WIADOMOŚCI STATYSTYCZNE

GŁÓWNY
URZĄD
STATYSTYCZNY

MIESIĘCZNIK
ROK XXI
WARSZAWA
GRUDZIEŃ 1976

12

w numerze:

SPIS TREŚCI

STATYSTYKA TERENOWA

INFORMATYKA W STATYSTYCE

INFORMACJE, PRZEGLĄDY, RECENZJE

СОДЕРЖАНИЕ

МЕСТНАЯ СТАТИСТИКА

ИНФОРМАТИКА В СТАТИСТИКЕ

ИНФОРМАЦИЯ, ОБЗОР, РЕЦЕНЗИИ

CONTENTS

REGIONAL STATISTICS

INFORMATICS IN STATISTICS

INFORMATION, SURVEYS, REVIEWS

Problemy ochrony danych komputerowych

mgr Antoni Bossowski

KILKA PRZYKŁADÓW ZAMIAST WSTĘPU

Dwaj pracownicy Centrum Rejestracji Ludności w Szwecji korzystając ze swych uprawnień wypożyczyli taśmy magnetyczne z rejestrami ludności i skopiowali je na innym komputerze. Oryginały zwrócili, a kopie sprzedali po zniżonej cenie klientowi tegoż centrum. Obaj zostali skazani na 6 miesięcy więzienia [17]. **Czy w polskim prawodawstwie kradzież informacji jest zaliczana do czynów zabronionych pod groźbą kary?**

Policjanta z Chicago oskarżono o wyciągnięcie i ujawnienie danych z Kryminalnego Centrum Informacji FBI, dotyczących osoby uwikłanej w kłopoty finansowe z jego kuzynem [17]. **Jak zabezpieczyć się przed sprzeniewierzeniem osób uprawnionych?**

W jednej z amerykańskich agencji ubezpieczeniowych znaleziono nadajnik radiowy ukryty w centralnym procesorze komputera. Nadajnik był w stanie transmitować informacje do specjalnego odbiornika [17]. W innym centrum amerykańskim należącym do zakładów Coca-Cola w Atlancie pod pokrywą siekacza papieru znaleziono miniaturowy aparat filmowy produkcji japońskiej, który dokonywał automatycznie zdjęć wydruków komputera przeznaczonych do zniszczenia. Konserwator dokonując systematycznych przeglądów wymieniał tylko rolkę filmu szpiegując w ten sposób na rzecz firmy konkurencyjnej [9]. **Czy nasze ośrodki informatyki i komputery są dostatecznie zabezpieczone przed szpiegostwem?**

Pięciu studentów jugosłowiańskich zostało aresztowanych na skutek podejrzenia o dokonanie zmiany danych w komputerze przeznaczonych do wydruku na końcówkach abonenckich uniwersyteckiego centrum obliczeniowego. W miejsce przetworzonych danych podstawili oni hasła antyrządowe [17]. Pewien programista w Nowym Jorku zaprogramował komputer tak, aby ten automatycznie eliminował murzynów przy naborze i selekcji nowych pracowników [17]. Inny programista poważnego przedsiębiorstwa niemieckiego zmienił program zgodnie z przyjętą zasadą o uproszczeniu rozliczeń poprzez zaokrąglanie przelewów do całych DM. Program jednak zmienił w ten sposób, że wszystkie zaokrąglenia dokonywane były w dół, a pozostałe z tej transakcji fenigi przekazywane były na jego konto. Do czasu przypadkowego wykrycia uzbierał sumę 450 tys. DM [20]. **Czy można skontrolować pracę programisty?**

W jednej z polskich gazet codziennych znalazła się wzmianka, w której autor z dumą donosił o sukcesie pewnej grupy programistów, którzy wygrali w totolotka dzięki temu, że założywszy w pamięci komputera bazę danych o wylosowanych dotychczas numerach „zaprzęgali" następnie komputer do obliczania prawdopodobieństwa kolejnych losowań. **Czy była to praca planowa czy niekontrolowana? Kto zapłacił za pracę komputera, którego jedna godzina kosztuje kilka tysięcy złotych? Czy istnieje jakaś norma określająca etykę informatyka?**

MIEJSCE PROBLEMU

Kilka przedstawionych wyżej przykładów nadużyć związanych z komputeryzacją, tłumaczy dlaczego prawie na całym świecie zaczęto poważnie interesować się problematyką ochrony danych komputerowych. Informatyka weszła już na stałe w nasze życie. Wiele instytucji państwowych i przedsiębiorstw gospodarczych opiera swą działalność o funkcjonujące systemy informatyczne. Zakłócenie informacji w tych systemach oznacza zakłócenie funkcjonowania tych instytucji i przedsiębiorstw. Skutki zakłócenia mogą być niekiedy bardzo znaczące. Wyjście jest tylko jedno: poprzez właściwą ochronę wytworzyć rozsądnie wysoki stopień ochrony danych komputerowych. Dlatego to spośród różnych problemów jakie wywołane zostały stosowaniem informatyki wyłania się ostatnio i zajmuje ważne miejsce problem **ochrony danych komputerowych.** Ochrona danych stała się przedmiotem pracy naukowców, inżynierów i menagerów. Europejski Program Badawczy Diebolda poświęcił temu problemowi kilka międzynarodowych konferencji. Na konferencji w marcu 1972 r. poświęconej zapewnieniu bezpieczeństwa źródeł informacji [8] określono bezpieczeństwo danych jako **„ochronę danych przed przypadkowym lub zamierzonym dostępem osób nieuprawnionych oraz samowolną ich zmianą".**

Nadużycia komputerowe rozwijają się na świecie wraz ze wzrostem ilości stosowanych komputerów. Zrozumiałe jest więc, że przodują pod tym względem Stany Zjednoczone tym bardziej, że rozwojowi nadużyć sprzyja prywatna własność środków produkcji i konkurencja gospodarcza.

