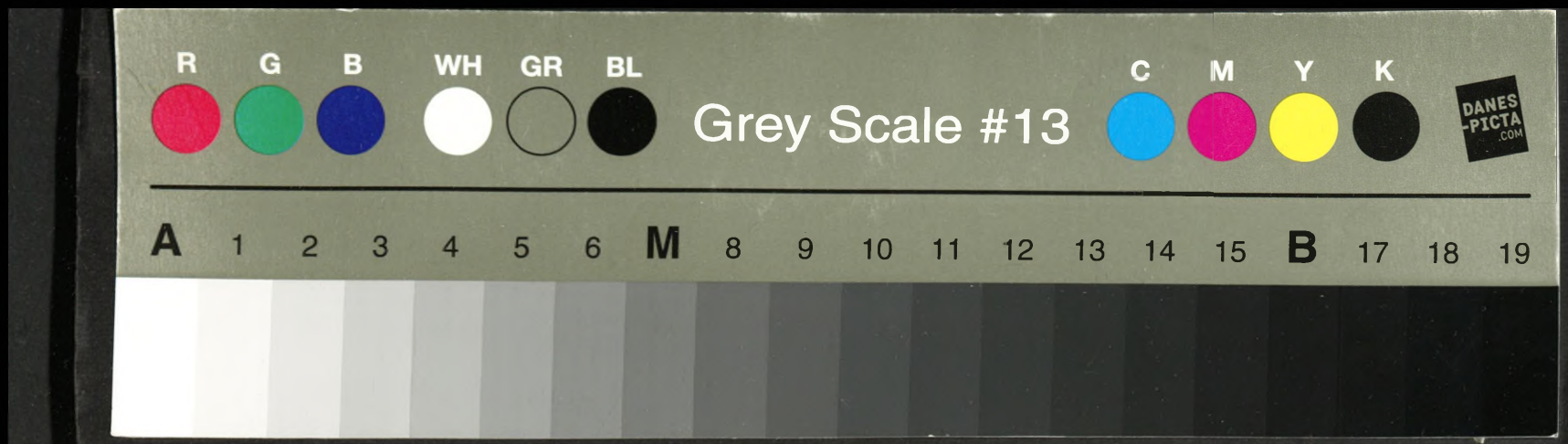


AKADEMIA SZTABU GENERALNEGO

IM. GENERAŁA BRONI
KAROLA ŚWIERCZEWSKIEGO

Egz. Nr 9

ZESZYTY NAUKOWE

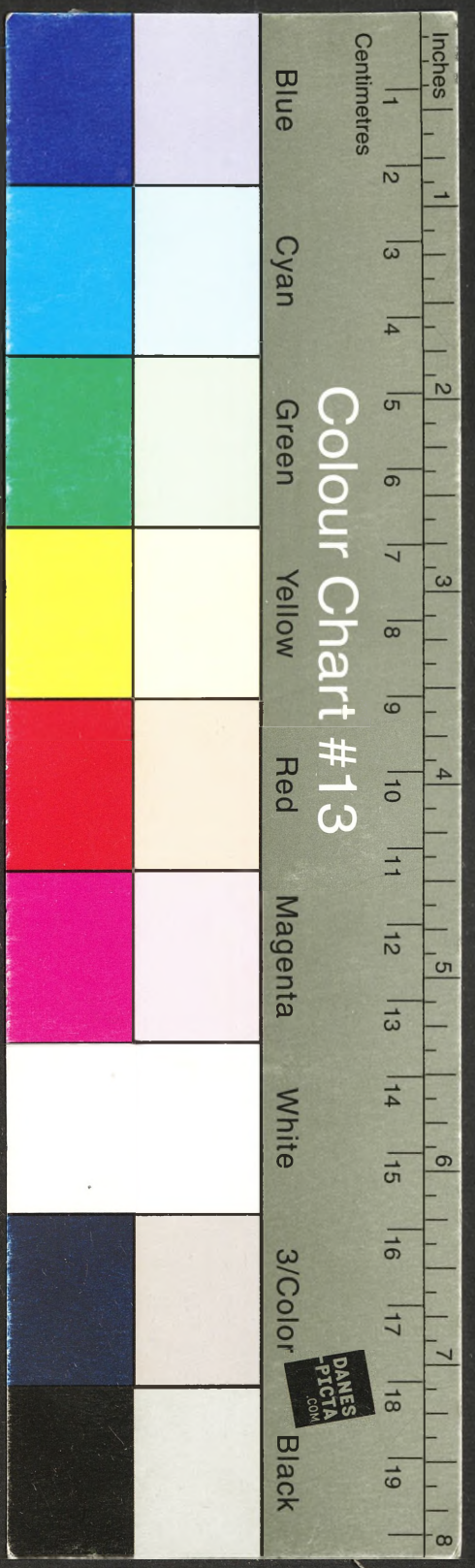
Ppłk rez. dr Zygmunt TOPOLEWSKI

KOMPUTEROWE ZABEZPIECZENIE POUFNOŚCI INFORMACJI

Rozprawa habilitacyjna

ZESZYT
Nr 07/89
Dodatek

WARSZAWA 1989



AKADEMIA
SZTABU GENERALNEGO
IM. GENERAŁA BRONI
KAROLA ŚWIERCZEWSKIEGO

ZESZYTY NAUKOWE

Ppłk rez. dr Zygmunt TOPOLEWSKI

KOMPUTEROWE ZABEZPIECZENIE POUFNOŚCI INFORMACJI

Rozprawa habilitacyjna

ZESZYT
Nr 07/89
Dodatek

WARSZAWA 1989

AKADEMIA SZTABU GENERALNEGO

im. gen. broni Karola Świerczewskiego

ppłk rez. dr inż. Zygmunt Topolewski

KOMPUTEROWE ZABEZPIECZENIE POUFNOŚCI INFORMACJI

Rozprawa habilitacyjna

Warszawa - 1989

Zamiast wstępu

Wojskowe systemy informatyczne są narażone nie tylko na infiltrację różnego rodzaju, np. podsłuch, przenikanie, przekłamanie, zniszczenie, ale przede wszystkim na przechwycenie informacji w czasie transmisji danych. Wszystkie te działania mają na celu uzyskanie ważnych (tajnych) informacji wojskowych przez rzeczywistego lub potencjalnego nieprzyjaciela. Mogą to być z pozoru nawet informacje błahe, np. rozszyfrowanie struktur organizacyjnych lub dyslokacji jednostek, jednak i one mogą doprowadzić do poniesienia przez wojsko nieobliczalnych i trudnych do ustalenia strat. Natomiast przechwycenie szczególnie ważnych informacji może spowodować podejmowanie błędnych decyzji na różnych szczeblach dowodzenia. Zabezpieczenie dostępu do informacji w systemach wojskowych jest zagadnieniem pierwszoplanowym. Ponadto wojskowi użytkownicy systemów informatycznych, którzy czerpią poważne korzyści z przetwarzania danych, nie mogą być narażeni na straty w postaci przenikania ich informacji do osób nieupoważnionych, czyli do nieprzyjaciela. Właśnie te sprawy związane z zagadnieniami ochrony ważnej informacji, a ściślej - informacji wojskowej, przyświecały autorowi w pisaniu niniejszej pracy, która w całości może i powinna być zastosowana w systemach wojskowych (co zostało podkreślone w punkcie 5.1).

