bądź kształcenia za granicą tak aby wiedza pozostająca do dyspozycji była jak najbardziej aktualna.

6.4. Rozmieszczenie i właściwe eksploatowanie sieci osobowych źródeł informacji.

Wszyscy bez wyjątku autorzy prac z zakresu ochrony systemów informatycznych zwracają uwagę na fakt, że najsłabszym ogniwem na wszystkich poziomach ochrony jest człowiek. Każda z metod ochrony bez względu na jej zakres, usytuowanie techniczne czy doskonałość dotyczy człowieka i od niego zależy. Podstawowym narzędziem pracy każdego pracownika operacyjnego resortu spraw wewnętrznych są osobowe źródła informacji. W przypadku obiektu jakim jest system informatyczny najistotniejszym jest ich właściwe rozlokowanie oraz eksploatacja. Pozyskiwanie osobowych źródeł informacji przy operacyjnej ochronie stałej powinno objąć poza wymogami instrukcyjnymi osoby mające kontakt z węzłowymi punktami systemu informatycznego, szczególnie tam gdzie występuje przetwarzanie danych wrażliwych oraz gdzie mogą wystąpic potencjalnie zagrożenia. Zadbać należy szczególnie o posiadanie źródeł szczególnie w grupach, zespołach opracowywujących wrażliwe systemy, eksploatujących bezpośrednio komputer oraz mających wpływ na tok realizowanych zadań. Nie bez znaczenia jest rola źródeł o charakterze manewrowym lub sygnalnym. Te pierwsze powinny zapewnić dostęp do najwrażliwszych punktów systemu

---

(55) W Wielkiej Brytanii problemami ochrony systemów informatycznych zajmuje się FAST (Federacja do Zwalczania Kradzieży Oprogramowania). We Francji Urząd do Scigania Przestępstw Podatkowych został całkowicie zmobilizowany do walki z komputerową przestepczoscią.
Zob. "Komputerowe piractwo", Slowo Ludu 1987 Nr 5.

informatycznego od procesu projektowania do konserwacji i zmian. Drugie winny informować o wszystkich sygnałach, gdzie może być spodziewane wystąpienia zagrożenia. W procesie eksploatacji źródeł należy dążyć do zrealizowania nastepujących zadań :

- otrzymanie pełnego w miarę możliwości obrazu o całokształcie prowadzonych prac ze szczególnym uwzględnieniem przetwarzania danych wrażliwych,
- rozpoznanie wszystkich pracowników ośrodka, szczególnie tych, którzy posiadają wszechstronną wiedzę, kwalifikacje oraz dostęp do wrażliwych punktów systemu,
- ciagłe badanie stanu klimatu pracy w ośrodku, tworzenia się nieformalnych grup pracowniczych, wykrywanie animozji i informowanie o sytuacjach mogących mieć następstwa w postaci konfliktu,
- ujawnianie, kontrolowanie i neutralizowanie osób o radykalnych bądź wrogich postawach zarówno w sferze politycznej, ekologicznej jak i ekonomiczno-społecznej celem niedopuszczenia do spowodowania przez nich jakichkolwiek perturbacji bez względu na płaszczyzne niezadowolenia czy motywy,
- śledzenie obiegu dokumentacji i materiałów oraz przestrzeganie zasad i przepisów o ochronie i bezpieczeństwie ośrodka w każdym ujęciu,
- uzyskiwanie szybkich i w miarę możliwości pełnych informacji o wszelkiego rodzaju symptomach świadczących o odstąpstwach od normy i sygnałach o możliwości wystąpienia zakłóceń,
- otoczenie szczególną opieką osób postronnych, głównie zza granicy przebywających na terenie ośrodka, osób wyjeżdżających za granicę, mających za granicą kontakty a także utrzymujących kontakty z osobami notowanymi w kartotekach resortu,
- analizowanie wzajemnego wpływu pomiędzy ośrodkiem i otoczeniem (np. w przypadku ośrodków, wewnątrz-zakładowych) pod kątem pojawienia się różnego typu zagrożeń szczególnie o charakterze gospodarczym,
- zbieranie informacji o nadużyciach gospodarczych, malwersacjach, kradzieżach, złej polityce kadrowej i gospodarczej oraz innych faktach destruktywnie wpływających na realizowanie zadań,
- posiadanie informacji o osobach przebywajgcych na terenie ośrodka po godzinach pracy, a także przebywających w miejscach, gdzie ich obecność jest zbędna, niepożądana lub bezprawna z ustaleniem ewentualnych motywów,
- uzyskiwanie poprzez odpowiednie źródła informacji bezpośrednio z systemu informatycznego dla celów operacyjnych zgodnie z potrzebami wszystkich jednostek resortu,

W punktach gdzie jest to konieczne ze względu na dużą wrażliwość danych należy przewidzieć i dążyć do zdublowania źródeł celem wzajemnej ich kontroli i potwierdzenia napływających informacji. Opracować należy równolegle system wzajemnej łaczności z uwzględnieniem nieobecności pracownika i sytuacji alarmowej co w przypadku konieczności szybkiego

reagowania na nieprawidłowosci w systemie informatycznym jest szczególnie ważne.

Przy operacyjnym rozpoznaniu ośrodków obliczeniowych, biorąc pod uwagę fakt specyfiki środowiska ludzi zajmujących się informatyką należy przewidzieć i realizować eksploatację osobowych źródeł informacji w ujęciu całego środowiska, z osobami z innych ośrodkow i otoczenia włącznie.

Powyższy model jest oczywiście abstrakcyjny, stworzony po to aby przewidzieć ewentualne wszystkie przypadki, a wiekszość jego rozwiazań powinna mieć charakter działań kontrwywiadowczych lub przy ochronie szczególnie ważnych systemów.

6.5. Rola i znaczenie konsultantów i biegłych.

Biorąc pod uwagę obszerność zagadnień informatyki, ciagły postęp i coraz wieksza i węższą specjalizację przy występowaniu konkretnych problemów należy dla potrzeb pracy operacyjnej i wstępnych czynności procesowych zapewnić sobie udział konsultantów. Udział ich jest szczególnie ważny przy zaistniałych wydarzeniach, gdzie w toku spraw operacyjnych lub przygotowawczych dąży się do oceny konkretnych materiałów pod względem przydatności procesowej. Podobnie można opinie konsultanta wykorzystać wcześniej przy ewentualnej ocenie materiałów wstępnych kwalifikując je do wszczęcia dochodzenia lub śledztwa. W dalszym toku nie ma przeciwwskazań aby konsultant wystąpił jako biegły.

6.6. Mozliwość zastosowania środkow techniki operacyjnej w ochronie systemow informatycznych.

Należy przewidzieć ewentualną możliwość wystąpienia poważnego zagrożenia o charakterze ciągłym bądź wchodzącego w zakres działań kontrwywiadowczych. Celem uzyskania konkretnych efektów trzeba będzie być może zastosować środki techniki operacyjnej, których użycie przy problemie ochrony systemów informatycznych nabiera nowych treści. Obok tradycyjnych takich jak PT, PP, PDF, W rozważyc należy specjalne. Podstawowym ich reprezentantem będzie podsłuch komputerowy (def.własna autora). Można go stosować :

- w formie biernej – gdy system operacyjny będzie bez wiedzy obsługi rejestrował wszystkie lub wybrane informacje, operacje lub dane,
  - gdy zamontowany zostanie dodatkowy monitor śledzący pracę systemu, bądź terminala w dowolnym punkcie.
- w formie czynnej – gdy wystąpi selekcja i gromadzenie informacji poprzez specjalny program lub urządzenie podłączone do obiektu śledzonego z ewentualną bazą alternatyw co do realizacji reakcji w określonych przypadkach,

Można zastosować rejestrowanie miejscowe (taśma, dysk) lub przesyłać informacje poza miejsce pracy obiektu

śledzonego możliwymi, dostępnymi metodami.

W przypadku mikrokomputera może wystąpić kopiowanie zawartości dysku lub podłączenie się do sieci.

7. PODSUMOWANIE.

Prognozy ewentualnych następstw niektórych przestępstw bądź zagrożeń w obszarze działania systemów informatycznych są zatrważające. Jako przykład podajmy ewentualność zatrzymania komputerów w londynskim City. Oblicza się, że przechodzi przez nie jedna czwarta wszystkich transakcji świata zachodniego, a ewentualność ich niefunkcjonowania np. w przypadku dywersji lub innej formy działań przestępczych spowodowałaby załamanie się zachodniego systemu w ciągu zaledwie 12 godzin (56). Do skutecznej realizacji ochrony systemów informatycznych niezbędne jest poznanie metod ochrony. Równolegle potrzebne to jest także w przypadku konieczności własnej infiltracji systemu, wtedy gdy zachodzi odpowiednio umotywowana konieczność. Metody rzadko występują pojedyńczo, z reguły ich różne formy są powiązane ze sobą tworząc na poszczególnych poziomach ochrony swoiste systemy ochrony. W niniejszym rozdziale próbowano podać najistotniejsze z nich omawiając je w różnych aspektach oraz zwracając szczególną uwagę na fakt, że znajomość metod rzutuje zasadniczo na możliwość sprawnej realizacji ochrony systemów informatycznych w aspekcie funkcji jednostek resortu spraw wewnętrznych.

---

(56) Por. Jożwin M. "Komputer przestępca", Nowator 1986 Nr 12.

IV. M O D E L O C H R O N Y.

Ochrona systemów informatycznych w aspekcie funkcji resortu spraw wewnętrznych będzie miała miejsce w konkretnych jednostkach administracyjnych, gospodarczych oraz innych gdzie praca takiego systemu będzie wykorzystywana. Realizować te ochronę będą przede wszystkim pracownicy zatrudnieni przy komputerach, decydenci oraz ludzie odpowiedzialni za niezawisłość systemu, najczęściej pracownicy różnego szczebla jednostek resortu spraw wewnętrznych.

Celem stworzenia pewnego uogólnienia metod ochrony dokonajmy przeglądu typowych systemów informatycznych według nastepujących zagadnień :

A. Struktura systemu.
B. Ocena aktualnego stanu ochrony.
C. Wystepujące w systemie potrzeby.
D. Wymogi stawiane instytucjom.
E. Zadania jednostek resortu spraw wewnętrznych.

1. SYSTEMY INFORMATYCZNE WYPOSAŻONE W KOMPUTERY BEZ TELETRANSMISJI.

Do grupy tej zaliczymy duże systemy autonomiczne i zakładowe (np. ZETO Kielce, FSS SHL, FLT ISKRA), średniej wielkości (np.Politechnika Świętokrzyska, CHEMAR) oraz małe, na których przetwarzanie danych odbywa się na minikomputerach.

A. Struktura systemu.

Przedstawiona została na rysunku nr.2. Główną cechą charakterystyczną w strukturze tej grupy systemów jest względna izolacja komputera i procesu przetwarzania od otoczenia i czynników zewnętrznych. Ze względu na to panuje przekonanie o małym prawdopodobieństwie wystąpienia zagrożeń i osłabienie zainteresowania problemami ochrony. Struktura jest typowa i uzależniona od sprzętu. Dominuje zestaw jednostki centralnej, czasem zdublowanej ze stanowiskami operatorskimi oraz rożnego rodzaju konfiguracją urządzeń zewnętrznych. W przypadku systemów autonomicznych występuje zaplecze administracyjno - gospodarcze, w systemach zakładowych jest ono z reguły umieszczone w jednostkach administracyjnych zakładu nadrzędnego.