Amerykanie [15, 17] definiują nadużycia komputerowe jako **„wszelki rodzaj działalności wyraźnie związanej z komputerami lub transmisją danych, w wyniku której poszkodowani niedobrowolnie ponoszą lub są narażeni na straty, krzywdy lub szkody, lub w wyniku której sprawcy osiągają, lub mogą osiągnąć zyski".**

Stanfordzki Instytut Badawczy, zajmujący się od lat poważnie tą problematyką, zebrał do 1973 r. jako materiał badawczy 148 przypadków nadużyć komputerowych [17]. Szczególnym sygnałem do rozpoczęcia studiów były dwa następujące oszustwa: w Nowym Jorku główny kasjer oddziału Union Dima Sawiqs Bank został oskarżony o zdefraudowanie ponad 1,5 mln dolarów poprzez manipulacje rachunkami w centralnym komputerze dokonane za pomocą komputerowej końcówki kasowej. W Los Angeles wykryto dwumilionowe oszustwo polegające na rozprowadzaniu 56 tys. sfałszowanych polis ubezpieczeniowych i innych manipulacjach dokonanych przez kierownictwo i niektórych pracowników Towarzystwa Ubezpieczeniowego. Kontrole rewizyjne w tym przedsiębiorstwie przeprowadzone w ciągu ostatnich trzech lat nie wykazały żadnych niedokładności. Brak jest informacji czy jakakolwiek inna instytucja w świecie poza Instytutem Stanfordzkim zajmuje się problemem zbierania i analizy przypadków nadużyć komputerowych. Z literatury wynika, że poszczególni autorzy zebrali do swych prac pewną ilość przypadków. D. van Tassel [18] z Uniwersytetu Kalifornijskiego w Santa Cruz analizuje przypadki nadużyć w Stanach Zjednoczonych. R. von zur Mühlen [14] z Bonn stwierdza na podstawie zebranych przypadków, że przestępstwa komputerowe stały się już w RFN zjawiskiem. R. Farr [9] z Wielkiej Brytanii zbiera przypadki szpiegostwa przemysłowego, a szczególnie szpiegostwa komputerowego i sposobów pominięcia ochrony. B. Allen [1] z Uniwersytetu w Wirginii zbiera przypadki nadużyć poprzez osobiste kontakty i prasę. S. Barlay [3] brytyjski dziennikarz i ekonomista zajmuje się zagadnieniami wywiadu komputerowego stwierdzając, że na skutek istnienia tego rodzaju przestępstw przemysł brytyjski i amerykański ponosi wielomilionowe straty. M. G. Wiesel [20] z dyrekcji generalnej policji federalnej RFN zajmuje się przestępczością komputerową głównie w jej prawnych aspektach.

Brak jest jakichkolwiek informacji o czynach przestępczych w krajach socjalistycznych. Sytuacja taka jest zrozumiała jeżeli uwzględnić następujące czynniki:

◆ nasilenie przestępczości komputerowej zależy od ilości eksploatowanych komputerów. Według ostatnich danych na świecie zainstalowanych jest około 150 tys. komputerów z czego na kraje socjalistyczne — poza ZSRR przypada około 3—4 tysiące;

◆ sprawca nadużyć komputerowych na ogół musi posiadać bardzo wysoką wiedzę fachową, którą zwykle zdobywa się w praktycznych zastosowaniach skomplikowanych zestawów maszyn do złożonych problemów, a zatem przestępczość zależy również od jakości zastosowań maszyn;

◆ nie pozostaje również obojętny system gospodarczy na przyczyny przestępstw; wzajemna konkurencja gospodarcza koncernów i firm sprzyja wewnętrznemu szpiegostwu gospodarczemu i sabotażom;

◆ istnieje zrozumiały opór przed ujawnieniem nadużyć przez kierownictwo przedsiębiorstw, aby podanie do publicznej wiadomości takiego faktu nie zaszkodziło reputacji firmy. W USA po ogłoszeniu, że Stanfordzki Instytut zajął się problematyką przestępczości komputerowej wpłynęło wiele zgłoszeń listowych i telefonicznych donoszących o nadużyciach komputerowych i proszących aby fakt zgłoszenia pozostał tajemnicą.

Brak źródeł krajowych nie upoważnia jednak do odrzucenia tematu, gdyż przygotowanie się do spotkania tych zjawisk w kraju wymaga wielu lat i ma bardzo poważne znaczenie. Brak źródeł krajowych nie upoważnia również do stwierdzenia, że w Polsce nie występują nadużycia mimo tak małego nasycenia środkami informatyki naszej gospodarki.

Rozpatrując przedmiot ochrony danych w szerokim zakresie można podzielić go za J. Martinem [13] na trzy następujące aspekty:

— **bezpieczeństwo danych** (security) dotyczące ochrony danych przed przypadkowym lub zamierzonym ujawnieniem osobom nieuprawnionym lub niekontrolowaną zmianą lub zniszczeniem;

— **poprawność danych** (accuracy) dotycząca funkcji przetwarzania, chroniąca przed utratą jakiejkolwiek istotnej informacji (danych) lub też wprowadzeniem do niej błędów;

— **ochrona danych prywatnych** (privacy) dotycząca prawa osób lub organizacji do samookreślenia kiedy, jak i w jakim wymiarze informacja o nich może być przekazana innym.

Omawiając poziom rozwoju poszczególnych aspektów bezpieczeństwa danych i ich znaczenie G. E. Hammings w przedmowie do książki J. Martina [13] pisze: „Poprawność, bezpieczeństwo i tajemnica danych być może nie są najbardziej fascynującymi aspektami przetwarzania ale stanowią one podstawę do określenia odpowiedzialności i respektu dla ludzkości... Po około 20 latach wciąż jeszcze nie mamy pełnej odpowiedzi na wszystkie te problemy. Nasza wiedza dotycząca poprawności danych została naprawdę wysoko rozwinięta, wiedza dotycząca bezpieczeństwa jest młodą i szybko rozwijającą się, a wiedza dotycząca tajemnicy jest zaledwie podstawowa".

Instytucjonalnie problemem bezpieczeństwa w USA zajmuje się Instytut Zabezpieczeń Komputerowych (Computer Security Institute) [7]. W grudniu 1974 r. instytut ten zorganizował w Nowym Jorku pierwszą konferencję poświęconą bezpieczeństwu systemów komputerowych. Ponadto instytut organizuje seminaria, opracowuje programy sprawdzające i wydaje fachową literaturę. Jest to jedyny instytut zajmujący się wszechstronnie problemem zabezpieczeń. W Europie problematyka bezpieczeństwa jest przedmiotem badań Europejskiego Programu Badawczego Diebolda. Podjęta została w 1972 r. poprzez wydanie dokumentu pt. „Ensuring the Security of the Information Resource" [8] stawiającego problem bezpieczeństwa po raz pierwszy w Europie oraz zorganizowanie konferencji w kwietniu 1972 r. na ten sam temat.