W dziedzinie ochrony informacji poszukiwano nieustannie nowych rozwiązań naukowych, które by umożliwiły opracowanie bardziej skutecznych metod, a jednocześnie nie utrudniały pracy w ośrodku obliczeniowym. Dokładna analiza dotychczasowego systemu ochrony wykazała, że we wszystkich metodach ochrony decydującą rolę odgrywa człowiek, którego do obecnej pory nie brano pod uwagę. Wykazywana skuteczność metod ochrony, której współczynnik określano jako bliski jedności

(0,99993), okazała się teorią. Przy określaniu skuteczności należało uwzględnić współczynnik człowieka wynoszący 0,5 (co szczegółowo przedstawiono w monografii [26, s. 40-41]). Wówczas otrzymana skuteczność rzeczywista dotychczasowych metod mieści się w granicach 0,40-0,49. Wykazano, że mała skuteczność metod i uciążliwość ich stosowania stały się podstawą powszechnej ignorancji. Wykazano również, że tak zwane zabezpieczenie dostępu do zbiorów (zagwarantowane przez program zarządzający czy system operacyjny GEORGE, a opracowany przez producentów komputerów) jest niczym innym jak elementarną zasadą wieloprogramowości komputera. Ponadto stosowanie tzw. żetonów czy haseł rozpoznawczych jest mało skuteczne i nie stanowi żadnego zabezpieczenia informacji w komputerze. W dobie sieci komputerowych(rozdz. 5), jedyną i skuteczną metodą jest szyfrowanie informacji. Mimo tej bezspornej prawdy próby zastosowania i wdrożenia rozwiązań nowych napotykają nadal na przeciwności nie do pokonania.

Nauka, określana często jako społeczna działalność ludzi, która ma na celu poznanie rzeczywistości, jest motorem wszelkich poczynań człowieka. Naukowa działalność ludzka wyrasta z potrzeb poznania i opanowania istniejącej rzeczywistości, nawet z chęci jej przekształcenia. Istotą nauki jest działalność człowieka wynikająca z potrzeby i konieczności poznania tej rzeczywistości. W badaniach odkrywamy niejednokrotnie prawdy będące jej odbiciem. Często dochodzimy do wniosku, że to, co odkryliśmy nie jest niczym innym, jak umownie przyjętym obowiązującym wzorcem myślowym, obwarowanym dogmatycznymi regułami, za którymi stoi cała hierarchiczna drabina naukowa. Od tego momentu stajemy się ludźmi bezbronnymi. Trafiliśmy na skałę nie do pokonania - a jak mówi przysłowie - "głową muru nie przebijesz".

Jeśli jednak w badanej dziedzinie dojdziesz do wniosku, że należy coś dodać, pozostawiając obowiązujące wzorce, jesteś wygrany. Wszyscy ci przyklasną, gdyż swą teorią nikomu nie zaszkodziłeś, nic nie zmieniłeś, a tylko dodałeś nowe myśli. Zapaliłeś jeszcze jedną świeczkę na oświetlonej drodze. Gorsza sprawa, jeśli przy wprowadzaniu nowej myśli jesteś zmuszony negować obowiązujące wzorce. Natomiast czeka cię zupełna klęska, jeśli próbujesz zmienić główny nurt myśli naukowej i rozpocząć marsz w przeciwnym kierunku. Każdy, kto chce tego dokonać, musi pogodzić się z negatywną oceną swych myśli, a nawet z wykluczeniem ze społeczności naukowej. Niestety w nauce obowiązują pewne przyjęte wzorce, a nawet ośmielę się powiedzieć, dogmaty uznane za obowiązujące prawdy naukowe. Nie próbuj więc tego zmienić - jesteś po prostu za słaby.

Jak w tej sytuacji może być realizowany postęp? Postęp, który jest procesem jakościowych przemian, w których toku dokonuje się przechodzenie obiektów, zjawisk, układów, pojęć ku formom wyższym i doskonalszym. Przecież nie tylko trudno, lecz zupełnie nie można sobie wyobrazić nauki bez postępu, bez zdarzeń permutacyjnych wynikających z usprawnień, bez procesu przechodzenia od stanów doskonałych do doskonalszych. Jeśli to zjawisko nie zachodzi w nauce, mówimy o zastoju, o braku postępu. Jest to jednak formalny zastój czy brak postępu. Życie, a wraz z nim technika, idzie do przodu. Postęp techniczny, niezależnie od naszej woli, zmusza do opracowania nowych zasad i pojęć, do nowego spojrzenia na powstałą rzeczywistość i nowej oceny istniejącego stanu. Proces oceny rzeczywistości powinien trwać ciągle. Powinien to być wieloetapowy proces przemian, proces rodzenia się nowych koncepcji i teorii. Ba - powinien być, ale nie jest. Zawsze ktoś lub coś staje w poprzek drogi.

Zdarza się jednak, że ktoś idzie przeciw utartym schematom, przeciw obowiązującym zasadom. Jeśli nie znajdzie poparcia ludzi wysoko postawionych w hierarchii nauki, ten przegrywa. Są jednak nieliczne przypadki, że komuś uda się przebić przez gąszcz zakazów, schematów i zakurzonych od starości, lecz obowiązujących, zasad naukowych. Wtedy nagle wszyscy zaczynają ten fakt dostrzegać. Chwalą go, czasami ktoś jeszcze gani. Jednak wszyscy zaczynają sobie zdawać sprawę, że w danej dziedzinie wystąpiło zjawisko rewolucji naukowej. Mamy więc do czynienia z jedną z form postępu zachodzącą w drodze procesu kierunkowych przemian w rozwoju społecznym. Oba te pojęcia, zarówno postęp, jak i rewolucja, mają wspólną cechę - występują przeciw wszystkiemu, co nieaktualne, stare, zmurszałe i wsteczne. Należy zgodzić się z twierdzeniem, że rewolucja w nauce to nic innego jak działanie przeciw (kontrrewolucja) obowiązującym zasadom myślenia (które kiedyś były rewolucyjne). Nikt nie określi mianem rewolucji naukowej podstawowych praw fizyki nauczanych w szkołach, które w swoim czasie były rewolucyjne. Nikt nie nazwie rewolucją teorii Kopernika, twierdzenia Einsteina czy wynalezienia pierwszej maszyny cyfrowej, chociaż dzieła te były bez wątpienia rewolucyjne.

Postęp w informatyce (jak wykazano w p. 1.3) przebiegał stosunkowo wolno, począwszy od roku 1623 do 1941, w którym opracowano pierwszą maszynę cyfrową. Od tej daty jesteśmy świadkami gwałtownego rozwoju sprzętu, języków programowania i technologii przetwarzania danych. Nowa rzeczywistość stawia nowe wymagania w zakresie ochrony informacji. Nie można trzymać się uparcie opracowanych przed wieloma laty naukowych teorii dotyczących metod informacji, chociaż te teorie, jeśli nawet nie były rewolucją w nauce, to niewątpliwie stanowiły postęp. Nie można uparcie trzymać się opracowanych zasad i metod, które są mało skuteczne i uciążliwe, a nawet niemożliwe do praktycznego zastosowania. Ich sku-

teczność oparto na prawdopodobieństwie ochrony, które - niestety - było tylko prawdopodobieństwem teoretycznym nie mającym nic wspólnego z rzeczywistością. Ponadto w świecie postępu technicznego dotychczasowe metody stały się mało skuteczne. Życie potwierdziło zasadę, że to, co kiedyś było postępowe i wystarczająco dobre, dziś staje się nieprzydatne, o wartości wprost muzealnej. Obecnie często informacja jest przesyłana liniami transmisji danych, czyli wychodzi poza ośrodek obliczeniowy. Jesteśmy już w tej chwili świadkami, że powstają sieci komputerowe, a nawet obserwujemy początki komputerowych sieci satelitarnych. Cóż więc znaczą w tych układach dotychczasowe metody ochrony, jeśli informacja jest przesyłana w kosmos i każdy ją może przechwycić. Dziś jest ważna prawie wyłącznie kryptologia, a dotychczasowe metody można spokojnie przekazać do archiwum. Jednak i tej oczywistej prawdy nie można wypowiadać głośno, bez narażenia się wyznającym dogmaty, za którymi stoi cały pozorny autorytet przyjętych schematów.