B. Ocena aktualnego stanu ochrony.

Z przeprowadzonych badań wynika, że w wymienionej grupie systemów dominują metody organizacyjne oraz fizyczne. Przy czym te ostatnie z reguły polegają na rozwiązaniach najprostszych - strażnicy, zamykane pomieszczenia. Metody programowe zawężaja się do procedur wbudowanych w system

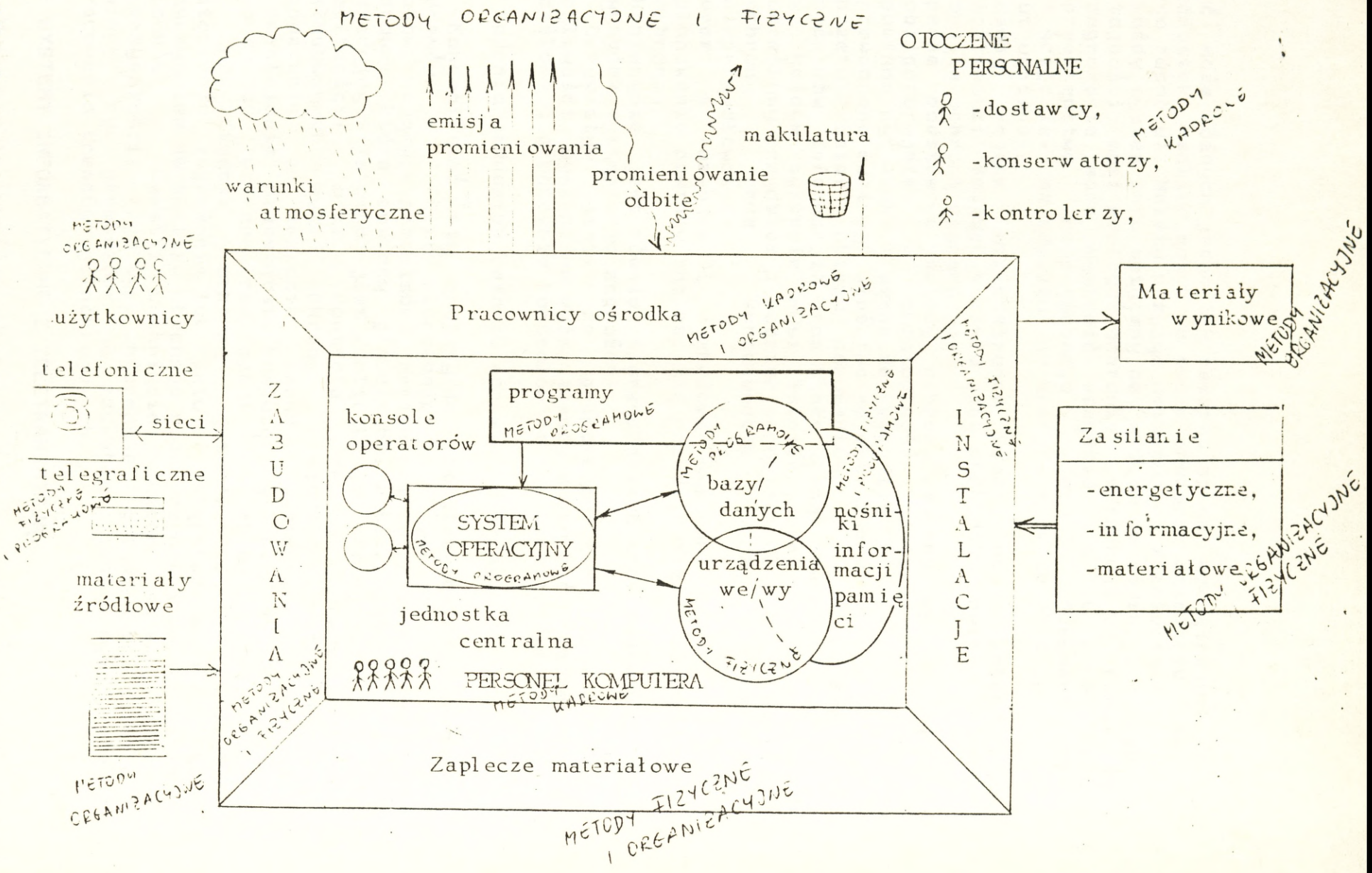
operacyjny i pakiety użytkowe. Metody organizacyjne mimo, iż są dokumentowane z powodu pozornej izolacji są lekceważone i omijane. W problematyce metod kadrowych panuje dowolność. Wiele stosukowo osób mających wszechstronną wiedzę na temat systemu posiada naturalny dostęp i możliwość ingerencji. Dostępna jest również ogólnie dokumentacja i biblioteka. Powodem karygodnego stanu rzeczy jest nagminny brak wyobraźni i przewidywania zagrożeń, jest to pochodna częstego obsadzenia na stanowiskach kierowniczych lub osób odpowiedzialnych za ochronę ludzi niekompetentnych i nie mających przygotowania informatycznego. Stwierdzono np. że przy przetwarzaniu zbiorów niejawnych w szafach pancernych przechowywuje sie wydruki komputerowe podczas gdy pakiety dysków jako niby nie mogące być przeczytane pozostawiono bez zabezpieczenia.

C. Wystepujące w systemie potrzeby.

Wiadomym jest, że nakłady ponoszone na metody ochrony skorelowane być powinny z wrażliwościa systemu oraz przetwarzanych informacji. W takcie prowadzonych badań okazało się, że niewielka cześć decydentów traktowała przetwarzane dane jako podlegające ochronie, a klauzulę "poufne" wręcz lekceważyla. Biorąc pod uwagę możność niezaangażowania metod ochrony, było to bardzo wygodne, jednak jest to źrodłem poważnego niebezpieczeństwa. Wszędzie tam gdzie przetwarzane są dane może wystąpic zagrożenie, stąd metody ochrony powinny być wprowadzane w każdym systemie. Ich instalacja oraz jakość musi oczywiście (jako, ze podwyższa znacznie koszty i czasem wydłuża proces przetwarzania) pozostawać w odpowiedniej proporcji do klauzuli tajności jaką posiadają dane lub ich wrażliwości innego typu. Najprostsze do wprowadzenia są oczywiście metody organizacyjne oraz proste formy metod fizycznych, których zastosowanie w większosci wypadków będzie w zupełności skuteczne. Tym niemniej istotna jest stała kontrola stosowania się do reżimu każdej metody, bowiem tylko wtedy spełni ona swoje zadanie. Olbrzymie możliwości tkwią również w metodach programowych, których wdrożenie nie pociąga za sobą poważniejszych kosztów, może byc wykonane w ramach własnego zespołu, a charakteryzuje się dużą skutecznością. Zarys metod ochrony obrazuje rysunek nr.2, a ich rodzaj i liczbę, a także umiejscowienie warunkują konkretne potrzeby i możliwości finansowe danego ośrodka. Tymczasem badania wykazały, ze fundusze na ochronę globalnie nie są brane w ogóle pod uwagę.

D. Wymogi stawiane instytucjom.

W celu poprawy istniejącego stanu rzeczy w aspekcie ochrony systemów informatycznych wymaga uporządkowania doprowadzenie do w miarę rzetelnego przestrzegania obowiazków w instytucjach posiadających lub będących systemami informatycznymi (powinno się to znaleźć w kompetencjach jednostek lub osób za to odpowiedzialnych,



RYS. 2. Metody ochrony w systemie informatycznym bez teletransmisji.

być może różnych jednostek resortu spraw wewnętrznych lub jednostek realizujących na swoim obszarze działania funkcje tego resortu). Należy przyjąć następujące założenia :

- każdy system informatyczny bez względu na rodzaj i klauzulę tajności musi podlegać ochronie. Warunkuje to fakt, że zagrożenie może wystąpić wszędzie, a po popełnieniu przestępstwa komputerowego jego udokumentowanie i ściganie, ze względu na specyfikę może być poważnie utrudnione,
- osoby mające wszechstronną wiedzę oraz potencjalne możliwości dostępu w wielu jego punktach powinny zostać objęte ochroną operacyjną,
- pewne podstawowe metody ochrony powinny być narzucone obligatoryjnie, a ewentualność zastosowania innych powinna być skonsultowana ze specjalistą z zewnątrz,
- prowadzona musi być właściwa rejestracja w kwestii procesu przetwarzania, obiegu dokumentów (w tym maszynowych nośników informacji) oraz stała wewnętrzna kontrola,
- w każdym systemie musi istnieć jasny i precyzyjnie określony przydział i podział odpowiedzialności za sprawy ochrony oraz konsekwencje przy ujawnieniu nieprawidłowości,
- wraz z rozwojem i rozbudową systemu już w sferze planowania powinny znaleźć się przedsięwzięcia w aspekcie ochrony,
- koniecznie jest również sporządzenie planów awaryjnych na wypadek wystąpienia zagrożeń.

Oczywistym jest, że proporcjonalnie do stopnia wrażliwości wymienione wyżej zasady muszą być rozszerzone, uściślone i gruntownie kontrolowane ich przestrzeganie.

E. Zadania jednostek resortu spraw wewnetrznych.

Koncentrować się powinny na profilaktycznej ochronie systemów w sferze planowania i egzekwowania metod i obowiązujących przepisów. Nacisk należy położyć na metody kadrowe, które powinny głównie być realizowane w sposób operacyjny. Istotna jest kwalifikacja informacji co do ich wrażliwości, oraz kontrola reżimu przestrzegania zastosowanych metod ochrony. Posiadając ogólnokrajowe rozpoznanie w zakresie trendów występowania zagrożeń i popełniania przestępstw komputerowych wiedzę tą należy wykorzystać podczas realizacji szerokiej profilaktyki na płaszczyźnie ochrony systemów informatycznych. Wystąpienie zagrożenia lub faktu przestępstwa powinno być przyczynkiem do analizy obecnego stanu rzeczy i wyciągnięcia wniosków w kwestii uniknięcia takiego stanu rzeczy w przyszłości. Tego typu informacje i gotowe doświadczenia powinny być gromadzone na szczeblu centralnym celem opracowania trendów ogólnokrajowych.

2. SYSTEMY INFORMATYCZNE Z TELETRANSMISJĄ.

W grupie tej wyróżnimy teletransmisję pomiedzy ośrodkami obliczeniowymi wzajemnie oraz pomiedzy ośrodkami

i oddalonymi terminalami (np.CIBEH,COIG,ZETO Katowice) (57).

A. Struktura systemu.

Elementem charakterystycznym dla tej grupy systemów jest teletransmisja czyli zespół urządzeń sterowania transmisją linii telekomunikacyjnych i teledatorów. Przy czym przesyłanie danych może również wystąpić pomiędzy dwoma komputerami. Od opisanego w poprzednim rozdziale systemu niniejszy różni się wystąpieniem problemów teletransmisji i urządzeniami. Wewnątrz omówionego już systemu funkcjonować będą centrale, modemy, multipleksory i selektory, a także urządzenia do szyfrowania danych. Jako urządzenia peryferyjne zastosowane być mogą terminale, czujniki, manipulatory, a także inne ośrodki obliczeniowe. Przesyłanie informacji może nastąpić po liniach komutowanych, dzierżawionych lub specjalnych (por.rysunek nr.3).