Jednym z podstawowych akcentów dokumentu Diebolda jest wykazanie, że **odpowiedzialność za bezpieczeństwo danych nie może spoczywać jedynie na kierownikach,** lecz musi być rozłożona na cały personel przetwarzania, a także na otoczenie. Problem personelu podnoszą różni autorzy. G. Wiesel [20] uważa, że problem personelu jest pierwszym słabym punktem bezpieczeństwa systemu informatycznego. J. Martin [13] omawiając problem odpowiedzialności głosi hasło: **„Za bezpieczeństwo odpowiada każdy"** („Security is everyone's responsibility"). Wielu autorów sugeruje wprowadzenie w ośrodkach informatyki stanowisk oficerów bezpieczeństwa [2, 8, 13], pilnujących przestrzegania przyjętych procedur ochrony i wprowadzających nowe metody ochrony.

W wielu pracach przewijają się również prawne aspekty ochrony danych. J. Mc Carthy [6] uważa, że żadnej organizacji ani państwowej, ani prywatnej nie powinno być wolno gromadzić żadnych kartek dotyczących wielkiej liczby ludzi poza ogólnie przyjętym systemem, którego wszystkie procedury są jawne, i który pozostaje pod społeczną i indywidualną kontrolą. A. Westin [19] polemizując z pojawiającymi się głosami o rzekomym zagrożeniu sfery prywatnej człowieka przez komputery uważa, że należy generalnie zrewidować dotychczasowe normy, aby zasady wolności osobistej współgrały z możliwościami jakie stwarza technika komputerów w dziedzinie szybkiego, efektywnego i zintegrowanego systemu decyzji. L. M. Baskir [4], członek podkomisji do spraw podziału władzy i prawa konstytucyjnego w Senacie Amerykańskim, postuluje wprowadzenie odpowiedniego ustawodawstwa jasno nakreślającego granice dotyczące sfery prywatnej obywateli. L. Baird [2] podkreśla konieczność opracowania nowych zasad klasyfikacji tajemnicy i sposobów postępowania z informacjami tajnymi, gdyż dotychczasowe przepisy dotyczą przeważnie dokumentów papierowych.

W wielu państwach podejmuje się działania, w celu prawnego zabezpieczenia tajemnicy danych komputerowych, dla ograniczenia zjawiska przestępczości i wszelkiego rodzaju samowolnych manipulacji informacjami banku danych.

Przykładem jest **Ustawa o Danych uchwalona przez Szwedzki Parlament w kwietniu 1973 r.** Ustawa ta reguluje m. in. zagadnienie wzajemnej zależności pomiędzy techniką komputerową, a tajemnicą. Jeden z przepisów stanowi, iż każdy prowadzący rejestr personalny bez zezwolenia lub dopuszczający się pogwałcenia tajemnicy zawodowej, może być ukarany grzywną lub skazany na karę więzienia do 1 roku. Ustawa o Danych wprowadza nowe stany faktyczne przestępstw, które polegają na: bezprawnym uzyskaniu dostępu do zapisów komputerowych oraz bezprawnych zmianach w zapisach; za te czyny grozi kara grzywny lub więzienia do 2 lat. Istnieje także podstawa do żądania zadośćuczynienia za każdą poniesioną szkodę, jakiej doznał obywatel wskutek niewłaściwej o nim informacji zawartej w banku danych [1].

Również **w Austrii podjęto w 1975 r. przygotowania do wydania ustawy mającej na celu ochronę danych komputerowych.** W projekcie podkreślono szczególnie zagadnienie ograniczenia kręgu osób mających dostęp do bnaku danych [12].

W RFN Komisja Spraw Wewnętrznych Bundestagu zaprosiła do publicznej dyskusji ekspertów z różnych dziedzin życia państwowego, gospodarczego i naukowego nt. **projektu ustawy o ochronie danych.** Ustawa precyzuje dozwolone procedury, określa odpowiedzialności, biorąc szczególnie pod ochronę dane osobowe [10].

OKREŚLENIE RYZYKA

Ogólna klasyfikacja niebezpieczeństwa i przyczyny według Diebolda podana jest w tablicy 1 na str. 32.

Z danych zebranych przez Stanfordzki Instytut Badawczy wynika, że nadużycia komputerowe pojawiły się około 10 lat temu. W pierwszych latach były to jednak pojedyncze przypadki. Tablica 2 obrazuje zarejestrowane przypadki nadużyć komputerowych według lat i rodzaju przestępstwa w przyjętej przez wymieniony instytut klasyfikacji. Zdecydowana większość tych przypadków dotyczy ośrodków rozlokowanych na terenie USA. Można na podstawie tego ze-

stawienia wysunąć spostrzeżenie, że nadużycia komputerowe jako zjawisko społeczne wystąpiły w USA od 1970 r., tj. od około 5 lat. W 1970 r. w USA było zainstalowanych 70000 komputerów. W ciągu lat 1970—1971 dokonano około 70 zarejestrowanych nadużyć. **W 1973 r. zainstalowanych było w świecie około 130 tys. komputerów. Do tego czasu dokonano około 150 nadużyć komputerowych.** Uwzględniając zauważalną zależność ilości nadużyć od ilości zainstalowanych komputerów można szacunkowo określić tę zależność jako: 1 nadużycie na około 1000 czynnych komputerów. Wskaźnik ten jest naturalnie właściwy jedynie dla początkowego stadium rozwoju nadużyć komputerowych, dla gospodarki kapitalistycznej i oszacowany jest z błędem posiadanych na ten temat informacji, tzn. jest zaniżony według ilości przypadków zarejestrowanych obejmujących poważniejsze czyny przestępcze.