Niewątpliwie postęp w informatyce w niektórych latach przybierał formy gwałtownych przemian, niemal przewrotu, rewolucji w nauce. Należy jednak na ten proces popatrzeć i z innej strony. Może nawet oczami poety, który pisze, by nie burzyć przeszłości ołtarzy, choć sami mamy doskonalsze wznieść. Właśnie to ostrzeżenie nas zobowiązuje. Nie przypuszczam, by ktokolwiek chciał niweczyć osiągnięcia swoich poprzedników. Gdyby jednak nie było roku 1623, to Hollerith może nie byłby w stanie skonstruować pierwszej maszyny pracującej na kartach dziurkowanych. Gdyby natomiast nie było maszyn licząco-analitycznych, nie byłoby komputerów itd. itd. Fakty te są najlepszym dowodem, że postęp w nauce jest niemożliwy bez głębokiej analizy tego, co było i co jest, bez wyciągnięcia wniosków z tej właśnie analizy. Postęp jest procesem ciągłym i rodzi się dzięki dotychczasowym osiągnięciom nauki. Rewolucja, chociaż stanowi proces

gwałtownych przemian, wyrasta również z istniejących i obowiązujących osiągnięć nauki. Nauka wymaga prawdy i dlatego uparcie dąży do jej odkrycia. Właśnie poszukiwanie prawdy jest motywem poznawania zjawisk, poznawania rzeczywistości, która na każdym etapie jest inna. Ta zmieniająca się rzeczywistość w zależności od czasu i warunków wymaga nowych pojęć, nowych definicji, nowego nazewnictwa, po prostu nowych prawd. Z tym należy się pogodzić. Jest to niezbędny warunek rozwoju nauki.

Jest to w końcu jeszcze jedna, niemniej ważna sprawa. Chodzi o akceptację polskiej myśli naukowej. Chodzi o to, by nie trzeba było jej przekazywać na Zachód, gdzie przyjmowana jest z otwartymi rękami. Chodzi o to, by rozwój polskiej myśli naukowej znalazł wreszcie u nas prawo obywatelstwa. By ludzie odpowiedzialni za jej postęp nie obrażali się, gdy ich teoria zostanie podważona. By pamiętali, że nowe osiągnięcia są możliwe dzięki ich pracy, dzięki odkrytym przez nich teoriom naukowym.

Podstawowe pojęcia używane w książce

DESZYFRACJA - proces polegający na poszukiwaniu klucza, którym przywraca tekst pierwotny.

ENTROPIA - w teorii informacji miara nieokreśloności, chaotyczności; wartość entropii $H(x)$ określa się wzorem

$$H(x) = - \sum_{i=1}^{n} P(x_i) \log P(x_i),$$

w którym $P(x_i)$ - prawdopodobieństwo przyjęcia przez zmienną losową X wartości x_i.

ERGODYCZNOŚĆ - w teorii informacji jest zjawiskiem, przy którym

- mimo wzrostu długości ciągu szyfrowego - nie zmienia się ilość informacji zawartych w nim. Gdy wiadomość (ciąg szyfrowy) ma właściwość ergodyczną, wówczas nieprzyjaciel nie otrzymuje informacji o kluczu.

IDENTYFIKACJA - sprawdzenie za pomocą systemu lub urządzenia czy określona osoba jest upoważniona do otrzymania lub przekazania informacji.

INFILTRACJA - celowe przenikanie nie upoważnionych osób (grup) do zbiorów informacji. Osoby te dążą zarówno do naruszenia poufności zbiorów, jak i do dezorganizacji systemu informatycznego.

KANAŁ - urządzenie do przesyłania informacji między procesorem lub pamięcią operacyjną a urządzeniami peryferyjnymi.

KLUCZ - jeden lub więcej znaków zawartych w wyodrębnionej jednostce zapisu danych używanych do operacji sortowania, wyszukiwania lub szyfrowania informacji.

KOD - system znaków umownych używanych do przekazywania informacji.

KOMPUTER KOMUNIKACYJNY - komputer umożliwiający współpracę komputerów lub urządzeń końcowych zainstalowanych w sieci komputerowej.

KONCENTRATOR - urządzenie realizujące zasadę zwielokrotnienia, pozwalające sygnałom z wielu wejść uczestniczyć w transmisji danych przez jedno lub kilka łączy. Koncentrator zamienia wiele wejść o różnych szybkościach na mniejszą liczbę wyjść o odmiennych szybkościach, co nie było możliwe w multiplekserze.

KONTROLER TELEKOMUNIKACYJNY - urządzenie do zdalnego sterowania transmisją informacji (protokołem komunikacyjnym). Urządzenie pracuje na szybkim łączu, zwanym czasem "magistralą", spełniającym jedynie funkcje zwielokrotniania.

KRYPTOGRAFIA - umiejętność przekształcania tekstu pisanego, zrozumiałego dla ogółu ludzi, w tekst utajniony - dostępny i możliwy do odczytania tylko przez odbiorcę.

KRYPTOLOGIA - nauka o utajnianiu informacji, obejmująca kryptografię i kryptoanalizę.

MOC KRYPTOGRAFICZNA - czas potrzebny na złamanie klucza i odczytanie zaszyfrowanej informacji. Czas mierzy się od chwili przechwycenia szyfrogramu do jego odczytania.

MODEM - (modulator - demodulator) urządzenie do nadawania zapisowi danych cyfrowych postaci sygnałów umożliwiających ich transmisję przez łącze telekomunikacyjne, a także do odtworzenia pierwotnej postaci zapisu.

MULTIPLEKSER - urządzenie umożliwiające jednoczesne przesyłanie wielu komunikatów przez jeden kanał.

PAKIET - blok informacji uzupełnianej pewnymi danymi dodatkowymi, pozwalającymi traktować całość jako jednostkę autonomiczną, umożliwiającą dobór trasy i przesyłanie w sieciach komputerowych.

PROTOKÓŁ - standardowe procedury telekomunikacyjne, organizujące transmisję danych między komputerami a terminalami.

PROCESOR - urządzenie w komputerze cyfrowym, umożliwiające wykonywanie autonomiczne ciągu rozkazów.

SIEĆ KOMPUTEROWA - układ komputerów, węzłów i urządzeń końcowych połączonych liniami (kanałami) transmisji danych.

SZYFR - rodzaj kodu, który utrudnia odtworzenie wiadomości osobie nie upoważnionej.

TERMINAL - urządzenie przeznaczone do kontaktowania się z komputerem z oddalonego od niego miejsca.

WĘZEŁ - element sieci komputerowej, zespół urządzeń między komputerem i końcówką. Węzły dzielimy na centralne (znajdujące się przy centralnym

systemie obliczeniowym) i końcowe (znajdujące się między kanałem i końcówką).

Definicje dotyczące poufności informacji według National Berau of Standards and Assn for Computing Machinery, 1974:

BEZPIECZEŃSTWO DANYCH polega na ich ochronie przed przypadkowym bądź umyślnym zniszczeniem, ujawnieniem lub modyfikacją.

POUFNOŚĆ jest pojęciem dotyczącym ludzi. Jest to prawo jednostki do decydowania o tym, jakimi informacjami chce się podzielić z innymi ludźmi i jakie jest skłonna od nich przyjąć.