B. Ocena aktualnego stanu ochrony.

Teletransmisja w naszym kraju występuje stosunkowo rzadko. Jest to głównie wynikiem złego stanu linii telekomunikacyjnych ogólnego stosowania oraz trudnościami technicznymi w wykorzystaniu ich do teletransmisji. Z przeprowadzonych badań wynika, że możliwość wystąpienia zagrożenia jest prawie całkowicie ignorowana. Sama zamiana sygnału jest dla decydentów pozornie wystarczająca rękojmią ochrony przesyłanych danych. Najniebezpieczniejsze jest to, że widząc i rozwiązując problemy techniczne nie bierze się w ogóle pod uwagę metod ochrony.

C. Występujące w systemie potrzeby.

W stosunku do typowych elementów systemu potrzeby będą analogiczne do opisanych w rozdziale poprzednim. Dodatkowej analizie poddać należy teletransmisję. Najsłabszym punktem w aspekcie ochrony w tej grupie systemów są linie przesyłu informacji, szczególnie tam gdzie do czynienia mamy z liniami komutowanymi i dzierżawionymi. Jedynym możliwym i koniecznym panaceum w tym zakresie jest szyfrowanie (58) informacji. Ta metoda programowa ze względu na stosunkowo niskie koszty i łatwość stosowania powinna być nieodzownym

---

(57) Baran Z. "Problemy transmisji danych", WKiŁ Warszawa 1979.

(58) Kulikowski J.L. "Informacja i świat w którym żyjemy" Wiedza Powszechna Warszawa 1978.
Martin J. "Organizacja baz danych" PWN Warszawa 1983.
Michalewicz Z. "Zagadnienia bezpieczeństwa baz danych", PWN Warszawa 1982.
Miiler J. "Informacja w cybernetyce. Informatyka" MON Warszawa 1974.
Sokołowski A. "Ochrona informacji komputerowych" MON Warszawa 1987.

elementem systemów z teletransmisją. Oddzielnym zagadnieniem są konkretne metody szyfrowania oraz dobór i przechowywanie kluczy. Ponadto przy stosowaniu teletransmisji uwagę należy także zwrócić na zagadnienie identyfikacji i uwierzytelniania, a również szczegółowe zabezpieczenie samego szyfratora. Wyraźnie daje się zauważyć, że w przypadku teletransmisji dominują metody programowe, jednak nie należy pomijać metod fizycznych i organizacyjnych. głównie przy ochronie linii przesyłu oraz central telekomunikacyjnych. Bez uwag do chwili obecnej pozostają jedynie światłowody.

D. Wymogi stawiane instytucjom.

Należy rozpatrywać je w dwóch grupach. Pierwsza to użytkownicy linii teletransmisyjnych. Ich obowiązkiem musi być szyfrowanie danych oraz przestrzeganie obowiązujących w tym zakresie norm i przepisów. Od strony kadrowej osoby mające dostęp do bloków szyfrowania powinny być objęte ochroną operacyjną. Wymagane jest prowadzenie rejestracji seansów teletransmisji i kontrolowanie ich prawidłowości. W wypadku przesyłania danych niejawnych konieczne jest periodyczne powtarzanie procesu uwierzytelnienia i identyfikacji podczas trwania seansu. Grupa druga to dysponenci linii transmisji danych. Do ich obowiązków w aspekcie ochrony należy zapewnienie ochrony linii i central. Praktycznie poza przypadkami specjalnymi możliwe będzie jedynie stworzenie systemu sygnalizacji występujących zakłóceń i nieprawidłowości, które świadczyć mogą o ewentualnościach infiltracji. Tym bardziej uwypuklić należy szyfrowanie.

E. Zadania jednostek resortu spraw wewnętrznych.

W aspekcie ochrony systemów informatycznych z teletransmisją polityka zadań powinna być prowadzona dwutorowo. Poza uwzględnieniem osób mających dostęp do urządzeń szyfrujących należy szczegółową opieką otoczyć proces szyfrowania. Procedury szyfrowania, przechowywania i aktualizacji kodów powinny być objęte kontrolą operacyjną i formalną. Konsekwentnie należy również egzekwować prowadzenie rejestracji seansów i czynności uwierzytelniania i identyfikacji. Istotne to być może w razie wystąpienia zagrożenia bądź przestępstwa komputerowego. Druga grupa zadań to kontrola dysponentów linii telekomunikacyjnych oraz urządzeń peryferyjnych szczególnie tam gdzie występują informacje o charakterze niejawnym.

3. SYSTEMY INFORMATYCZNE - PUNKTY PRZYGOTOWANIA NOŚNIKÓW INFORMACJI.

W systemie tego typu spotykamy się z rzekomym brakiem zagrożeń i ignorancją z tego powodu metod ochrony.

A. Struktura systemu.

Wyróżnimy tu cztery podstawowe elementy. Dokumenty źródlowe, z których dane są wprowadzane, urządzenie do wprowadzania danych wraz z nośnikami, personel oraz transport nośnikow do miejsca przeznaczenia. Cechą charakterystyczną jest rownież własność programow przetwarzajacych i danych w systemie, w ktorym nośniki są wprowadzane do komputera i przetwarzane (por. rysunek nr.4).

B. Ocena aktualnego stanu ochrony.

W poszczególnych badanych przypadkach jest ona diametralnie różna i uzależniona była w zasadzie od wyobraźni decydentów i ich stopnia uświadomienia co do potencjalnej możliwości wystąpienia zagrożeń. Z jednej strony dane, które powinny być chronione nie podlegały żadnej metodzie ochrony, głównie oparte to było na przekonaniu o bezzasadności bezpieczeństwa (np. NBP), z drugiej dane na nośnikach były identyfikowane kodem i nieczytelne bez odpowiedniego klucza. I to zarówno na samym nośniku jak i w ośrodku, ktory te dane przetwarza (np. PKO SA).

Zarejestrowano niechęć do przyjmowania do wiadomości możliwości zagrożeń i odsuwanie problemów ochrony na jak najdalszy plan i okres.

C. Wystepujące w systemie potrzeby.

Z racji faktu, że typowe metody fizyczne (strażnicy, klucze itp.) oraz organizacyjne są stosowane sporadycznie należy zwrócić szczególną uwagę na osoby wprowadzające dane, szczególnie te o charakterze niejawnym. Metody organizacyjne dotyczyć muszą obiegu dokumentów oraz postępowania z makulaturą i nośnikami rezerwowymi. Zadbać należy rownież o transport nośników do miejsca przetwarzania. W 62% badanych przypadków nośniki były po prostu zanoszone przez jedną osobę. W przypadku danych szczególnie wrażliwych pożądane byłoby szyfrowanie nanoszonych na wynikowy nośnik danych lub taka ich organizacja, aby w miejscu przetwarzania (lub gdzie mogłyby być nielegalnie odczytane) nie można było na ich podstawie uzyskać wiarygodnych informacji. Przewidzieć należy rownież zabezpieczenie w pakietach programowych przetwarzających dane, tak aby osoby niepowołane, a mające dostęp do systemu przetwarzajacego nie mogły danych infiltrowac.

D. Wymogi stawiane instytucjom.

Poza metodami fizycznymi oraz organizacyjnymi, które powinny byc udokumentowane i kontrolowane, na etapie tworzenia pakietów programowych u dysponenta systemu przetwarzającego należy wprowadzić zabezpieczenia programowe celem uniknięcia infiltracji danych przez osoby obsługujące

komputer. W przypadkach danych wrażliwych, osoby mające do nich dostęp powinny być objęte ochroną operacyjną. Zabezpieczony powinien być również transport nośników oraz procedury w sytuacjach awaryjnych.

E. Zadania jednostek resortu spraw wewnętrznych.

W omawianym typie systemów ze względu na dwóch co najmniej dysponentów istnieje duże prawdopodobieństwo usiłowania zrzucenia odpowiedzialności na drugą stronę lub powierzenie ochrony przez właściciela danych dysponentowi komputera. Ktoś z zewnątrz powinien rozstrzygnąć ten problem i wyegzekwować przydział i podział odpowiedzialności zgodnie z istniejącym stanem rzeczy. Powinna również istnieć zewnętrzna kontrola obiegu dokumentów oraz transportu nośnika.

4. SYSTEMY OPARTE NA MIKROKOMPUTERACH.

Obecny wzrost ich występowania przekroczył wszelkie oczekiwania. Pojawiły się i pojawiają w każdej instytucji każdego szczebla i każdej gałęzi.

A. Struktura systemu.

W formie podstawowej to mikrokomputer (mikroprocesor), płyta główna, monitor, klawiatura, drukarka, stacje miekkich dysków, dysk sztywny. Ponadto często występują: ploter, streamer i modem. Jako nośniki poza dyskiem sztywnym używane są dyskietki i taśmy streamera. Specyfika tego systemu polega na tym, że każdy z w/w elementów możliwy jest do przeniesienia w rękach, a całość mieści się na większym biurku (59).

B. Ocena aktualnego stanu ochrony.

Ponieważ elementy tego systemu są stosunkowo drogie i posiadają niewielkie gabaryty na ogół są dobrze zamknięte. Ujawniono przypadki zamknięcia całego systemu przez dyrektora i niedopuszczenie do niego nikogo. Sam dyrektor nie znał się na komputerach, a zestaw kupiony za sporą kwotę nie był w ogóle rozpakowany. Nie mniej środki fizyczne w tym zakresie należy ocenić pozytywnie. Występują kraty w oknach, drzwi obite blachą i systemy alarmowe. O wiele więcej do życzenia przedstawiała strona software'owa. Rozpowszechniła się tendencja do ładowania w pamięć mikrokomputera dokładnie wszystkiego, kupuje się gotowe pakiety bądź konstruuje indywidualne dla własnych potrzeb. Jedynym zabezpieczeniem występującym masowo jest forma metody programowej-hasło (60). Przewidują ją kolejne wersje

---

(59) Porównaj przypis Nr 32 w niniejszej rozprawie.

(60) Zob. Blatchford C.W. "Computer Crime, the need for data Security", Management Services 1986 Nr 9.

dBase, najpopularniejszego narzędzia konstrukcji baz danych. Jest to zabezpieczenie najpowszechniejsze i zarazem najsłabsze. Na to rzutuje popularność dBase i stosunkowo prosta procedura dotarcia do hasła, a zatem i do zgromadzonych danych. Ponadto ze względów użytkowych praktykowane jest tworzenie rezerwowej bazy danych umieszczonej na dysku sztywnym. Duplikat przechowywany jest bądź na dyskietkach bądź na tasmie streamera. Występujące metody organizacyne pozwalają na przechowywanie nośnikow typu dyskietka czy taśma w szafach pancernych, pomijają one jednak zazwyczaj mozliwość skopiowania zbioru bezpośrednio ze sztywnego dysku. Podobnie lekceważone są procedury identyfikacji i uwierzytelniania, a w praktyce administrator systemu ma swobodny dostęp do wszystkich danych. Nieprzestrzegana jest rowniez higiena pracy na mikrokomputerze w aspekcie czynnosci antywirusowych, a stosowanie szczepionek ochronnych występuje niezwykle rzadko.