TABL. 1. KLASYFIKACJA NIEBEZPIECZEŃSTW

Istota niebezpieczeństwa	Przypadek	
	losowy	zamierzony
Niesprawność systemu	Pożar Brak zasilania Awaria klimatyzacji	Sabotaż
Zniszczenie danych	Wymazanie pamięci Zniszczenie biblioteki programów	Sabotaż Kradzież
Zmiana danych	Błąd maszyny Użycie złej taśmy	Oszustwo
Ujawnienie danych	Dostarczenie lub skierowanie wyjścia do nieupoważnionej osoby	Kradzież

Źródło: Diebold Research Program Dec. E 92-5.

TABL. 2. ZAREJESTROWANE PRZYPADKI NADUŻYĆ KOMPUTEROWYCH WEDŁUG LAT I RODZAJÓW

Lata	Wandalizm	Kradzież informacji lub mienia	Kradzież lub defraudacja finansowa	Bezprawne użycie sprzętu lub sprzedaż usług	Ogółem	W tym przypadków udowodnionych
Ogółem . .	**26**	**49**	**50**	**23**	**148**	**61**
1964	0	1	3	0	4	2
1965	0	0	1	0	1	0
1966	0	0	1	0	1	1
1967	0	0	0	1	1	0
1968	1	1	4	0	6	1
1969	3	4	1	0	8	5
1070	7	5	6	5	23	11
1971	6	16	19	6	47	12
1972	6	15	10	8	39	15
1973[a]	3	7	5	3	18	14

a Pierwsze półrocze.

Źródło: Stanford Research Institute.

Znamienne jest zjawisko wystąpienia głównie dwóch rodzajów nadużyć, tj.: kradzieży informacji lub mienia (jedna trzecia przypadków) oraz kradzieży lub defraudacji finansowej (również jedna trzecia przypadków). Uznając, że nadużycia mające na celu oszustwo finansowe są nadużyciami typowymi dla świata przestępczego zauważyć należy, że interesującym zjawiskiem jest kradzież informacji. Jest to nadużycie typowe dla informatyki, która spowodowała koncentrację informacji; często nie poddaje się ono dotychczasowym normom prawnym przystosowanym do tradycyjnego obiegu informacji. Dotychczas bowiem informacja jako taka nie była przedmiotem ochrony. Znajdowała się ona prawie zawsze na nośniku papierowym, który zwany był zwykle dokumentem. Przedmiotem ochrony był więc dokument z właściwym mu gryfem tajności i właściwą mu mocą prawną. Kradzież informacji zapisanej na nośniku komputerowym często nie narusza ani nośnika, ani samej informacji. Nadużycie polega na tym, że osoba nieupoważniona posiadła nielegalnie informację. Problem ten niewątpliwie wymaga nieco innego spojrzenia i głębszego opracowania.

Około 17% zarejestrowanych przypadków dotyczy przestępstw nazwanych wandalizmem. Najczęściej uległy zniszczeniom pamięć lub komputery, przy czym sprawcy używali do tego celu najczęściej bomb lub pistoletów. Tego typu nadużyć, aczkolwiek przynoszą one wielką szkodę systemom informatycznym, nie można uznać za typowe dla informatyki. Bardziej słuszny wydaje się pogląd uznający je za przestępstwa typowe dla społeczeństwa amerykańskiego. Nie lekceważąc takich przestępstw można przypuszczać, że w społeczeństwie polskim częstość wystąpienia przypadków wandalizmu będzie znacznie mniejsza.

Około 15% nadużyć dotyczy bezprawnego użycia sprzętu lub sprzedaży usług. Jest to następny rodzaj nadużyć, który należy uznać za bardzo typowy dla okresu komputeryzacji usług. Można by kontrowersyjnie twierdzić, że bezprawne użycie sprzętu występuje i w innych dziedzinach i datuje się od czasu gdy postęp techniki stworzył skomplikowane narzędzia, których wysoki koszt ogranicza możliwość powszechnego zakupu. Istnieją jednak powody do uznania tych nadużyć za typowe dla informatyki. Są to następujące powody:

◆ **koszt jednej godziny pracy komputera** jest bardzo wysoki i wynosi, według stawek obowiązujących w krajach kapitalistycznych, **od 200 do 800 dolarów** za godzinę, zaś **w Polsce od 2500 do 5000 zł za godzinę pracy komputera.** Zatem wystarczy sprzedaż 1—2 godzin pracy komputera aby uzyskać wynagrodzenie równe miesięcznym zarobkom kwalifikowanego pracownika.

◆ w systemach komputerowych pracę wykonuje automat praktycznie bez udziału człowieka i w sposób trudno zauważalny, co stwarza sprzyjające warunki dla ukrycia nadużyć.

Uznając przypadki bezprawnego użycia za charakterystyczne należy również zauważyć, że są one typowe dla różnych systemów gospodarczych. Mogą one również występować w Polsce, zwłaszcza jeżeli rozumie się je w szerokim zakresie niegospodarności. W Polsce nie zajmowano się jeszcze problematyką tego typu nadużyć, a w tym i kwestią niegospodarności, nie można w związku z tym podać oficjalnie stwierdzonych przypadków takich czynów. Na podstawie znajomości działania ośrodków informatyki można jednak przypuszczać, że przypadki niegospodarności występują w większości polskich ośrodków informatyki.

Znamiennym zjawiskiem, które można spostrzec w tablicy 2 jest bardzo niski, tzn. około 40% wskaźnik ilości przypadków udowodnionych w stosunku do przypadków ujawnionych. Nadużycia komputerowe należą do wyjątkowo trudnych dowodowo nadużyć i to tak ze względu na poziom sprawców, jak i ze względu na najczęściej nikłe materialne dowody nadużyć.

KOMPLEMENTARNOŚĆ METOD OCHRONY

Pracownik IBM Systems Research Institute J. Martin, autor wielu opracowań z dziedziny informatyki, w swoim podstawowym dziele „Security, Accuracy and Privacy in Computer Systems" [13] dowodzi, że właściwe zabezpieczenie uzyskuje się tylko wtedy gdy stosuje się szereg, wzajemnie uzupełniających się metod ochrony. W tym zakresie rozróżnia on cztery poziomy zabezpieczeń przedstawione schematycznie na rys. 1.