TAJNOŚĆ jest pojęciem dotyczącym danych. Jest to atrybut danych opisujący stopień ochrony, której mają one podlegać.

NIENARUSZALNOŚĆ jest pojęciem dotyczącym danych. Dane nienaruszone to takie, które nie zostały złośliwie zmienione, ujawnione lub zniszczone.

1. INFORMACJA W SYSTEMACH KOMPUTEROWYCH

Informacja odgrywa istotną i decydującą rolę w wielu dziedzinach naszego życia. Informację tworzymy, gromadzimy, przetwarzamy i przekazujemy lub przesyłamy na odległość. Zjawisko to związane, a raczej nazwane, informacją łączy się szczególnie z cywilizacją. Mówiąc o cywilizacji mamy na myśli nie tylko osiągnięcia w nauce, kulturze czy sztuce, ale przede wszystkim zjawiska związane z organizacją i technologią produkcji i stosunkami międzyludzkimi.

Informacja to element procesu wiążącego człowieka z otoczeniem, to podstawowy element określonej cywilizacji. Trzeba także pamiętać, że właśnie informacja spełnia podstawową funkcję w procesach poznawczych. Pośredniczy ona w procesie zrozumienia rzeczywistości, w procesie jej odzwierciedlenia w naszej świadomości. Dlatego informacja powstaje, tworzy się, a raczej uzyskujemy ją głównie przez obserwację zjawisk otaczającego nas świata. Analizując to zjawisko, J.L. Kulikowski pisze: "Nie ma istotnych powodów, aby z prawnego punktu widzenia traktować pod tym względem informację inaczej niż traktujemy dziś dobra naturalne kraju, jego przyrodę, zasoby wodne lub atmosferę" [7, s. 6]. Uważam to stwierdzenie za podstawę do poważnego potraktowania samej informacji, która na równi z innymi dobrami naszego kraju winna być gromadzona i wykorzystywana, a jednocześnie odpowiednio zabezpieczona i chroniona.

W uchwale Rady Ministrów PRL z dnia 12 lutego 1971 roku znajdujemy następującą definicję informatyki, a w niej informacji: "Informatyka dotyczy całokształtu prac nad zbieraniem, przechowywaniem i przetwarzaniem zakodowanej informacji, opracowywaniem i wykorzystywaniem w gospodarce narodowej oraz zapewnieniem potrzebnych do tego środków technicznych". Mimo że informatyka weszła do słownika polskiego w końcu 1968 roku,

to już w 1971 roku znalazła dla siebie prawo obywatelstwa w postaci uchwały, z której wynika, że jej głównym celem jest automatyzacja działań na informacji. Czym jest więc sama informacja, której podporządkowano jedno z największych osiągnięć XX wieku - komputer. Według słownika "Informacja - miara zmniejszenia nieokreśloności wiedzy u odbiorcy sygnału (wiadomości) o stanie nadawcy lub o pewnym zdarzeniu" [22]. Informacją zajmuje się nauka zwana nauką o informacji. Ingeruje ona w różne dziedziny dotyczące tworzenia, przetwarzania, przechowywania, przesyłania, wyszukiwania i selekcjonowania informacji a w końcu wzbogacania ludzkiej myśli naukowej w różnych dziedzinach wiedzy [3], [5].

1.1. Informacja - towar szczególnego rodzaju

Powyższe rozważania wskazują na znaczenie samej informacji, wartość informacji przechowywanej i przesyłanej, a szczególnie jej wartość dla innych nauk. Ażeby jednak w pełni zdać sobie sprawę z istoty informacji i z jej roli w dzisiejszym społeczeństwie, należy dokonać analizy historycznych przemian cywilizacyjnych i roli, jaką odegrała informacja. Na obecnym etapie są znane dwie cywilizacje: przemysłowa i rolnicza, wraz ze swoimi licznymi odmianami. W ostatnich dziesiątkach lat naszego stulecia zaczyna się tworzyć nowa cywilizacja - cywilizacja informacji komputerowej, lub wprost - cywilizacja informacji. Tworzy się ona obok cywilizacji przemysłowej, w której przetwarzanie informacji staje się głównym procesem ekonomicznym. Wraz z wprowadzaniem automatyzacji zmniejsza się udział bezpośredniej pracy ludzkiej w procesie produkcji, co gorsze - zaczyna narastać konflikt pomiędzy kapitałem a pracą. Konflikt ten prowadzi nieuchronnie do różnego typu rewolucji. Ogólnie znane jest rodzenie się rewolucji w społeczeństwach nisko uprzemysłowionych. W tym przy-

padku zachodzi ciekawe zjawisko tworzenia się cywilizacji przemysłowych bez konfliktów pomiędzy pracą a kapitałem. Zjawisko to można tłumaczyć humanitarnymi założeniami ustroju oraz wysoką świadomością wytyczającą kierunek postępu. Jednak w ślad za postępem wkracza na rynek produkcyjny nowy towar - informacja. Bez niej nie może obyć się żaden zakład przemysłowy, żadne przedsiębiorstwo handlowe, żadna nauka określonej wiedzy ani też ludzie sprawujący władzę. Bez szybkiej i wiarygodnej informacji nie można sobie wyobrazić postępu technicznego. Informacja staje się elementem niezbędnym przy wszelkich poczynaniach. Staje się towarem koniecznym człowiekowi. Jest to jednak towar niezwykły, inny nawet niż pieniądz. Pieniądz podlega wszelkim prawom towarowym, a informacja tym prawom nie podlega, a mimo to jest towarem. Jakie są więc cechy charakterystyczne informacji, właściwe tylko jej?

Pierwsza z nich to niezniszczalność informacji w trakcie konsumpcji. Oznacza to, że liczba informacji nie zmniejsza się w toku jej wykorzystywania.

Drugą cechą przynależną wyłącznie informacji jest możliwość powiększania się liczby informacji w toku użytkowania. Informacja pobrana z centralnej bazy danych może wzbogacić bazy poszczególnych użytkowników, bez uszczerbku dla źródła centralnego.

Trzecią cechą są szczególnego rodzaju właściwości synergetyczne. To znaczy, że wartość sumy informacji jest większa niż suma informacji składowych. Zjawisko to należy tłumaczyć tym, że informacja jako szczególny rodzaj towaru posiada również szczególną wartość: jest nią jakość. Podział sumy informacji na części obniża jakościowo ich wartość, a może się zdarzyć, że któraś z części nie będzie posiadała żadnej wartości, czego nie można powiedzieć o innych towarach, a szczególnie o pieniądzu.

1.2. Konieczność ochrony informacji

W literaturze o ochronie informacji występuje jeden główny czynnik uzasadniający jej konieczność. Czynnikiem tym jest zasada gromadzenia informacji w miarę postępu techniki i rozwoju sprzętu komputerowego. Komputerowe przetwarzanie informacji spowodowało nie spotykaną dotychczas centralizację przechowywanej i przetwarzanej informacji. Spowodowało to niewątpliwie zagrożenie poufności informacji i konieczność jej ochrony. Centralizacja nie byłaby taka groźna dla poufności informacji, gdyby informacja nie stała się czynnikiem kształtującym naszą cywilizację i decydującym o jej rozwoju.

Ponadto informacja jako towar szczególnego rodzaju, który - niezależnie od innych cech - ma również wartość i cenę. I to także decyduje o konieczności ochrony. Ochrona w tym przypadku jest tym bardziej konieczna, gdyż wartość informacji często zależy od jej jakości.

Należy również pamiętać o jeszcze jednym elemencie związanym z koniecznością ochrony informacji. A. Sokołowski sformułował to następująco: "Utrata informacji nie tylko dezorganizuje działania systemu informatycznego, ale przede wszystkim może spowodować podejmowanie na różnych szczeblach błędnych decyzji" [24, s. 17].