C. Wystepujące w systemie potrzeby.

Problemy ochrony w systemach informatycznych opartych na mikrokomputerach są zagadnieniem całkowicie nowym. O ile w kwestii zasad i metod ochrony w tak zwanej "ciężkiej informatyce" powstało wiele opracowań, drobiazgowo niejednokrotnie omawiających poszczególne punkty systemów pominięta jest ta problematyka w przypadku mikrokomputera. Symptomatycznym jest fakt, że z powodu odmiennej struktury i działania nie można przenieść metod i zasad ochrony w ich pełnej postaci, a większość z nich chociaż będzie miała zastosowanie, to jednak zasadniczo zmieni swe miejsce w hierarchii ważności. Nie do pomyślenia była np. w przypadku duzych komputerów kradzież jednostki centralnej.

Nastepujące problemy rzutują na politykę ochrony mikrokomputerowego przetwarzania. Po pierwsze, małe gabaryty wszystkich elementow systemu mikrokomputerowego rzutują na stosowanie metod fizycznych. Dotyczy to głównie nośników informacji. Wspominano w niniejszej pracy, że napęd dysku sztywnego będący wielkości kasety magnetowidowej kosztuje 3 lub 6 mln zł., a o jego zawartości wręcz nie wypada wspominać. Powszechność stosowania i jednolite standardy powodują, że grono osob potrafiących obsługiwać prawie każdy mikrokomputer jest niewyobrażalnie wielkie. Z racji przechowywania na jednym dysku sztywnym wielu baz danych, dostęp do systemu ma wiele osób, a administrator może z reguły swobodnie penetrować wszystkie zbiory. Systemy alarmowe jeżeli są instalowane powinny sygnalizować nie tylko próbę dotarcia do danych ale i kradzież software'u i hardware'u. Niewypracowane są odrębne zasady polityki ochrony, a całe postępowanie w tym zakresie przyjmowane jest z reguły per analogia. Czas kopiowania całych dyskietek jest rzędu sekund, a dostęp do nośników czystych nie przedstawia żadnych problemów. Kierownictwa jednostek użytkujących systemy nie są zorientowane w podstawowych problemach i uzależnione są od specjalistów, niejednokrotnie

z innych przedsiębiorstw. Nie występuje izolacja sprzętu i integracja personelu obsługujacego jak w przypadku dużych ośrodków obliczeniowych. W podawanych wymogach dla mikrokomputerow w 92% nie pojawił się problem zabezpieczenia zbioru w ogóle. Odrębnym tematem jest obecne zagrożenie wirusami komputerowymi, ochrona przed nimi, leczenie i profilaktyka z higieną włącznie.

Tego rodzaju problemów jest wiele i one stymulują konieczne do zastosowania metody. Wsród nich wyrożnimy organizacyjne, fizyczne oraz programowe.

Metody organizacyjne :

Z każdym zakupionym komputerem, lub mikrokomputerami powinno się wiązać przyjęcie na etat przeszkolonego człowieka. Dostęp do mikrokomputera powinien być rejestrowany (równolegle kontrolowany software'owo). Osoba odpowiedzialna za system nie powinna mieć dostępu do parametrow uzbrajających. Pomieszczenie powinno być okratowane, drzwi zabezpieczone odpowiednio i plombowane. Nośniki wymienne powinny się wyróżniać określoną cechą i być odpowiednio przechowywane. Stanowisko pracy musi być tak ustawione aby dostęp wizualny miała tylko osoba obsługująca. Sprzątanie pomieszczeń powinno odbywać się w obecności osoby odpowiedzialnej.

Metody fizyczne :

Wiażą się z nimi nastepujace sprawy. Zamki w drzwiach powinny być takie aby uniemożliwić wyjęcie klucza po otwarciu, a klucz powinien być każdorazowo zdawany. Plombować powinna osoba spoza personelu systemu. Komputer powinien mieć osobne, ewentualnie ukryte wyłączanie zasilania. Telefon jeżeli jest w pomieszczeniu mikrokomputera powinien uniemożliwić przesyłanie danych. Niezbędna jest sygnalizacja alarmowa.

Metody programowe :

Do podstawowych zasad ich stosowania zliczymy fakt, że poza standartowym hasłem należy opracować taki tryb zabezpieczeń, aby nie można było uzyskać dostępu do zbiorów szczególnie wrażliwych. Ponadto powinna istnieć procedura niepozwalająca na wprowadzanie programów narzędziowych. Parametry uzbrajające, hasła powinny być tak wprowadzone i ulokowane, aby nikt nie miał dostępu do innego poza swoim (dotyczy głównie specjalistów obsługujących systemy). Szczególnie wrażliwe dane powinny być szyfrowane.

Wymienione wyżej rozwiązania i propozycje nie wyczerpują całego zestawu możliwych zabezpieczeń, głównie ze względu na olbrzymi postęp w dziedzinie mikrokomputerów oraz dostępności, która pozwala na rozwój wszechstronnej inwencji w łamaniu ochrony.

D. Wymogi stawiane instytucjom.

W kwestii ochrony systemów informatycznych opartych o mikrokomputery zakłady uzytkujące je zobowiązane są przede wszystkim do zabezpieczenia pomieszczeń w których będą one użytkowane oraz zapewnienia odpowiednich procedur administracyjnych w celu zabezpieczenia wymienionych wyżej problemów. Ponieważ oprogramowanie i bazy danych są autonomiczne przewidzieć również należy zabezpieczenie metodami programowymi. Udokumentowany być musi podział odpowiedzialności oraz metody dostepu do zbioru. Osoby mające dostęp i znające system powinny podlegać ochronie operacyjnej w stosownych przypadkach.

E. Zadania jednostek resortu spraw wewnętrznych.

W obszarze zastosowań mikrokomputerów przy obecnej tendencji stosowania ich do wszystkiego i wszędzie oraz wystepującej z reguły jedno lub dwuosobowej obsłudze nadzór zewnętrzny musi być kwalifikowany. W koniecznych przypadkach odpowiedni pracownicy powinni kontrolować zawartość pamięci oraz skuteczność procedur bezpieczeństwa. Podczas badań stwierdzono próby opracowań planów na wypadek MOB na zakładowym mikrokomputerze kompletnie niezabezpieczonym. Poza tym odpowiednie są rutynowe czynności jak w poprzednich przypadkach.

5. SYSTEMY INFORMATYCZNE ZŁOŻONE Z MIKROKOMPUTERÓW POŁĄCZONYCH W SIEĆ.

Do grupy tej zaliczymy zarowno połączenia równoległe komputerów jak i wyspecjalizowane pakiety i urządzenia sieciowe (np. D-LINK) (61).

A. Struktura systemu.

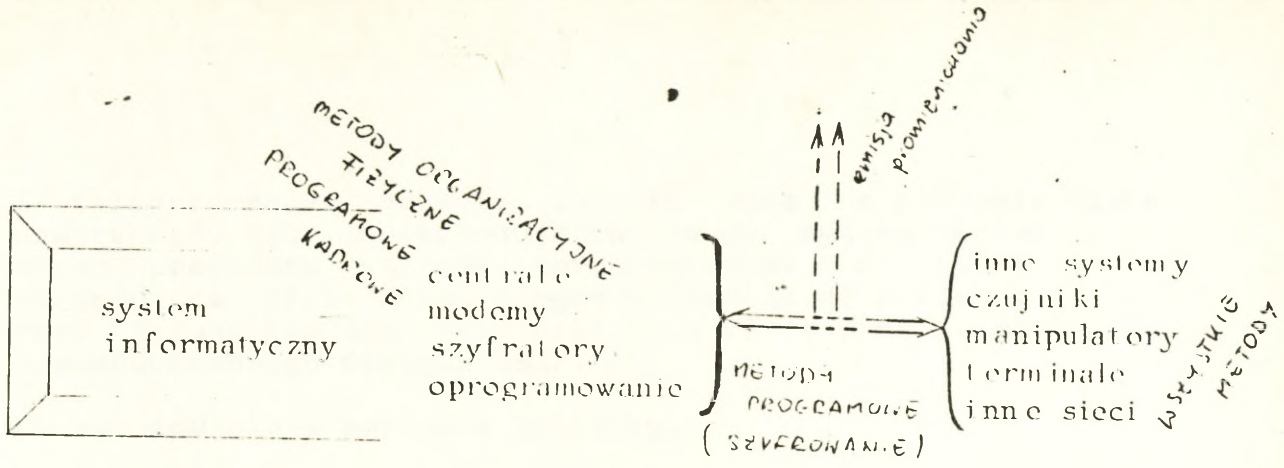
Przedstawiony na rysunku nr.6 system charakteryzuje się możliwością przesyłania danych z jednego mikrokomputera do drugiego, użytkowaniem wspólnie pamięci i urządzeń peryferyjnych. Najczęściej występuje tzw. "komputer matka" nadzorujący pracę całej sieci.

B. Ocena aktualnego stanu ochrony.

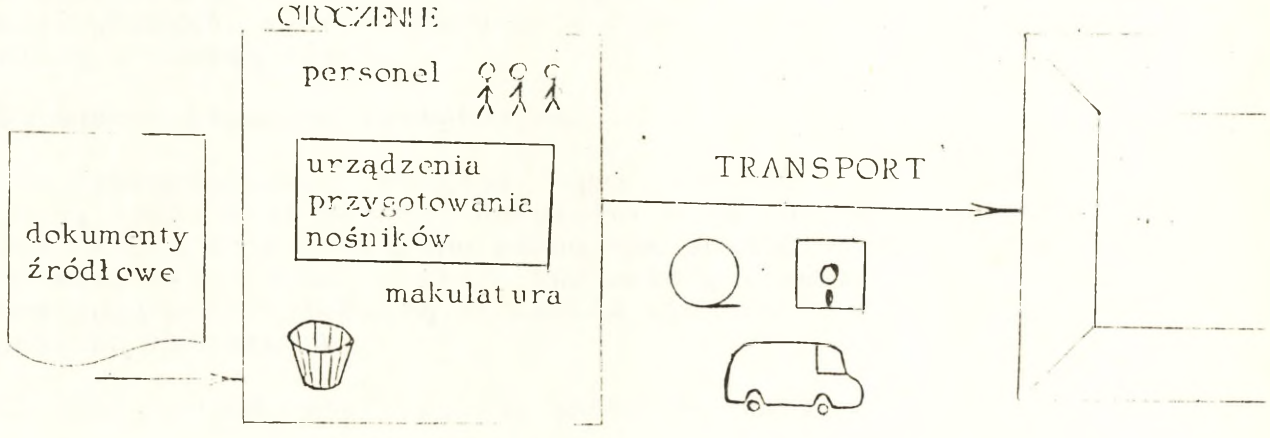
W przypadku sieci prostych dostępnych w kraju proponowane jest powszechnie stosowanie hasła nie mniej większość z nich nie jest w pełni wdrożona i sprawdzona, a zatem trudno mówić o ich stanie bezpieczeństwa. Odmiennie przedstawia się problem sieci wyspecjalizowanych. Autor napotkał i miał możliwość zapoznać się z siecią mikrokomputerową IBM System 36 . Wielostanowiskowa