Systemowe zabezpieczenie poprawności działania komputera oraz systemowa automatyczna kontrola dostępu do informacji oraz jej przetwarzania. Systemowe metody zabezpieczeń są integralną częścią systemów operacyjnych nowoczesnych komputerów. Obejmują one głównie:

— matematyczną i logiczną kontrolę danych w procesie przetwarzania,

— uwarunkowanie dostępu do zbiorów danych znajomością zadanych haseł,

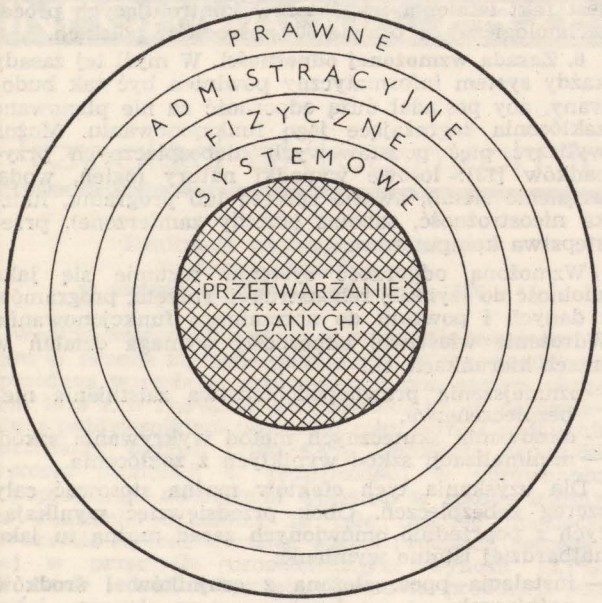
— zróżnicowanie zezwoleń na operacje na danych na czytanie, modyfikowanie, dopisywanie itp.

Systemowe zabezpieczenia uznaje się za podstawowe i najważniejsze w gronie stosowanych różnych metod ochrony.

Fizyczne zabezpieczenie obejmuje szereg metod opartych o osoby i środki techniczne. Są to różnego rodzaju systemy alarmowe, zamki, strażnicy, czujniki ppoż. i in. Mają one na celu:
— ochronę przed przypadkami losowymi (pożar, woda),
— ochronę przed niepożądanym dostępem do informacji osób nie upoważnionych.

Administracyjne metody zabezpieczeń, to jest zbiór administracyjnych rygorów proceduralnych działających w celu:
— prawidłowego użycia sprzętu i wykorzystania systemów informatycznych,
— kontroli zatrudnionego personelu,
— przestrzegania ustalonej procedury technologicznej,
— kontroli zachowania się osób nie zatrudnionych.

Zabezpieczenie prawne i społeczne. Obejmuje ono zbiór norm prawnych ustalających zakazy i nakazy postępowania w strefie czynów zabronionych pod groźbą kary, jak również w strefie etyki. Zagadnienia te pozostają do dzisiaj nie rozwiązane i wywołują szereg dyskusji, zwłaszcza gdy w grę wchodzi kwestia społecznej kontroli danych osobowych. Coraz więcej krajów uznaje jednak, że w zinformatyzowanym społeczeństwie ochrona prawna informacji jest konieczna.



Rys. 1. Cztery poziomy zabezpieczeń

PROPONOWANE ZASADY OCHRONY DANYCH

Wdrażając opracowany system ochrony informacji należy pamiętać, że zapewnienie odpowiedniego bezpieczeństwa danych komputerowych jest na ogół przedsięwzięciem bardzo kosztownym. Z ekonomicznego punktu widzenia można by sformułować pogląd, że koszt systemu zabezpieczeń nie powinien być większy niż ewentualne straty wynikłe z powodu jego braku. Zasada ta jest częstokroć bardzo trudno wyliczalna gdyż różna jest wartość informacji i różne mogą wynikać wielkości szkód z jej utraty lub ujawnienia. System ochrony powinien być precyzyjnie przemyślany, opracowany i dopasowany do danego systemu informatycznego i wartości zawartych w nim danych. Z tego więc względu projekt ochrony powinien być integralną częścią projektu każdego systemu informatycznego.

Poniżej zostaną sformułowane pewne zasady, których stosowanie w praktyce wpływa istotnie na funkcjonowanie systemu zabezpieczeń. Wybierając te zasady autor niniejszej pracy oparł się o dostępną literaturę światową, o analizę stanu informatyki w Polsce oraz o własne doświadczenia w tej dziedzinie [5]. Niektóre z tych zasad konfrontowane będą z odpowiednimi aspektami stanu bezpieczeństwa informacji w polskich ośrodkach informatyki. Badania na ten temat przeprowadzone zostały w Instytucie Problematyki Przestępczości, pod kierunkiem prof. B. Hołysta przy współpracy autora niniejszej pracy [11].

1. **Zasada odpowiedzialności osobistej.** Każdy pracownik uczestniczący w procesie przetwarzania informacji jest odpowiedzialny za ochronę danych, za ścisłe przestrzeganie zasad bezpieczeństwa i norm technologicznych. Zasada ta znajduje swoje uzasadnienie w daleko posuniętej specjalizacji pracowników informatyki oraz złożoności procesów przetwarzania informacji. W takiej sytuacji trudno byłoby sprawować ścisły nadzór i przeciwnie prawie każdy pracownik centrum może stosunkowo łatwo, mimo istniejącego nadzoru, dokonać czynu zagrażającego informacji.

W literaturze zachodniej zasada ta zawarta jest w haśle „Security is everyone's responsibility" [13]. Na tle tej zasady nasuwają się dwie refleksje. **Po pierwsze** wydaje się potrzebne formalno-prawne uregulowanie tej kwestii, zarówno z przedmiotowej, jak i podmiotowej strony. Oparcie się bowiem wyłącznie na istniejących przepisach np. o ochronie tajemnicy czy ochronie mienia może okazać się niewystarczające. Co najmniej jedno przedsięwzięcie wydaje się konieczne, tj. **wpisanie każdemu pracownikowi informatyki obowiązku dbania o bezpieczeństwo systemu i ochronę danych do zakresu obowiązków służbowych.** Można się natomiast zastanowić, czy należy kierownika z tytułu pełnionej funkcji obciążać odpowiedzialnością większą niż osobistą odpowiedzialnością jako informatyka. **Po drugie,** skoro praca informatyka jest dziedziną samodzielną, trudno kontrolowaną, skoro od jej jakości tak bardzo zależy wynik, zarówno w sferze bezpieczeństwa efektywności jak i ekonomicznej opłacalności, to czy nie warto jej uczynić bardziej społecznie odpowiedzialną? **Może na wzór służby zdrowia warto wprowadzić kodeks etyki informatyka i w ślad za tym zezwolenia na wykonywanie zawodu?**