1.3. Marzenia i rzeczywistość w ochronie informacji

W literaturze światowej dużo pisze się o ochronie informacji, metodach ochrony systemu kompleksowego, architekturze maszyn sterujących systemami ochrony, matematycznych modelach ochrony, pozatechnicznych aspektach bezpieczeństwa danych obszarów przyszłych badań. Ostatnio pojawiły się takie hasła, jak "tajny kod nie do złamania", "jawny klucz", "bezpieczny system szyfrowania" oraz wiele podobnych dotyczących tak

zwanej jawności kluczy lub całego systemu ochrony. Trzeba przyznać, że takie hasła, zabarwione posmakiem propagandy, pobudzają fantazję ludzką. Począwszy od szyfru Cezara, sięgającego początków naszej ery, po dzień dzisiejszy wszelkie metody ochrony informacji były trzymane w ścisłej tajemnicy. Dotyczyły one przede wszystkim ochrony tajemnicy państwowej i wojskowej. Pojawienie się haseł o jawności metod, a szczególnie kluczy szyfrowych, może pobudzić nawet najspokojniejsze umysły.

Skąd ta nagła zmiana w poglądach na system ochrony informacji i w dodatku przejście z jednej skrajności w drugą - od ścisłej tajemnicy, do całkowitej jawności? Ażeby w pełni zdać sobie sprawę ze zmiany poglądów na zagadnienie ochrony informacji, należy rozpatrzyć rozwój komputeryzacji, a szczególnie technologię przetwarzania danych.

Można z całą pewnością stwierdzić, że przełomem w przetwarzaniu danych był rok 1623, w którym Wilhelm Schickard, profesor języków biblijnych i astronomii w Tybindze, wynalazł pierwszą maszynę do dodawania i odejmowania. Mogła ona również mnożyć i dzielić za pomocą tabliczki mnożenia. Chociaż po drodze wynaleziono wiele maszyn i aparatów liczących, to jednak kolejnym momentem przełomowym był rok 1888. Dopiero po 265 latach Herman Hollerith skonstruował maszynę umożliwiającą sumowanie danych wydziurkowanych na kartach. Był to prototyp tabulatora. Był to jednocześnie początek maszyn licząco-analitycznych, które wykorzystano przy spisie ludności w USA w 1890 r., w Kanadzie w 1891 r. oraz w Rosji w 1897 r. Od tej chwili notuje się silny rozwój maszyn liczących opartych na technice przetwarzania danych. Już w 1941 roku opracowano pierwszą maszynę cyfrową, pierwszy komputer pracujący na przekaźnikach, a w 1947 r. zastosowano pamięć magnetyczną w postaci bębna magnetycznego. Zastosowanie pamięci magnetycznej stworzyło nowe możliwości rozwoju komputerów. Jesteśmy świadkami burzliwego rozwoju

zarówno sprzętu, jak i języków programowania, a szczególnie technologii przetwarzania danych, której zasady zmieniają się wraz z możliwościami technicznymi. Pierwsze maszyny cyfrowe pracowały wyłącznie jednoprogramowo i dopiero po zastosowaniu programów zarządzających przekształcono je w maszyny wieloprogramowe. Przetwarzanie danych odbywa się w ośrodkach obliczeniowych, w których koncentruje się cały cykl technologiczny, począwszy od dokumentów źródłowych do informacji wynikowej w postaci tabulogramu. Ochronę informacji zawężono do samego ośrodka obliczeniowego, a jej metody są trzymane w ścisłej tajemnicy.

Jednak wraz z rozwojem sprzętu komputerowego zachodzi konieczność zmiany technologii przetwarzania i przesyłania informacji. Metody ochrony w zakresie zabezpieczenia samego komputera czy nawet całego ośrodka stały się niewystarczające, jeśli informacje są transmitowane. Teletransmisja wymaga szyfrowania przesyłanej informacji. Dotychczasowe systemy ochrony i szyfrowanie tradycyjne za pomocą tajnego klucza są anachroniczne. To co było dobre, co było rewelacją kilka lat temu, stało się nagle nieprzydatne. Nowa technologia wymaga nowych i bardziej skutecznych metod ochrony.

W ostatnich kilku latach nastąpił rozwój sieci komputerowych, a nawet komputerowych sieci satelitarnych. Jesteśmy świadkami, że postęp techniczny wyprzedził tak dalece proces technologiczny, że nie jesteśmy w stanie dotrzymać kroku. Tymczasem wraz z rozwojem sprzętu rośnie krąg zleceniodawców i rosną wymagania w zakresie przetwarzania danych. Tworzą się coraz to nowe i większe sieci komputerowe i satelitarne. Im szerzej stosuje się transmisję danych, tym bardziej rośnie niebezpieczeństwo przechwycenia informacji. Odróżnienie przeciwnika od przyjaciela jest po prostu niemożliwe. Nie można więc mówić o metodach ochrony,

o zabezpieczeniu technicznym czy organizacyjnym. Jedyną i słuszną drogą do rzeczywistej ochrony informacji jest kryptologia.

Nowa rzeczywistość postawiła przed kryptologią nowe zadania. Dotychczas zadaniem kryptologów było opracowanie metody szyfrowania, której przeciwnik nie był w stanie złamać. Jednocześnie należało opracować takie zasady deszyfracji, by można było rozszyfrować każdą informację przeciwnika. Tego typu zadanie, chociaż trudne do zrealizowania, było realne i wystarczające na etapie przesyłania informacji pomiędzy dwoma komputerami czy też komputerem centralnym a oddalonym terminalem (końcówką). W takich układach można było mówić o tajnych kluczach szyfrowych, częstej ich wymianie. Zadanie to stało się nierealne w sytuacji sieci komputerowych, a szczególnie satelitarnych, którymi informacja jest przesyłana w kosmos i praktycznie każdy może ją przechwycić. Dziś nie wystarcza samo szyfrowanie informacji, chociażby metoda miała dużą moc kryptograficzną. Sieci komputerowe stawiają przed nami nowe wymagania, które muszą być spełnione, jeżeli chcemy chronić informację. Wymagania te są następujące.

1) Metoda szyfrowania musi mieć dużą moc kryptograficzną. Oznacza to, że o jakości metody decyduje jej odporność na złamanie szyfru (klucza) przez kryptoanalityków.

2) Metoda musi mieć możliwość identyfikacji nadawcy i odbiorcy przesyłanego meldunku. Chodzi o to, by nadawca przekonany był, że przesyłana informacja trafi do określonego odbiorcy i tylko on może ją rozszyfrować. Również odbiorca musi być przekonany, że otrzymany meldunek został przesłany przez właściwego nadawcę, czyli nie stanowi tak zwanej "fałszywki" - meldunku celowo sfałszowanego.