---

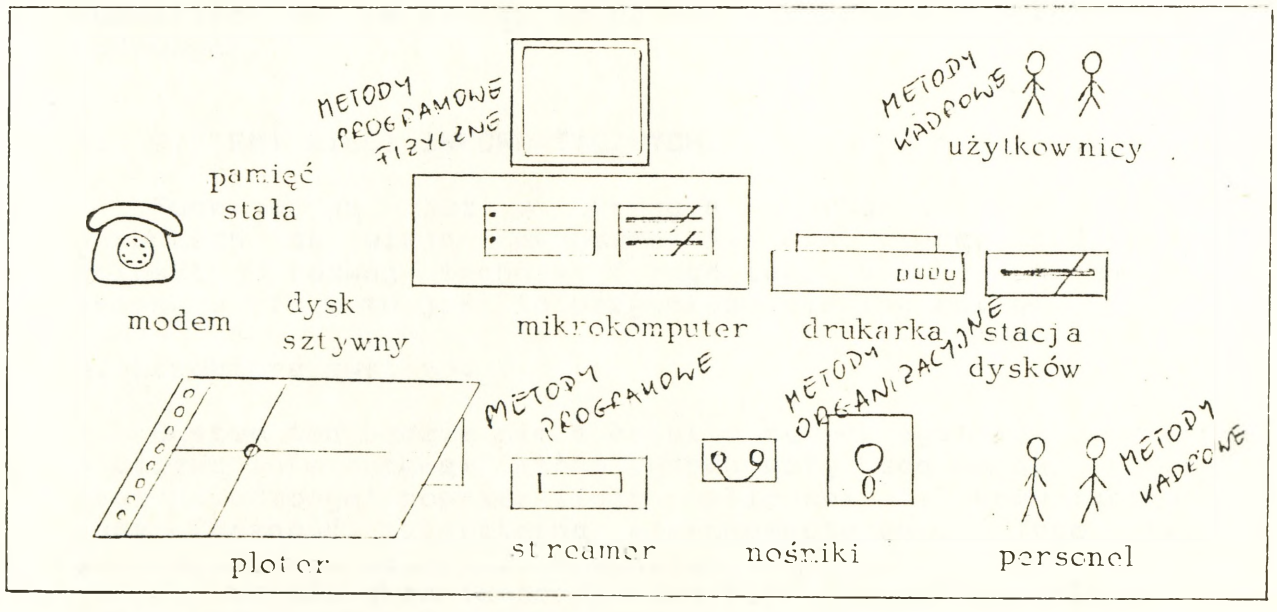
(61) Por. Orkiszewski J. "Jeden dla wszystkich - systemy wielodostępne", Mikroklan 1986 Nr 1.



RYS.3. Metody ochrony w systemie informatycznym z teletransmisją.



RYS. 4. Metody ochrony w systemie informatycznym - punkcie przygotowania nośników.



RYS. 5. Metody ochrony w systemie mikrokomputera.

i wieloprogramowa pozwala chronić dane na poziomie hasła czy rekordu (62). Funkcjonuje co prawda system haseł, nie mniej procedury są tak zorganizowane, że tylko osoba zakładająca daną bazę danych ma dostęp do swoich zbiorów. Przewidziano blokadę terminali oraz alarm oraz rejestrację nieupoważnionego dostępu (63).

C. Wystepujące w systemie potrzeby.

Sieć mikrokomputerów to możliwość posługiwania się wspólnymi zasobami oraz dostęp do zbiorów z odległego miejsca. Całokształt potrzeb wyczerpuje w zasadzie IBM System 36, gdzie od strony software'owej przewidziano na normalnym poziomie kompletne i dosyć skuteczne zabezpieczenie. Metody fizyczne są analogiczne do pojedyńczych mikrokomputerow z tym, że objąć one również muszą przewody sieci.

D. Wymogi stawiane instytucjom.

Zabezpieczenie takiego typu jak omówiono powyżej ma jedną wadę. Musi istnieć dokument, w którym zebrane są hasła lub klucz dzięki któremu można się dostać do zbioru haseł. To musi skutecznie zabezpieczyć metoda organizacyjna. Osoby redagujące architekturę elementów systemu powinny być objęte ochroną operacyjną.

E. Zadania jednostek resortu spraw wewnętrznych.

Powinny polegać na wykwalifikowanej kontroli funkcjonowania systemu ochrony. Kontrole należy przewidzieć sukcesywne, uwzgledniając wiele wariantów naruszeń norm ochrony. W omawianym przypadku IBM 36 przy dwóch terminalach stwierdzono zapisanie hasła na biurku i ściennym kalendarzu. Pozwoliło to na dostęp do bardzo rozbudowanej bazy danych kadrowych.

6. SYSTEMY SIECI INFORMATYCZNYCH.

Funkcjonują już w krajach zachodnich, w naszych warunkach są wizją przyszłości, ale biorąc pod uwagę kolosalny rozwój techniki i jego tempo a także dynamiczne zmiany w kraju to jest to przyszłość nie tak odległa.

A. Struktura systemu.

System ten będzie się składał z dużych systemów opartych o ciężką informatykę, które dysponowały będą bazami danych, oraz połączonymi poprzez linie publiczne, telekomunikacyjne bądź łącznością satelitarną mikrokomputerami. Tego typu

---

(62) Wdraża obecnie ten system PEUT "Exbud" w Kielcach.
(63) Por. Szuniewicz R. "Minstrel 4 EP wielodostep na wielu procesorach", Mikroklan 1987 Nr 8.

systemy juz funkcjonujące na zachodzie (np. EURONET), wymieniają się miedzy soba informacjami gwarantując pełne możliwości wykorzystania zdobyczy informatyki.

C. Wystepujące potrzeby.

Ochrona koncentrować się będzie poza ochroną autonomiczną poszczególnych elementów sieci, na ochronie transmisji oraz blokowaniu wejść systemowych przed infiltracją aktywną - programową. Brak takiej ochrony zaowocował w krajach zachodu rozprzestrzenieniem się poprzez łącza telefoniczne epidemii wirusów komputerowych. Doprowadziło to do katastrofalnych skutków, głównie w postaci utraty danych, których usuwanie trwało bardzo długo (w wielu punktach dane zostały utracone bezpowrotnie, a efekty działania wirusów pociagnęły za sobą wielomilionowe straty finansowe). Jednak obecnie poprzez systemy sieci informatycznych rozsyłane są szczepionki przeciwwirusowe oraz niektóre systemy zarażone mogą być leczone (64).

D. Zadania jednostek resortu spraw wewnętrznych.

Koncentrować się będą na kompleksowej ochronie sieci, jednak na obecnym poziomie techniczno-naukowym w resorcie realizacja zadań w tym zakresie byłaby conajmniej utrudniona.

7. METODY OCHRONY BAZ DANYCH.

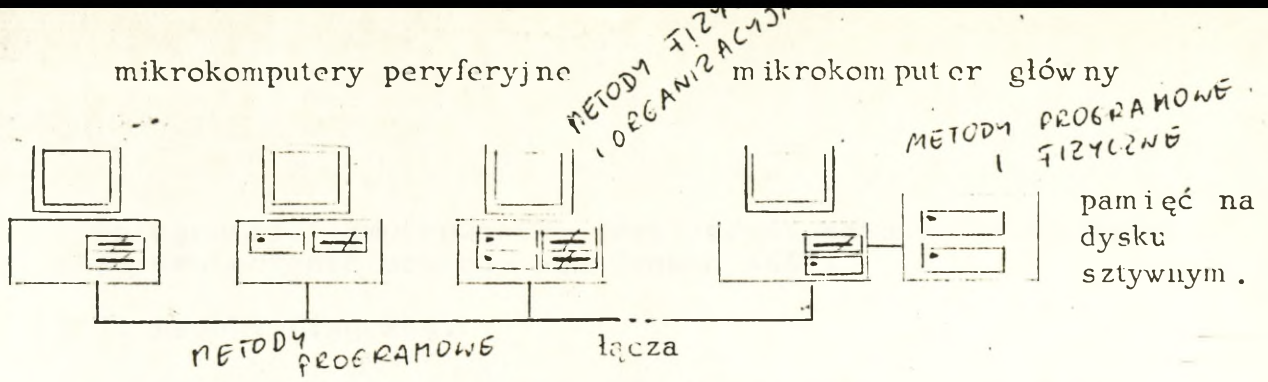
Bazy danych stanowią najwrażliwszy element systemu informatycznego każdego typu i każdej konfiguracji. Rozpatrywać je będziemy w dwóch aspektach - programowym oraz fizycznym (por. rysunek nr.8).

7.1. Aspekt programowy.

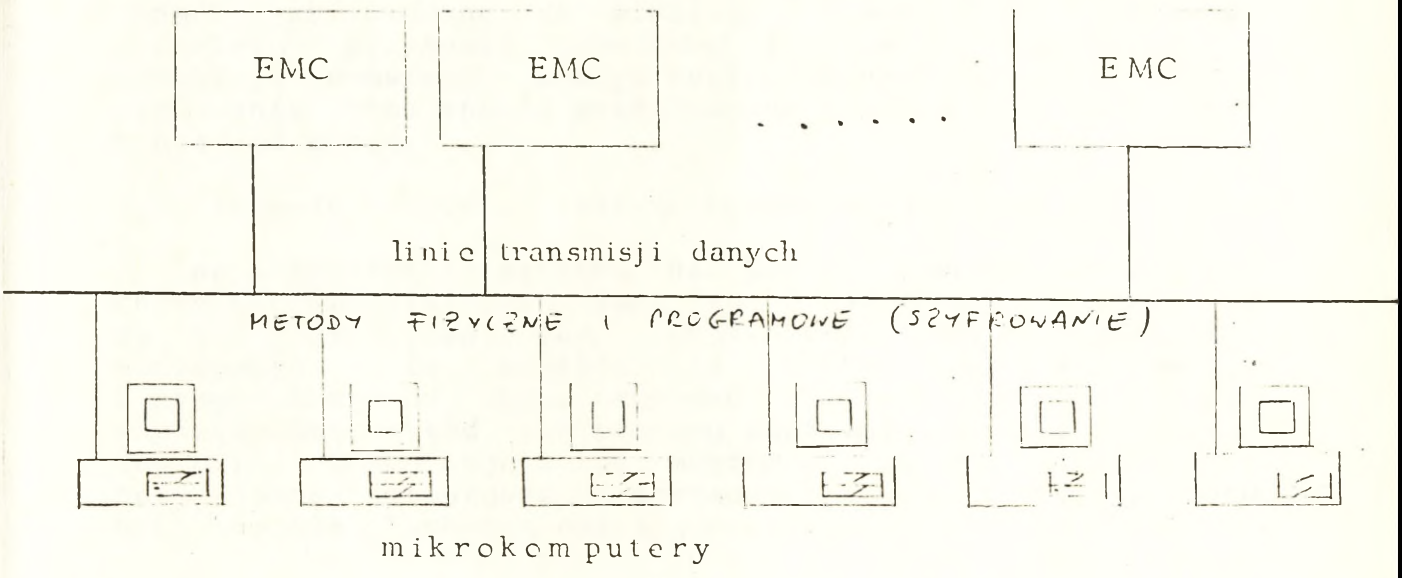
Związany jest z logiczną strukturą bazy danych oraz jej zawartoscią. Dostęp do bazy danych może nastąpic poprzez system operacyjny lub programy użytkowe. One to właśnie powinny przewidzieć programowe blokady dostępu bez upoważnienia, one również winny udostępniać (czyli pozwolić czytać, aktualizować lub kasować) odpowiednie typy danych zgodnie z posiadanym upoważnieniem. Ponieważ istnieje ryzyko próby odczytywania bazy danych poza osłoną programową systemu operacyjnego lub programów użytkowych najbezpieczniejszym sposobem na zabezpieczenie logiczne bazy danych jest jej zaszyfrowanie. Moze być ono najprostsze i polegać na oddzieleniu identyfikatorów od danych, a może przyjąć subtelne i wyrafinowane formy z dziedziny