2. **Zasada drzwi zamkniętych** (ang. „Closed shop") [8]. Zasada ta głosi, że ośrodki informatyki powinny być chronione przed nie kontrolowanym wstępem osób nie zatrudnionych, a także przed penetracją przez pracowników wybiegającą poza potrzeby procesu technologicznego. W ośrodkach informatyki musimy wyróżnić w tym celu dwa rodzaje obszarów. Jedne tzw. technologiczne, tj. te w których znajdują się maszyny, nośniki informacji, końcówki itp. oraz drugie tzw. biurowe, gdzie pracują programiści, projektanci i inny personel. Naturalnie szczególnej ochronie podlegają pomieszczenia technologiczne. Osoby nie zatrudnione w ośrodku nie powinny wchodzić do ośrodka bez kontroli, a przebywać w nim powinny w towarzystwie osoby, do której przyszły. Taka zasada dotyczy naturalnie pomieszczeń biurowych. Wyklucza się natomiast prawie całkowicie wchodzenie osób obcych do pomieszczeń technologicznych. **Wstęp do pomieszczeń technologicznych powinni mieć wyłącznie upoważnieni do tego pracownicy i tylko w celu wykonania zadania.**

W polskich ośrodkach informatyki brak jest jeszcze nawyków stosowania powyższej zasady. Obecnie zaledwie 10% ośrodków stosuje kompleksowe zabezpieczenie przed nie kontrolowanym wstępem osób nie zatrudnionych. Polega ono na kontroli celu przybycia, towarzyszeniu osobie obcej przebywającej na terenie ośrodka, zamknięciu pomieszczeń technologicznych i ustanowieniu systemu upoważnień regulujących dostęp do newralgicznych jego punktów. W większości ośrodków (około 90%) zabezpieczenie jest mniej kompleksowe. Tak np. w 50% ośrodków nie zamyka się pomieszczeń technologicznych, a w 40% ośrodków nie stosuje się kontroli wejścia osób obcych na teren.

Wydaje się, że jest to zasada łatwa do zastosowania, istotna dla problemu bezpieczeństwa i godna zalece-

nia. Wprowadzenie jej wymaga pewnych przedsięwzięć natury administracyjnej, jak wydanie właściwych instrukcji i wprowadzenia odpowiedniego systemu upoważnień, a także przedsięwzięć natury fizycznej, tj. zainstalowanie zamków, zabezpieczeń i zatrudnienia strażników.

3. **Zasada ograniczonego dostępu do informacji.** Dla zmniejszenia skuteczności ewentualnego wywiadu stosuje się taki podział zadań wśród pracowników ośrodka aby ograniczyć dostęp do informacji. W myśl tej zasady każdy powinien wiedzieć tylko tyle ile to wynika z jego zadań. Zasada taka jest praktykowana już w krajach o zaawansowanym stopniu zastosowań informatyki i znana pod hasłem „Need-to-know" [8]. W praktyce opiera się ona głównie na następujących trzech warunkach:

— dostęp do komputera i zbiorów informacji posiadają tylko uprawnieni do tego pracownicy i tylko w celu wykonania zadania,
— wszystkie programy i zbiory informacji zgromadzone są odrębnie w specjalnej bibliotece informacji, z której wydaje się je odpowiednio do bieżącego zadania,
— uzyskanie informacji z komputera wymaga znajomości odpowiednich haseł umieszczanych w programach na ogół przez użytkowników — właścicieli informacji.

W Polsce — podobnie jak inne zasady — ta również nie jest w pełni jeszcze stosowana. Pierwsze dwa warunki stosowane są w około 25% ośrodków, trzeci natomiast zaledwie w kilku. Jest to niewątpliwie zasada godna polecenia, gdyż działając wspólnie z zasadą drzwi zamkniętych może stanowić skuteczną barierę ochronną przed nie kontrolowanym dostępem do sprzętu i informacji. Pierwszy warunek wymaga jedynie odpowiedniej procedury, drugi wpływa na wewnętrzną konstrukcję budynku trzeci natomiast może być stosowany przy nowoczesnych komputerach posiadających odpowiednio rozbudowane systemy operacyjne.

4. **Zasada ochrony systemowej.** Bardzo istotną i uznawaną obecnie za jedną z podstawowych metod ochrony przed niepożądanym dostępem do informacji jest ochrona informacji i kontrola procesu dokonywana przez sam komputer, zwana ochroną systemową. Odpowiednie do tego celu algorytmy są sterowane przez systemy operacyjne nowoczesnych komputerów i automatycznie wykonywane, a uzyskane wyniki warunkują dalszą procedurę przetwarzania. Do najczęściej stosowanych algorytmów należą:

— identyfikacja użytkownika na podstawie nazw katalogowych i znajomości odpowiednich procedur,
— kontrola uprawnień zgłaszającego się użytkownika na podstawie zgodności podanych haseł,
— sprawdzanie zastrzeżeń ograniczających udostępnianie informacji zgromadzonej w bazie danych;
— uwzględnianie narzuconych ograniczeń wykonania programów,
— automatyczna rejestracja wykonanych prac itp.

Wykorzystanie systemów operacyjnych dla celów profilaktycznych wymaga wysokiego poziomu wiedzy fachowej w zakresie oprogramowania oraz nowocześnie zorganizowanych komputerów. Bezsporna jednak wydaje się opinia, że komputery mogą w tej dziedzinie oddać nam olbrzymie usługi wykonując szereg procedur szybciej i bardziej precyzyjnie niż człowiek. Ten rodzaj ochrony wykorzystuje się w Polsce w bardzo małym stopniu. Zaledwie jeden na 10—12 ośrodków korzysta z możliwości systemów operacyjnych przy identyfikacji użytkownika i ochronie danych przez hasła szyfrowe, mimo że co najmniej co czwarty komputer zainstalowany w Polsce posiada sprawny do tego celu system operacyjny.