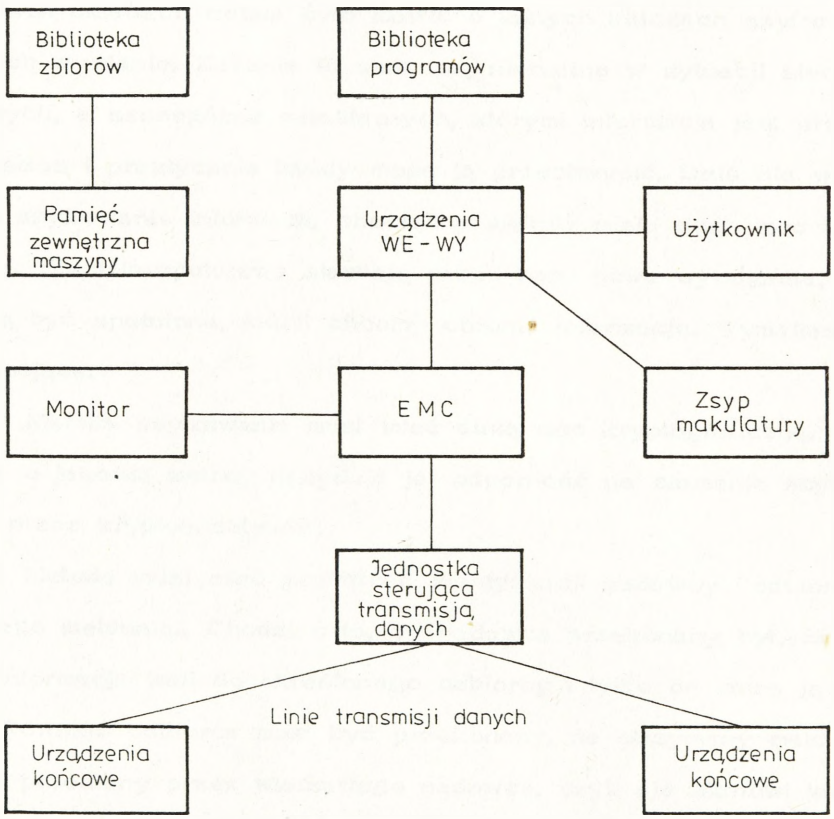
3) Metoda musi mieć możliwość szyfrowania nagłówka (adresu), a

mimo to możliwość przesyłania różnych ciągów szyfrowych (zaszyfrowanej informacji) w sieciach komputerowych.

Spełnienie tych wymogów gwarantuje bezpieczne przesyłanie informacji w sieciach. Do tej pory nie uwzględniano drugiego i trzeciego wymagania, a nawet je lekceważono. Dziś nie można lekceważyć żadnego z wymienionych warunków. Ponadto metoda musi być jawna, a mimo to niemożliwa do złamania przez osobę nie upoważnioną. W praktyce można spełnić wymienione trzy wymogi i jawność metody. Jest to jednak zupełnie odmienne zagadnienie, wymagające osobnego opracowania.

2. INFILTRACJA W SYSTEMACH KOMPUTEROWYCH

Zbiory informacji w systemach komputerowych mogą być narażone na niepoprawny odczyt, celowe przekłamanie lub zniszczenie. Jest to groźne przede wszystkim tam, gdzie są one magazynowane lub przetwarzane, tzn. w pamięci zewnętrznej i wewnętrznej komputera, w bibliotece zbiorów danych, w bibliotece programów, w urządzeniach WE-WY, w liniach transmisji danych, u personelu obsługującego i technicznego, a nawet u samego użytkownika (rys. 1).



Rys. 1. Wykaz elementów narażonych na infiltrację

2.1. Sposoby infiltracji

Znając elementy narażone na infiltrację należy rozpatrzyć, jakimi sposobami mogą posługiwać się osoby nie upoważnione, by zdobyć określone informacje. Według Sokołowskiego [23, s. 21-33] infiltrację dzielimy na: przypadkową i celową, którą z kolei dzielimy na pasywną i aktywną. Niektóre rodzaje infiltracji możemy określić jako szpiegostwo komputerowe, szczególnie w odniesieniu do systemów wojskowych.

W wyniku infiltracji przypadkowej informacja dostaje się w ręce osoby niepowołanej. Jest to spowodowane błędnym działaniem systemu lub emc. Wtedy należy powtórzyć wydawnictwa. Infiltracja ta może wystąpić również na skutek niewłaściwego postępowania personelu obsługującego, technicznego, zaniedbań użytkownika, operatora lub osoby nadzorującej pracę systemu.

Infiltracja pasywna, często określana mianem infiltracji celowej, polega m.in. na przyłączeniu się do przewodów transmisji danych, przechwytywaniu i badaniu kopii wydawnictw komputerowych, badaniu a nawet kradzieży nośników informacji lub kopiowaniu i wynoszeniu poza teren ośrodka obliczeniowego taśm magnetycznych, ich wydawnictw.

Infiltracja aktywna polega na stosowaniu takich metod, jak:

a) uzyskiwanie dostępu do systemu przez osoby nie upoważnione,

b) uzyskiwanie potwierdzenia tożsamości lub hasła prawowitego użytkownika,

c) korzystanie z przyłączanych urządzeń końcowych, gdy właściwy użytkownik zawiesza pracę,

d) przechwytywanie informacji użytkownika i podstawianie jej w miejsce innych informacji,

e) nielegalne korzystanie z komputera w czasie nie rejestrowanych prac konserwatorskich,

f) nielegalny wydruk zawartości pamięci komputera po zakończeniu działania programu [26, s. 7].

Inną, lecz nie mniej niebezpieczną infiltracją, jest oszustwo i szpiegostwo komputerowe. Znane są przypadki tzw. oszustwa dokonywanego na listach płac, polegającego na niewycofywaniu kartotek zmarłych lub zwolnionych pracowników. W krajach Europy Zachodniej rozpowszechnia się szpiegostwo komputerowe systemów gospodarczych. Przenikanie informacji może przynieść ogromne straty gospodarce narodowej w dowolnym kraju. Natomiast przenikanie informacji w systemach wojskowych może mieć daleko gorsze następstwa i spowodować trudne do oszacowania szkody [23, s. 17].

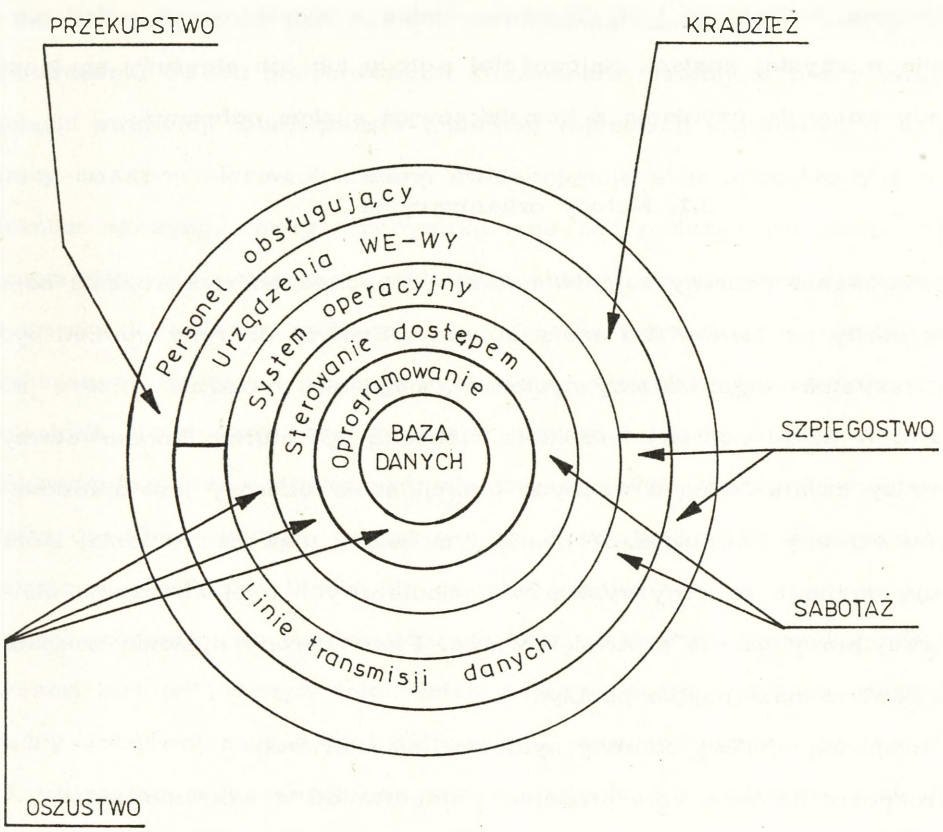
Metody infiltracji można ująć w pięć podstawowych grup:

1) przekupstwo,
2) oszustwo,
3) kradzież,
4) szpiegostwo,
5) sabotaż.