---

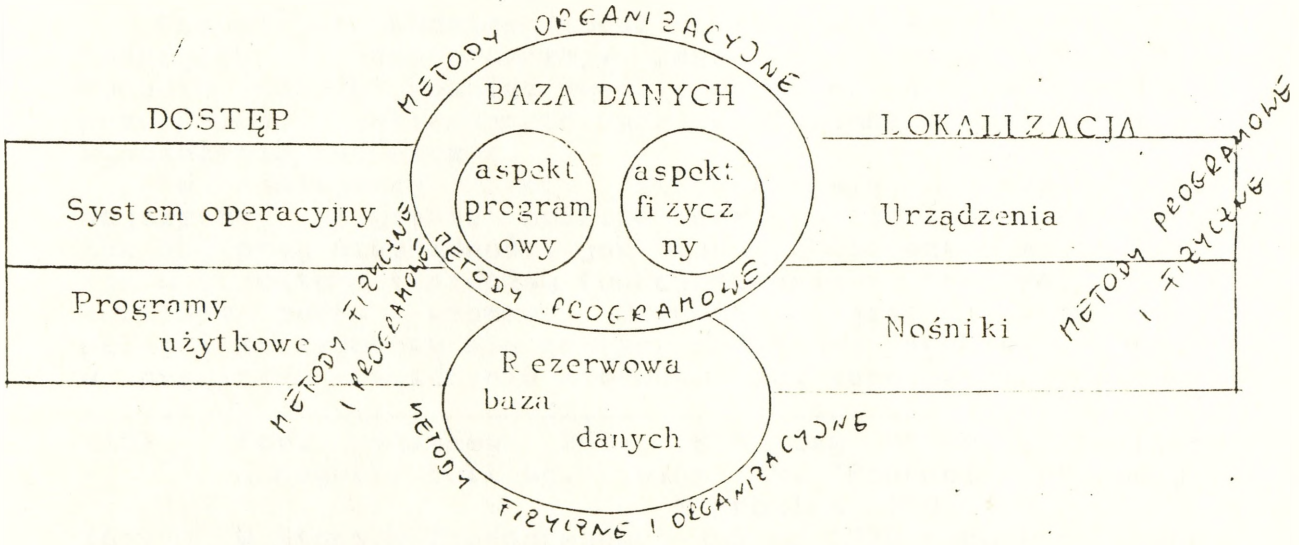
(64) Należy zwrócić uwagę na konieczność szyfrowania informacji przesyłanych w sieciach zob. Topolewski Z. "Ochrona informacji w sieciach komputerowych" Nowator 1987 Nr 7 - 8.



RYS. 6. Metody ochrony w systemach mikrokomputerów połączonych w sieć.



RYS.7. Metody ochrony w systemach informatycznych sieciowych.



RYS.8. Metody ochrony i problemy baz danych.

kryptografii. Szyfrowanie jest jedyną metodą, gwarantującą dużą skuteczność ochrony baz danych (65).

7.2. Aspekt fizyczny.

Przejawia się on w tym, że każda baza danych musi być umiejscowiona na jakimś nośniku, w jakimś urządzeniu. Metody ochrony fizyczne oraz organizacyjne winny wypełnić lukę w barierze ochronnej. Urządzenia i nośniki powinny być zamykane, a możliwość kradzieży nośnika lub skopiowania bazy danych zredukowana do minimum. Potencjalna możliwość kradzieży przemawia dodatkowo za metodą szyfrowania. Odrębnego omówienia wymaga rezerwowa baza danych, której ulokowanie oraz sposób przechowywania muszą być specjalnie brane pod uwagę.

7.3. Zadania jednostek resortu spraw wewnętrznych.

Na płaszczyźnie ochrony baz danych zadania muszą mieć charakter kwalifikowany. Bazy muszą podlegać kontroli co do ich umiejscowienia, użytkowania oraz możliwości kopiowania. Ze względu na fakt, że są jednym z najwrażliwszych ogniw systemu powinno się do badania skuteczności metod ich ochrony stosować techniki symulacji zagrożeń. Osoby mające lub mogące mieć kontakt i dostęp do bazy ponad normatywne programowe dopuszczenie powinny być objęte ochroną operacyjną (66).

8. MODEL OCHRONY W ASPEKCIE FUNKCJI RESORTU SPRAW WEWNETRZNYCH.

Rozpatrywać będziemy model ochrony w trzech podstawowych funkcjach : rozpoznawczej, zapobiegawczej i wykrywczej. Ponadto należy również zwrócić uwagę na system szkolenia pracowników realizujących wyżej wymienione zadania oraz na wyposażenie techniczne.

W niniejszej pracy starano się przedstawić jak najszerzej wszystkie możliwe poziomy i metody ochrony, tak aby przy niezbędności jak najdokładniejszego zagłębienia się w strukturę i procesy funkcjonowania systemu dać pewien możliwie pełny wzorzec. Oczywiście jest to model zbyt pełny i szczegółowy dla potrzeb codziennej praktyki, jednak w przypadku uściślenia kierunku zainteresowania, podania

---

(65) Por. systemy DES, RSA czy kartę CP-8 firmy Honeywell Bull wg. Liwinski R. "Poufność informacji" Mikroklan 1987 Nr 3.

(66) W Stanach Zjednoczonych już od 1978 roku Departament Obrony realizuje "Computer Security Initiative Program". W ramach tego programu opracowywane są, i wypróbowywane różne metody ochrony baz danych. Zob. "Bezpieczeństwo systemów komputerowych" Przegląd Techniczny, Wiadomości i Propozycje. 1987 Nr 14.

problemu, poziomu lub zagrożenia można się nim posłużyc dobierając odpowiednie partie.

8.1. Aspekt rozpoznawczy.

Jak juz wspominano podstawowym materiałem jakim posługują się jednostki resortu spraw wewnętrznych podczas realizacji swoich zadań na wszystkich płaszczyznach jest informacja. Ona rownież jest podstawą podczas realizacji funkcji rozpoznawczej w zakresie ochrony systemów informatycznych.

Przy aspekcie rozpoznawczym należy wspomnieć o trzech dodatkowych problemach :

Pierwszy to sposoby zbierania informacji. W praktyce resortu stosuje się zdobywanie jej drogami oficjalnymi, przez rozmowy w różnej formie lub analizę dokumentow i stanu faktycznego. Inną metodą są czynności operacyjne czyli zdobywanie informacji w sposób niejawny przy pomocy osobowych źródeł informacji lub środków techniki operacyjnej. Pomimo tych formalnych nazw problem współpracy np. w naszym przypadku z jednostkami realizujacymi funkcje jednostek resortu spraw wewnętrznych jest normalny i oczywisty na każdej szerokości geograficznej. Podobnie na całym swiecie stosuje się w celu zdobycia konkretnej wiedzy najnowsze zdobycze techniki.

Drugi to moment w którym ta informacja jest potrzebna bądź pewna cykliczność jej zdobywania. Literatura podaje w tym przypadku takie rodzaje źrodeł jak sygnalne, doraźne, manewrowe itd. (67). Rozwiązanie zaowocuje na bazie doświadczenia pracownika i aktualnych realiow konkretnej sytuacji.

Trzeci to zespół cech charakterystycznych informacji takich jak jej terminowość, kompletność, trafność, wiarygodność itp. Równolegle zwrócić uwagę należy nie tylko na końcowego adresata informacji ale i kanał jej przesyłu i jego kompetencje (potencjalne wystąpienie szumów) bądź wypatrzenia w przypadku gdy pracownik konkretnie ją odbierający od źrodła nie jest zorientowany w temacie którego ona dotyczy.

Podsumowywując aspekt rozpoznawczy ważnym wydaje się fakt, ze w stosunku do nastepnych jest on i pierwotny i wtórny. On będzie stymulował aspekt zapobiegawczy oraz potwierdzał i uzupełniał informacje w procesie wykrywczym.

8.2. Aspekt zapobiegawczy.

Również realizowany dwiema drogami jawną i operacyjną. Zainspirowany moze być na bazie rutynowej zaplanowanej kontroli ujawniającej potencjalne możliwości zagrożeń.

---

(67) Korepta L. Matula E. "Praca operacyjna Służby Bezpieczeństwa" Departament Szkolenia i Doskonalenia Zawodowego MSW Warszawa 1984.

Jednak jedna z zasad Murphy'ego głosi, że gdy obiekt sprawdzany wie o tym że jest kontrolowany pracuje na ogół bez zarzutu łacznie ze stale psującymi się elementami, nie tak jak codziennie. Zapobieganie na bazie informacji operacyjnej, wyczucia pracownika czy też jego doświadczenia w konkretnym problemie pozwoli na rzeczywiste zapobieżenie mogącemu wystąpić zagrozeniu. Dodatkowo zapobiegać można rownież drogą operacyjną gdy czynności neutralizujące zarzewie zagrożenia wykonuje osobowe źródło informacji.

8.3. Aspekt wykrywczy.

Najtrudniejszy i zarazem najbardziej odpowiedzialny. Kłopotliwe jest to, że poza zdobyciem informacji należy ją udokumentować i to w ściśle przewidzianej normami formie i także w miarę możliwości poprzeć dowodami co jak wykazaliśmy w przypadku przestępstw komputerowych jest niesłychanie skomplikowane.