5. **Zasada kontrolowanego przetwarzania.** Najbardziej ogólnym i podstawowym przeciwdziałaniem nadużyciom jest utrzymywanie wzorowego porządku, wysokiej dyscypliny pracy i ścisłe przestrzeganie ustalonych procedur technologicznych. Wyrazem takiej dyscypliny jest istnienie i przestrzeganie przemyślanych instrukcji oraz kontrolowanie postępowania zgodnego z przepisami. Do szczególnie newralgicznych punktów procesu technologicznego, wymagających kontroli zalicza się: pracę komputera, użycie końcówek abonenckich, obieg informacji, dopuszczenie programów i systemów do eksploatacji oraz użycie systemu operacyjnego komputera. Wszystkie te czynności powinny być dokładnie rejestrowane. Istnienie organu kontrolnego wzmacnia przestrzeganie dyscypliny i podnosi poziom bezpieczeństwa, dlatego też **ważnym elementem organizacji ośrodków jest istnienie mocnego zespołu pracowników zdolnych do sprawowania kontroli merytorycznej i administracyjnej nad procesem technologicznym w ośrodku.**

Przedmiotem ataku w wielu nadużyciach komputerowych są programy. Za ich pomocą można wykonać nie planową pracę lub dokonać zmian w danych. Programy można zmienić w taki sposób aby potem eksploatowane dokonywały same systematycznych nadużyć. Przeciwdziałaniem tego rodzaju nadużyciom jest ochrona programów, wydawanie ich tylko dla wykonania określonej pracy i kontrola ich działania po każdorazowej zmianie wprowadzonej do programu.

Sprawowanie dobrej merytorycznej kontroli zwłaszcza w zakresie użycia systemu operacyjnego, poprawności procesu technologicznego lub „czystości" programu wymaga chyba najwyższej wiedzy informatycznej i inteligencji. Dlatego też uzyskanie zdolnych do tego pracowników wymaga czasu i intelektualnych inwestycji. Znacznie łatwiejsze do wprowadzenia są te aspekty dyscypliny, porządku i kontroli, które wchodzą w zakres działań administracyjnych. Z przeprowadzonych badań wynika, że i na tym polu jest u nas wiele jeszcze do nadrobienia. Pozytywnym zjawiskiem jest fakt istnienia inspektorów kontrolujących proces technologiczny w prawie 50% ośrodków polskich.

6. **Zasada wzmożonej odporności.** W myśl tej zasady każdy system informatyczny powinien być tak budowany, aby posiadał dużą odporność na nie planowane zakłócenia zagrażające jego funkcjonowaniu. Można wyliczyć pięć podstawowych niebezpiecznych przypadków [13]: losowe wypadki natury (ogień, woda, trzęsienie ziemi), awaria sprzętu lub programu, ludzka nieostrożność, sabotaż (szkody zamierzone), przestępstwa komputerowe.

Wzmożoną odporność systemu rozumie się jako zdolność do szybkiej rekonstrukcji sprzętu, programów i danych i powrotu do normalnego funkcjonowania. Wdrożenie właściwej odporności wymaga działań w trzech kierunkach, tj.:

— zmniejszenia prawdopodobieństwa zaistnienia niebezpieczeństwa,
— stosowania skutecznych metod wykrywania szkód,
— minimalizacji szkód wynikłych z zakłócenia.

Dla uzyskania tych efektów można stosować cały szereg zabezpieczeń. Obok przedsięwzięć wynikających z poprzednio omówionych zasad można tu jako najbardziej istotne wymienić:

— instalacja ppoż. złożona z czujników i środków gaśniczych,
— utrzymywanie dublujących aktualnych zbiorów danych, programów, i dokumentacji w bezpiecznym miejscu,
— uczulenie pracowników i przeszkolenie ich w zakresie działania awaryjnego,
— posiadanie sprawnych środków softwarowych i hardwarowych do testowania systemu.

W polskich ośrodkach informatyki coraz szerzej wdraża się metody zabezpieczeń podnoszących stopień odporności systemów na wypadki. Tak np. instalacja ppoż. wraz z przeszkoleniem załogi funkcjonuje w 77% obiektów, a 60% ośrodków stosuje zasadę dublowania zbiorów danych i programów.

* * *

Na zakończenie prezentacji kilku wybranych zasad ochrony danych wskazane wydaje się krótkie wyjaśnienie intencji autora. Otóż jest to prezentacja dyskusyjna, obejmująca pewien zbiór poglądów na temat ochrony systemów informatycznych możliwych do przyjęcia w warunkach polskich, nie pretendująca do wyczerpania tematu.

BIBLIOGRAFIA

[1] B. Allen — „Danger ahead! Safeguard your Computer" Harvard Business Reviev, Nov-Dec. 1968.

[2] L. L. Baird — „An Analitical Approach Identifying Computer Vulnerability" Security Products News, V—VI, 1974.

[3] S. Barlay — „Tajne interesy" — przedruk fragmentów w B. S. z dnia 13 IV 1974 pt. *Zbrodnia doskonała, czyli jak okraść komputer.*

[4] L. M. Baskir — „Erfahrungen mit Öffentlichen Databanksystem in USA" The Diebold Research program — Europe Symposium 24 IV 1972.

[5] A. Bossowski — Nadużycia komputerowe i ochrona informacji, *„Studia kryminologiczne, kryminalistyczne i penitencjarne"* nr 4, 1976.

[6] J. Mc Carthy — „Rewolucja informacyjna" tłum. w zbiorze: „Dziś i jutro maszyn cyfrowych", PWN, W-wa 1969.

[7] Computer Security Institute: Announcing the First Annual Computer Security Conference and Workshop, New York, Dec. 1974.

[8] The Diebold Research Program — Europe „Ensuring the Security of the Information Resource" Document No E 92. March 1972.

[9] R. Farr: „Społeczeństwo infomacji i szpiegostwo technologiczne" (tłum. OBRI); Conference proceedings meeting XXX Diebold Research Program — Europe, Hamburg, March 12—14, 1974, Doc. No EC 30.

[10] Handelsblatt, 31. 03. 1976 r: „Heftige Kontroverse um das Datenschutz Gesetz".