Osoby nie upoważnione, ażeby uzyskać informacje z bazy danych lub transmitowane, mogą oddziaływać na następujące elementy związane z przetwarzaniem danych:

1) personel obsługujący,
2) system operacyjny,
3) oprogramowanie użytkowe,
4) urządzenia WE-WY,
5) pamięć zewnętrzna,
6) linie transmisji danych,
7) sterowanie dostępem do bazy.

Współzależności między grupami działań infiltracyjnych i elementami związanymi z przetwarzaniem danych pokazano na rys. 2.



Rys. 2. Podstawowe kierunki infiltracji

3. METODY OCHRONY INFORMACJI KOMPUTEROWEJ

Metody ochrony informacji komputerowej można podzielić na trzy grupy: organizacyjne, techniczne i programowe. Żadna z wymienionych metod nie występuje w czystej postaci. Najczęściej metody lub ich elementy są łączone. Wtedy mamy do czynienia z kompleksowym system ochrony.

3.1. Metody organizacyjne

Organizowanie ochrony zbiorów należy rozpocząć od wyznaczenia odpowiedniej osoby na stanowisko szefa ochrony. Szefami ochrony powinni być przede wszystkim organizatorzy systemów, mogą się wywodzić także z programistów. W skład ochrony komputera wchodzą operatorzy, konserwatorzy i kierownicy zmian. Jedną z ważnych funkcji szefa ochrony jest opracowanie planu ochrony komputera. W planie tym należy ująć zagadnienia, które zobrazują ważność ochrony systemów komputerowych i jej znaczenie dla prawidłowej pracy całego przedsiębiorstwa. Plan ochrony systemu komputerowego zawiera następujące punkty:

1) kompletną analizę ochrony systemu komputerowego,

2) rozpoznanie oraz opis procedur i usprawnień w zakresie metod ochrony zbiorów,

3) opis elementów ośrodka obliczeniowego i zakładu, w których stosowane metody nie zaspokajają na bieżąco potrzeb ochrony zbiorów,

4) oszacowanie kosztów, wymagań technicznych i zmian organizacyjnych koniecznych do realizacji środków ochrony,

5) dokładny, czasowy plan realizacji programów z uwzględnieniem przetwarzania szczególnie ważnych systemów.

Ponadto w planie ujmuje się takie zagadnienia, jak zabezpieczenie biblioteki programów, taśm i dysków, zabezpieczenie przeciwpożarowe, prowadze-

nie ewidencji pracy emc, klasyfikację danych, programów i dokumentacji, politykę personalną, procedury testujące i kontrolę wewnętrzną [4].

Najistotniejsze jest jednak ścisłe rozliczenie czasu pracy komputera i kontrola wstępu do hali maszyn. Rozliczenie czasu pracy emc polega na prowadzeniu trzech podstawowych dokumentów: dziennika pracy maszyny, książki ewidencji tabulogramów i książki rejestracji monitorów. W dzienniku pracy maszyny kierownik zmiany ewidencjonuje stan początkowy i końcowy licznika maszyny, osoby przebywające na hali podczas realizacji ważnych programów oraz pobierane i oddawane zbiory danych wraz z dokumentacją systemów. W książce ewidencji tabulogramów prowadzi się rejestr wszystkich wykonanych na emc i przekazanych do użytkownika wydawnictw. Ponadto rejestruje się wydawnictwa wykonane błędnie i dokonuje adnotacji o ich zniszczeniu. Ważne tabulogramy niszczy osobiście kierownik zmiany w obecności operatora systemu i maszyny. Na specjalną uwagę zasługuje książka rejestracji monitorów. Wszystkie ośrodki traktują wydruk z monitora jako dokument potrzebny do realizacji programów użytkowych, kompilacji itp. Tymczasem jest on jedynym dokumentem dającym pełen obraz pracy emc. Tak ważny dokument musi być rejestrowany i przechowywany wraz z dokumentami podlegającymi szczególnemu zabezpieczeniu. Na podstawie tych dokumentów rozlicza się emc z przetwarzania danych, konserwacji i testosowania oraz awarii maszyny [26]. Każde odstępstwo od podanych zasad stwarza możliwość infiltracji lub wykonywania nielegalnych prac na zbiorach danych.

3.2. Metody techniczne

Metody techniczne to pewien układ techniczny i określony sposób postępowania. Mają one zabezpieczyć zbiory przed infiltracją lub sam komputer przed uszkodzeniem. Dlatego przez układ techniczny rozumiemy takie urządzenie, które chroni przed dostępem osób nie upoważnionych, wykrywa

przypadki zagrożenia zbiorów lub pomieszczeń ośrodka. Układy techniczne można podzielić na trzy grupy:

a) identyfikujące (głos ludzki, linie papilarne, za pomocą karty z odcinkiem TM),

b) zabezpieczające,

c) alarmujące.

Ad a. W różnych krajach prowadzone są badania dotyczące możliwości komunikowania się człowieka z maszyną cyfrową. Stwierdzono, że te same słowa wypowiedziane przez różnych ludzi, a przedstawione za pomocą sonogramu, wyraźnie różnią się między sobą. Na sonogramie jest przedstawiony graficzny obraz słowa wymawianego przez użytkownika i w postaci binarnej zapisany w pamięci komputera. Technika ta umożliwia zastosowanie słów-haseł znanych użytkownikom, które przed przystąpieniem do pracy są przez nich wypowiadane. Komputer porównuje sonogram z hasłem osoby zgłaszającej się i w razie zgodności podsystem ochrony dopuszcza osobę do pracy. W przeciwnym razie zgłaszający się nie ma dostępu do systemu.

Zasada identyfikacji polega na porównaniu odcisków palców z zapamiętanymi przez komputer wzorcami odcisków. Pracą taką metodą kieruje podsystem ochrony, który może być tak zaprojektowany, by w razie wykrycia próby korzystania z systemu przez osobę nie upoważnioną, odłączył dane urządzenie, a fakt ten zarejestrował lub natychmiast zaalarmował obsługę komputera. Urządzenie to może zapewnić największy stopień bezpieczeństwa zbiorów. Skuteczność takiej metody teoretycznie wynosi około 99,97%. Z powodu dużych kosztów urządzenie to może być stosowane w wyjątkowych przypadkach i w systemach stanowiących tajemnicę państwową [25]. Jak podaje Sokołowski [23, s. 107] model urządzenia identyfikującego można wykonać w Polsce. Podstawowy element urządzenia - głowica magnetyczna kartowa typu GKM-3 jest produkowana przez Zakład Urządzeń Informatyki

MERA-MAT. Pozostałe elementy urządzenia mogą być wykonane w warunkach laboratoryjnych. Metoda identyfikacji polega na wykorzystaniu karty z tworzywa sztucznego, do której jest przytwierdzony pasek TM z zapisem identyfikującym użytkownika. Urządzenie końcowe (terminal) ma układ odczytujący informacje z paska TM oraz możliwość zapisania informacji na nim. Do zalet reprezentowanej metody należą: stosunkowo mały koszt układu czytająco-piszącego i prostota czynności wykonywanych przez użytkownika w czasie identyfikacji.