8.4. System szkolenia pracowników realizujących funkcje resortu spraw wewnętrznych.

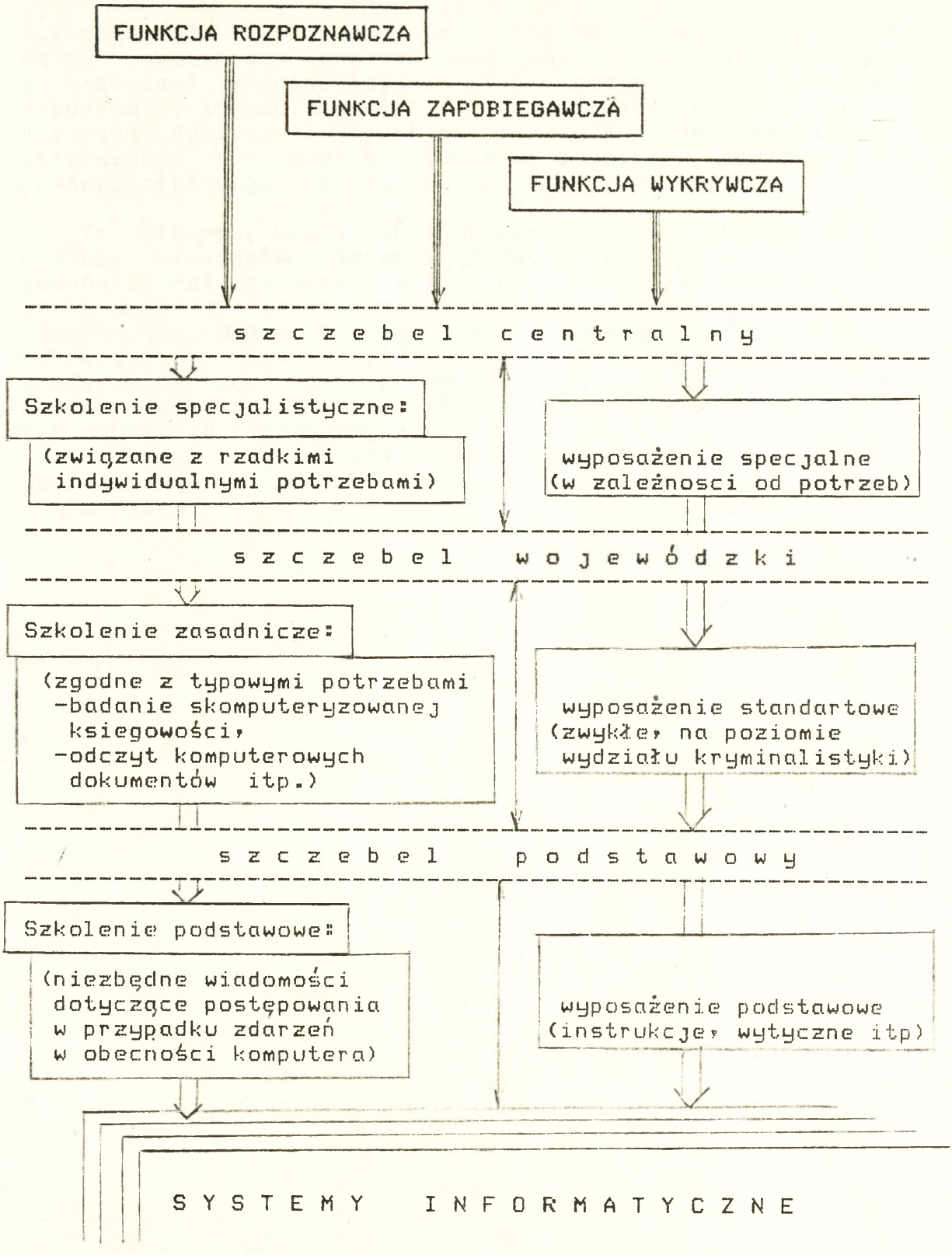
Został juz wstępnie omówiony jednak warto chyba podejść również do problemu perspektywicznie (68). Niezbędne jest takie ułożenie szkolenia aby pracownicy mający do czynienia z zagadnieniami ochrony nie byli kompletnymi dyletantami. I tak już zmuszeni są w niewielkim zakresie posługiwać sie systemami chociażby obsługując automatyczną informację na dworcu kolejowym. Jednak na szczeblach podstawowych pracownik musi mieć instrukcyjnie podane co ma robić i o czym pamietać gdy podczas wykonywania podstawowych czynności natknie się na jakąś formę systemu komputerowego. Podobnie analizując różne formacje i specjalności wśród pracowników konieczne jest szczegółowe określenie dolnego pułapu obszaru wiedzy jaki pracownik na danym stanowisku musi mieć opanowany. Co więcej, w związku z faktem, że informatyka jest jedną z najbardziej i najszybciej ewoluujących dyscyplin nauki i życia to rownież należy przewidzieć w procesie szkolenia. Szkolenie pracowników na szczeblu centralnym powinno być tak zrealizowane, aby mógł być rozwiązany każdy problem z dowolnej dziedziny informatyki. Implikuje to staże za granicą lub ścisłą współpracę z jednostkami cywilnymi.

8.5. Wyposażenie techniczne.

Uwarunkowane jest oczywiście zasobnoscią jednostek, niemniej niezbędnym wydaje się aby na szczeblu wojewódzkim drobne ustalenia (t.j. większość z tej pozycji) mogły być

---

(68) W celu jak najszybszego usunięcia braków w know-how o przestepczości komputerowej, FBI szkoli agentów na trzytygodniowym kursie w Akademii FBI w Quantico (Wirginia) gdzie laicy stają się specjalistami. Por."Computerkriminalitat", Kriminalistik 1984 Nr 12.



Rys.9. Model ochrony systemów informatycznych w aspekcie funkcji jednostek resortu spraw wewnętrznych.

wykonane bez odwoływania się do szczebla centralnego. Na dzień dzisiejszy powinny się one conajmniej pokrywać z zakładami kryminalistyki i ich możliwościami w zakresie ekspertz w innych sprawach. Zespół na szczeblu centralnym powinien dysponować sprzętem jaki tylko jest możliwy do osiągnięcia lub zapewnić sobie w przypadku sporadycznych konieczności użycia dostęp do sprzętu rzadkiego.

To główna grupa zadań i problemów w stosunku do modelu ochrony systemów informatycznych w aspekcie funkcji jednostek resortu spraw wewnetrznych. Wskazano w tej pracy wiele metod i rozwiązań techniczno-organizacyjnych, lub ich propozycji. Jednak najistotniejszym ogniwem każdego systemu ochrony jest i będzie człowiek. M.Wessel w swojej pracy (69) stwierdził, ze "czynnik ludzki stanowi ostatnią niewiadomą w rachunku komputerowym plusów i minusów. W grę wchodzą tu tak subtelne i nieuchwytne czynniki jak wpływ emocjonalny i intelektualny. Ich analiza i ocena mogą być najtrudniejsze, stając się w pewnych dziedzinach zadaniem najbardziej pilnym". Warto o tym pamiętać.

---

(69) Zob. Wessel M.R. "Komputer a społeczeństwo", WP Warszawa 1976.

Z A K O Ń C Z E N I E .

Ochrona systemów informatycznych w aspekcie funkcji jakie wykonywać powinny jednostki resortu spraw wewnętrznych to problem teraźniejszości i przyszłości. Zaistnienie ich w naszej rzeczywistości to kwestia najbliższych dni. Funkcjonowanie systemów informatycznych w naszym życiu to juz teraźniejszość, przestępstwa na nich i przy ich pomocy to również problem dnia dzisiejszego. Przeciwdziałanie przestępstwom nie powinno być odkładane, nowe struktury, nowe schematy działania powinny zaowocować również i w tym obszarze. Postępujące zachłystywanie się demokratycznymi swobodami nie powinno przesłonić realnej oceny sytuacji i to szczególnie na tych odcinkach gdzie skutki mogą być niewyobrażalne i pewne sprawy mogą być nie do odzyskania. Na bazie wieloletniego doświadczenia oraz prognoz rozwoju sytuacji należy stwierdzić, ze ochrona systemów informatycznych przy w takim tempie postępującej informatyzacji życia musi mieć zaplecze operacyjne nie tylko dla zabezpieczenia przed zagrożeniami ale i dla świadomej operacyjnej infiltracji tych ochranianych systemów przez jednostki resortu spraw wewnętrznych. Im więcej informacji umieszczanych będzie w bazach danych obsługiwanych przez systemy, im bardziej będzie miała być skuteczna praca policji i pokrewnych jej jednostek tym systemy informatyczne i ich bazy będą celem dla pracowników resortu. Można co prawda tłumaczyć, że formalnie za zgoda prokuratora lub sędziego śledczego każdą informację można będzie uzyskać nie mniej należy wziąć pod uwagę różnicę pomiedzy standartowymi nośnikami informacji a nośnikami wykorzystywanymi przez komputer (autor celowo nie poruszał tej kwestii wcześniej, ponieważ zabezpieczenie materiałów w tym i nośników dla potrzeb sądu to tematyka wchodząca w zakres wymiaru sprawiedliwości). Praktyka obecna działań z zakresu ścigania wskazuje, że większość materiałów przed przekazaniem ich do pionu sprawiedliwości jest co najmniej potwierdzana operacyjnie. Należy powiedzieć wyraźnie i bez zbędnego zakłamywania się, że metody operacyjne były, są i będą wykorzystywane, w ochronie systemów informatycznych również. Jest to wysoce skuteczne i wydajne narzędzie i w niniejszej pracy starano się pokazać pewne wzorce do jego wykorzystywania. Poza problemami pracy operacyjnej oraz wykorzystywaniem informacji zawartej w ochranianych systemach należy także wspomnieć o konieczności infiltracji środowiska informatycznego. Ludzi pracujących przy komputerach jest juz bardzo wielu (zachodnie źródła podają, że jest to co czwarty pracujący obywatel). Wielu jest także informatyków doskonale znających systemy, języki programowania, będącymi wspaniałymi fachowcami. Ale stosunkowo niewielka jest grupa ludzi będąca artystami w swojej dziedzinie, ludzi potrafiących "łamać" blokady ochronne, wdzierających się mimo przeszkód do każdego miejsca w systemie i powodujących, że komputer staje się powolnym im narzędziem. Ci ludzie powinni być znani

pracownikom resortu, a w przypadku pojawienia się poważniejszych perturbacji powinni być rozpatrywani jako potencjalni sprawcy przestępstw lub co najmniej współudziałowcy.

B. Goldstein twierdzi (70), że "nadejdzie taki dzień, gdy każdy oficer policji będzie posiadał przeszkolenie z technik komputerowych a władze regionalne będą dysponować własnymi ekspertami do spraw przestępstw elektronicznych. Przemysł komputerowy stworzył swój żargon na wszystko, dlaczego więc nie nazwać przyszłego oficera śledczego do spraw przestępstw komputerowych "compucop" (komputeroglina)." Do realizacji nowego typu zadań takich jak praca operacyjna w środowisku informatyków (trzeba z nimi umieć rozmawiać na tematy zawodowe), badanie skomputeryzowanych baz danych (np. księgowości), ochrona zabezpieczeń (podczas kontroli, symulacji oraz własnych czynności infiltracyjnych) i innych potrzebny jest nowy rodzaj policjanta, kontrwywiadowcy, pracownika resortu lub realizującego jego funkcje pracownika cywilnego takiego aby podołał nowym zadaniom a raczej starym zadaniom ale w nowym obszarze i na nowym sprzęcie.

Z myślą o takim rozwiązaniu pisana była niniejsza praca.

---

(70) B. Goldstein : "Electronic Frand : the Crime of the Future", International Criminal Police Review, 1985 Nr 391.