[11] B. Hołyst — „Ochrona informacji w polskich ośrodkach informatycznych". Materiały z konferencji nt. Prawne Problemy Systemów Informatycznych, Wrocław 20 V 1976.

[12] R. Hytha — Datenschutzgesetz gegen Computer — Terror. „Kriminalistik" nr 8, 1975.

[13] J. Martin — „Security, Accuracy and Privacy in Computer Systems" Prentice — Hall Inc., Englewood Cliffs, New Jersey 1973.

[14] R. A. H. v. zur Mühlen: „Computer — Kriminalität Gefahren und Abwehr — massnahmen" Luchterhand, Berlin, 1973.

[15] D. B. Parker — „Computer Related Crime and Data Security", Report No 477, Stanford Research Instytute, Dec. 1972.

[16] A. Sokołowski — *Ochrona zbiorów informacji w systemach informatycznych* „Informatyka" nr 12, 1973.

[17] Stanford Research Institute, Mento Park, California 94026: „Computer Abuse" Final Report, Nov. 1973.

[18] D. Van Tassel — „Information Security in Computer Environment"; Computer and Automation, Vol. 15, No. 8, 1969.

[19] A. Westin, M. Baker — „Databanks in a Free Society" Quadrangle Books N. Y., 1972.

[20] M. G. Wiesel — „La Criminalite Informatique", Traitement de l'Informatique 1974, pp. 37—45.

INFORMACJE. PRZEGLĄDY. RECENZJE

Przegląd aktualnych informacji gospodarczych

Realizacja ważniejszych zadań społeczno-gospodarczych w okresie styczeń—październik 1976 r.

Według wstępnych danych w **przemyśle uspołecznionym** w okresie styczeń—październik 1976 r. produkcja sprzedana wzrosła w porównaniu z tym samym okresem 1975 r. o 11,3%. W październiku br. w porównaniu z październikiem ubiegłego roku wzrost produkcji sprzedanej wynosił tylko 4,4%. Obniżenie dynamiki wzrostu produkcji w październiku w porównaniu z poprzednimi miesiącami wpłynęło w sposób istotny na obniżenie dynamiki za całe dziesięć miesięcy. W okresie styczeń-wrzesień wzrost produkcji sprzedanej w przemyśle uspołecznionym wynosił 12,1%. W sumie jednak osiągnięta dynamika produkcji jest nadal znacznie wyższa od założonej w Narodowym Planie Społeczno-Gospodarczym na 1976 r., przewiduje się bowiem, że w skali rocznej powinien nastąpić wzrost produkcji o 8,1%.

Przeciętne zatrudnienie wzrosło w omawianym okresie o 0,6%. W NPSG na rok bieżący zakłada się wzrost przeciętnego zatrudnienia o 1,4%, tempo wzrostu zatrudnienia było więc znacznie niższe od planowanego.

Osobowy fundusz płac wzrósł w porównaniu z okresem styczeń-październik 1975 r. o 9,6%. Dynamika wzrostu osobowego funduszu płac przewyższała dynamikę założoną w NPSG na 1976 r., w którym przyjęto, iż w skali rocznej osobowy fundusz płac powinien być wyższy w porównaniu z 1975 r. o 7,9%.

Wydajność pracy w przemyśle uspołecznionym w okresie styczeń-październik 1976 r. była więc wyższa w porównaniu z tym samym okresem ubiegłego roku o 10,6%. Wspomniany spadek tempa wzrostu produkcji w październiku spowodował również spadek tempa wzrostu wydajności pracy w porównaniu z okresem styczeń-wrzesień br. Mimo to osiągnięty w okresie dziesięciu miesięcy wzrost wydajności pracy był nadal znacznie wyższy od przyjętego w planie na rok bieżący, gdzie założono iż wyniesie tylko 7,3%.

Osiągnięty w okresie styczeń-październik przyrost produkcji sprzedanej był w 94,7% rezultatem wzrostu wydajności pracy oraz w 5,3% rezultatem wzrostu zatrudnienia. W NPSG na 1976 r. zakłada się, iż przyrost produkcji z tytułu wzrostu wydajności pracy wyniesie 91,4%, zaś z tytułu wzrostu zatrudnienia 8,6%, osiągnięte więc relacje są lepsze od planowanych.

Zaawansowanie wykonania rocznych zadań NPSG w zakresie produkcji sprzedanej, która po dziesięciu miesiącach wynosi 84,0%, jest wyższe od udziału tego okresu w wykonaniu zadań rocznych w 1975 r. (81,6%). Wyższe jest również zaawansowanie wydatków z osobowego funduszu płac, które wynosi 83,5%, podczas gdy w okresie styczeń-październik ubiegłego roku wynosiło 82,1% wykonania całorocznego.

W uspołecznionych przedsiębiorstwach budowlano-montażowych produkcja podstawowa osiągnięta w okresie dziesięciu miesięcy br. była w o 5,8% wyższa od produkcji osiągniętej w analogicznym okresie 1975 r. W październiku br. w porównaniu z październikiem ubiegłego roku produkcja podstawowa wzrosła tylko o 2,0%, co obniżyło wskaźnik za okres narastający. W okresie styczeń-wrzesień br. wzrost produkcji podstawowej wynosił 6,2%. W Narodowym Planie Społeczno-Gospodarczym na 1976 r. zakłada się wzrost produkcji podstawowej o 6,9%, osiągnięta więc w okresie dziesięciu miesięcy dynamika jest niższa od planowanej w skali rocznej.

Przeciętne zatrudnienie w okresie styczeń-październik br. było w porównaniu z tym samym okresem ubiegłego roku niższe o 1,7%. W NPSG na 1976 r. założono obniżenie dynamiki wzrostu zatrudnienia o 1,2%, osiągnięte więc wskaźniki świadczą o tym, że zahamowanie tempa wzrostu zatrudnienia w budownictwie jest większe od planowanego.

Osobowy fundusz płac wzrósł w porównaniu z okresem styczeń-październik ubiegłego roku o 2,8%, wobec zakładanego w NPSG wzrostu o 2,3%. Przekroczenie tempa wzrostu założonego na cały rok było więc po dziesięciu miesiącach stosunkowo niewielkie.