B I B L I O G R A F I A

1. Antyszpiegowskie okna.
   Nauka i technika - Serwis Zagraniczny, 1988, Nr 1453
2. Baran Z. - Problemy transmisji danych.
   WKiŁ Warszawa 1979.
3. Bezpieczeństwo systemów komputerowych.
   Horyzonty Techniki - Suplement, 1988.
4. Bezpieczeństwo systemów komputerowych.
   Przegląd techniczny-Wiadomości i Propozycje,1987,Nr 14.
5. Bielecki J. - Oprogramowanie mikrokomputerowych.
   WKiŁ Warszawa 1987.
6. Bielecki J. - System VSAM.
   WNT Warszawa 1987.
7. Blatchford C.W. - Computer Crime, the need for data Security.
   Management Services, 1986, Nr 9.
8. Borak S. Klaczak J. - System operacyjny George 3.
   WNT Warszawa 1981.
9. Braver H. - Forms of Computer Abuse.
   Revija za kriminalistiko in kriminologijo, 1982, Nr 2.
10. Yaohan Chu - Organizacja i mikroprogramowanie maszyn cyfrowych.
    WNT Warszawa 1979.
11. Computerkriminalitat.
    Kriminalistik, 1984, Nr 12.
12. Computerkriminalitat : Weniger Falle - bacher Schaden.
    Kriminalistik, 1984, Nr 1.
13. Curvey C.E. Eaton C.E. - Identification of IBM Keypunch Machines by their Printed Products.
    Journal of Forensic Sciences, 1976, Nr 4.
14. Date C.J. - Wprowadzenie do baz danych.
    WNT Warszawa 1981.
15. Dusza komputera - systemy operacyjne.
    Mikroklan, 1987, Nr 4.
16. 19-letni uczeń postrachem producentów komputerów.
    Echo Dnia, 1988, Nr 54.
17. Dziurnikowski A. - Zastosowanie środkow i metod informatyki dla wspomagania zarzadzania.
    Zeszyty naukowe ASW, 1978, Nr 20.
18. Dziurnikowski A. - Rola i miejsce środkow informatyki i metod w procesie podejmowania decyzji.
    Zeszyty Naukowe ASW, 1979, Nr 25.
19. Elektroniczna blokada oprogramowania.
    Przegląd Techniczny-Wiadomości i propozycje,1986, Nr 45
20. Flores I. - Urządzenia zewnętrzne komputerów.
    WNT Warszawa 1979.
21. Głowacki M. - Systemy operacyjne DOS i OS.
    WNT Warszawa 1982.
22. Goldstein B. - Electronic Frand:the Crime of the Future.
    International Criminal Police Review, 1985, Nr 391.
23. Guarding against Computer Crime.
    Computer Weekly, 1982, Nr 391.

24. Hansen P.B. - Podstawy systemów operacyjnych.
WNT Warszawa 1979.
25. Hearnden K. - Computer Crime:Multimilion Pound Problem.
Long Range Planning, 1986, Nr 6.
26. Herold H. - Kunfige Einsatzformen der EDV und ihre Auswirkungen im Bereich der Polizei.
Kriminalistik, 1974, Nr 9.
27. Hofmann L.J. - Poufność w systemach informatycznych.
WNT Warszawa 1982.
28. Idzkiewicz A. - Ochrona informacji w procesie przetwarzania.
PWE Warszawa 1979.
29. Informatyka - poradnik dla ekonomistów. Pod redakcją E. Niedzielskiej.
PWE Warszawa 1977.
30. Jeden dla wszystkich - systemy wielodostępne.
Mikroklan, 1986, Nr 1.
31. Jaźwin N. - Komputer przestępca.
Nowator, 1986, Nr 3.
32. Kalinowska H. - Terminologia bezpieczeństwa systemów.
Prasa Techniczna, 1986, Nr 3.
33. Karpinska A. - Komputerowi piraci.
Rzeczpospolita, 1986, Nr 303.
34. Kuster D. - System INPOL.
Kriminalistik, 1983, Nr 1.
35. Kleiber M. Szuniewicz R. - Komputer osobisty typu IBM PC - możliwości zastosowań profesjonalnych.
PWN Warszawa 1988.
36. Komputerowe piractwo.
Słowo Ludu, 1987, Nr 5.
37. Komputerowy skok na bank.
Przegląd Techniczny-Wiadomości i propozycje,1987,Nr 13.
38. Kontrowersje.
W służbie MO, 1986, Nr 5.
39. Korepta L. Matula E. - Praca operacyjna Służby Bezpieczeństwa.
Departament Szkolenia i Doskonalenia Zawodowego MSW
Warszawa 1982.
40. Kroh J. - Zabezpieczenie programów.
Mikroklan, 1987, Nr 11-12.
41. Kulikowski J. L. - Informacja i świat w którym żyjemy.
WP Warszawa 1978.
42. Liebiediew W.N. Sokołow A.P. - System operacyjny OS JS. Podstawy użytkowania.
PWE Warszawa 1982.
43. Madej D. Marasek K. Kuryłowicz K. - Komputery osobiste.
WKiL Warszawa 1987.
44. Madnick S. E. Donowan J. J. - Systemy operacyjne.
PWN Warszawa 1983.
45. Majewski W. - Wirusowa gorączka.
Komputer, 1988, Nr 11.
46. Martin J. - Dialog czlowieka z maszyna cyfrowa.
WNT Warszawa 1976.

47. Martin J. - Organizacja baz danych.
PWN Warszawa 1983.
48. Michalewicz Z. - Zagadnienia bezpieczeństwa baz danych.
PWN Warszawa - Lodz 1982.
49. Miiler J. - Bank danych - zbiory.
Zeszyty Naukowe ASW, 1974, Nr 2-3,
50. Miiler J. - Bank danych - relacje.
Zeszyty Naukowe ASW, 1974, Nr 5.
51. Miiler J. - Informacja w cybernetyce. Informatyka.
MON Warszawa 1974.
52. Minstrel - 4 EP - wielodostęp na wielu procesorach.
Mikroklan, 1987, Nr 8.
53. Naur P. - Zarys metod informatyki.
WNT Warszawa 1979.
54. Nowak E. Sawicki Z. - Pamięci maszyn cyfrowych - konstrukcja i technologia.
WNT Warszawa 1977.
55. Olesinski J. Staniszkis W. - Projektowanie baz danych.
PWE Warszawa 1984.
56. Oprogramowanie z blokada.
Przegląd Techniczny, 1987, Nr 11.
57. Parker D.B. - Computer Related Crimes.
Journal of Forensic Sciences, 1974, Nr 9.
58. Parlewicz P. Więckowski A. Zawadzki G. - - System operacyjny MUEL-85.
Mikroklan, 1986, Nr 3.
59. Pilawski B. - Komputer narzędziem pracy organizatora.
PWE Warszawa 1984.
60. Poufność informacji.
Mikroklan, 1987, Nr 3.
61. Przeniknęli nawet do NASA, Piractwo komputerowe Klubu Chaos z RFN.
Echo Dnia, 1988, Nr 53.
62. Rosiak H. - Organizacyjne ujęcie procesu dydaktycznego WSO MSW w Legionowie z wykorzystaniem komputera .
Zeszyty Naukowe WSO, 1987, Nr 2-3.
63. Safuta J. - Komputery, "wirusy" i piraci.
Slowo Ludu, 1988, Nr 79.
64. SBD/TP RODAN, System Bazy Danych i Teleprzetwarzania.
Centrum Projektowania i Zastosowań Informatyki,
ZETO ZOWAR - dokumentacja systemowa, 1988.
65. Shaw A.C.- Projektowanie logiczne systemów operacyjnych.
WNT Warszawa 1980.
66. Sokołowski A. - Ochrona informacji komputerowych.
MON Warszawa 1987.
67. Striżeñec M. - System człowiek - komputer.
PWN Warszawa 1985.
68. Strześniewski S. H. - Bezpośrednie systemy informacyjne.
PWE Warszawa 1985.
69. System wielodostepny ITM W4-16 Xenix System V.
PPZ ITM - dokumentacja systemowa, 1987.
70. Systemy cyfrowe wieloprocesorowe, Comtree Corporation.
WNT Warszawa 1980.

71. Szpiegostwo komputerowe.
Express Wieczorny, 1987, Nr 73.
72. Tanenbaum A. S. - Organizacja maszyn cyfrowych w ujęciu strukturalnym.
WNT Warszawa 1980.
73. Tiedemann K. - Betrug mit Hilfe des Computers.
Kriminalistik, 1984, Nr 11.
74. Tomaszewski T. - Kryminalistyczna problematyka przestepczości komputerowej.
Problemy kryminalistyki, 1980, Nr 143.
75. Topolewski Z. - Analiza i synteza ochrony informacji w procesach przetwarzania i teletransmisji danych.
Wydawnictwo Politechniki Wrocławskiej, Wrocław 1985.
76. Topolewski Z. - Mozliwości ochrony informacji w sieciach komputerowych.
Nowator, 1988, Nr 3.
77. Topolewski Z. - Ochrona informacji w sieciach komputerowych.
Nowator, 1986, Nr 7-8.
78. Ukryte gwiazdy - systemy operacyjne.
Mikroklan, 1986, Nr 2.
79. Walczak T. - Komputery - zasady działania i metody zastosowań.
PWE Warszawa 1987.
80. Weitzman C. - Systemy minikomputerowe.
WNT Warszawa 1979.
81. Wielodostępne bazy danych.
Mikroklan, 1987, Nr 10.
82. Wielodostępny Dedykowany System Bazy Danych CX-DMOS.
Computex CO LTD PPZ - dokumentacja systemowa 1987.
83. Wierzbicki T. - Mikrokomputery - poradnik użytkownika.
PWN Warszawa 1986.
84. Wikło S. - Stan prac nad wdrażaniem systemu informatycznego WSO MSW w Legionowie z uwzględnieniem mozliwosci zakupu na rynku krajowym sprzętu i oprogramowania.
Zeszyty Naukowe WSO MSW, 1987, Nr 2-3.
85. Wojna przeciw piratom.
Mikroklan, 1987, Nr 10.
86. Wymann J. J. - EDV - Sicherheit in Klein und Mittelbetrieben.
Der Organisator, 1987, Nr 1.
87. Vasaros F. - Elektronikus adatrogzites feldolgozas a kiemelt buncselekmenyek gyomonzasanal.
Belugyi Szemle, 1981, Nr 9.
88. Visura N. - Die Computerkriminalitat.
Der Organisator, 1987, Nr 1.
89. Yourdon E. - Projektowanie systemów o działaniu bezpośrednim.
WNT Warszawa 1976.
90. Zalewski J. - Czym jest UNIX ? System plików.
Mikroklan, 1986, Nr 1.
91. Zapewnienie poufności w procesie przetwarzania danych.
Materiały na konferencje naukową. TNOiK Warszawa 1978.

Janusz TRAWKA

Ochrona systemów informatycznych
w aspekcie funkcji jednostek
resortu spraw wewnętrznych.

Praca doktorska

napisana pod kierownictwem naukowym

płk prof. dr hab. Władysława FILARA

zawiera 80 kart ponumerowanych

Wydrukowano w 5 egz.
Egz.Nr 1-5 - Bibl.Nauk.DZS
Wyk. por. TRAWKA
Druk ONJO MSW
Nr PF186/88