Ad b. Najczęściej stosuje się układy zabezpieczające w postaci urządzeń technicznych, służących do ochrony zbiorów informacji. Do nich można zaliczyć zamki przy urządzeniach końcowych, żetony do uruchomienia terminali, zamki kodowo-magnetyczne przy wejściu do pamięci komputera, ochronę techniczną pamięci magnetycznych i specjalne szafy do przechowywania zbiorów. Zamki przy urządzeniach końcowych są fizycznym zabezpieczeniem dostępu do komputera. Użytkownik, po przekręceniu klucza w zamku, wprowadza przez urządzenie końcowe określony identyfikator i rozpoczyna pracę. Kolejnym dogodnym sposobem jest uruchomienie urządzenia po wrzuceniu określonego żetonu. Metoda ta może być stosowana w lecznictwie, uczelniach itp., czyli tam, gdzie jest wskazany dostęp do maszyny za pomocą żetonu.

Ad c. Jednym z obecnie stosowanych układów alarmujących jest urządzenie sygnalizacji przeciwpożarowej. Do układów alarmujących można zaliczyć m.in. fotokomórki, układy reagujące na temperaturę i układy reagujące na otwieranie drzwi. Układy alarmujące chronią przed dostępem osób nie upoważnionych, przed pożarem i przed wpływem fal elektromagnetycznych.

3.3. Metody programowe

Spośród wszystkich metod ochrony zbiorów metody programowe zasługują na szczególną uwagę. Główne ich zalety to

- możliwość zaprogramowania i wdrożenia własnymi siłami w poszczególnych ośrodkach obliczeniowych,
- różne możliwości stosowania szyfrów, kodów, identyfikatorów, systemów kontroli itp.,
- niekomplikowanie procesu przetwarzania danych,
- duże prawdopodobieństwo ochrony,
- realizacja ich przez sam komputer.

Programowane metody ochrony zbiorów są na pewnych etapach procesu przetwarzania jedynymi metodami, które mogą skutecznie chronić zbiory informacji. Polegają one na opracowaniu i zastosowaniu programów, podprogramów lub segmentów oraz odpowiednim etykietowaniu TM, aby zabezpieczyć zbiory informacji przed osobami nie upoważnionymi.

3.4. Kompleksowy system ochrony

Przedstawione na wstępie niniejszej pracy wymagania dotyczące systemu ochrony zbiorów polegają na znalezieniu takiego systemu, który by gwarantował dużą skuteczność systemu ochrony, a jednocześnie nie utrudniał pracy ośrodkom obliczeniowym. Dotychczasowe systemy ochrony danych nie spełniają tych wymagań. Wpłynęło to decydująco na brak ochrony zbiorów w większości ośrodków obliczeniowych. Aby udowodnić te stwierdzenia, przytoczono dwa zestawy wymagań stawianych systemowi ochrony zbiorów.

Wasserman w pracy [31] podaje w formie zdań pytających 12 warunków, które należy spełnić, aby system był zabezpieczony.

1. Czy istnieje ogólna koncepcja ochrony?

2. Czy istnieją metody ochrony maszyn i wyników?

3. Czy prowadzi się kontrolę wejścia, wyjścia i błędów?

4. Czy jest komórka kontroli jakości?

5. Czy w programach dokonuje się systematycznie zmiany?

6. Czy systemy są wystarczająco sprawdzone?

7. Czy przewidziano dostateczną kontrolę konwersji?

8. Czy istnieje właściwy podział odpowiedzialności?

9. Czy ośrodek obliczeniowy ma właściwe zabezpieczenie?

10. Czy są procedury awaryjne?

11. Czy ośrodek jest odpowiednio ubezpieczony?

12. Czy eksploatowane systemy są regulamie rewidowane?

Jeżeli na wszystkie postawione pytania - stwierdza Wasserman - otrzymamy odpowiedź twierdzącą, to eksploatowany system jest prawidłowo zabezpieczony.

Drugi przykład, to kompleksowy system ochrony zbiorów powszechnie aprobowany, który jednocześnie jest niemożliwy do zrealizowania w praktyce. Wymagania tegoż systemu Miszczak [9] ujął następująco.

A. Problemy ogólne

1. Ochrona powinna zabezpieczać przed następującymi rodzajami naruszeń:

a) przypadkowymi:

- błędem użytkownika,
- błędem systemu;

b) infiltracją pasywną:

- podsłuchem linii komunikacyjnej,
- wykorzystaniem promieniowania elektromagnetycznego;

c) infiltracją aktywną:

- nie kontrolowanym dostępem do zbiorów,
- podawaniem się za upoważnionego użytkownika,

- fizycznym zagarnięciem zbiorów,

- eksploatacją nielegalną systemu.

2. Pierwszym krokiem na drodze stworzenia systemu ochrony jest analiza systemu pod kątem jego odporności na naruszenia. Dopiero następnie można przystąpić do projektowania zabezpieczeń. W trakcie analizy należy postępować następująco:

a) opisać otoczenie, w którym system działa lub ma działać,

b) zidentyfikować cechy, które zabezpieczenie powinno koniecznie uwzględnić,

c) sprawdzić, czy w istniejącym systemie występują już pewne cechy zabezpieczenia,

d) ustalić, czy występujące cechy spełniają wymagania punktu b).

3. System ochrony powinien zapewnić identyfikację następujących obiektów:

a) użytkowników indywidualnych,

b) terminali,

c) programów indywidualnych,

d) danych - w dół do poziomu elementu lub rekordu.

4. Rejestracja dostępu do danych powinna funkcjonować za pomocą jednego (lub wszystkich) z poniższych sposobów:

a) klasyfikacji hierarchicznej danych (tajne specjalnego znaczenia, tajne, poufne),

b) podziału danych na kategorie lub przedziały,

c) sformułowania ograniczeń dostępu do poszczególnych obiektów,

d) restrykcji zależnej od zawartości danych,

e) ograniczeń zależnych od kontekstu danych,

f) ograniczeń na podstawie procedur wprowadzonych przez użytkownika.

5. Użytkownikom lub programom powinny być nałożone ograniczenia na pewne lub wszystkie z następujących przywilejów dostępu:

a) czytanie,

b) pisanie:

- modyfikacja,
- dopisywanie,
- wprowadzanie,

c) usuwanie lub zerowanie.

6. Podstawowymi zadaniami systemu ochrony są identyfikacja, kontrola, wykrywanie i rejestrowanie wszystkich zmian danych.

B. Niezbędne pociągnięcia administracyjne i organizacyjne

1. Administracyjne:

a) ograniczyć dostęp do komputera,

b) sprawdzić niezgodność modyfikacji krytycznego oprogramowania systemu,

c) testować i weryfikować zmiany oprogramowania systemowego i procedur zabezpieczających,

d) doskonalić kontrolę administracyjną,

e) ograniczyć przywileje (swobodę) personelu w możliwym do przeprowadzenia stopniu,

f) kontrolować wszystkie wejścia i wyjścia, klasyfikować dane pod względem ich sensu i wartości,

g) analizować wprowadzone dane, rejestrować operacje, mierzyć czas pracy i porównywać z planem,

h) prowadzić podręczną rejestrację dostępu do systemu.

2. Organizacyjne:

a) prowadzić konsekwentną politykę ochrony w stosunku do wszystkich,

b) ustanowić pełnoetatowe stanowisko kierownika ochrony,

c) przy każdym terminalu ustalić osobę odpowiedzialną osobiście za jego ochronę,

d) zabezpieczyć biblioteki taśm i dysków,

e) zdjąć odpowiedzialność i władzę z ludzi sprzeciwiających się ustaleniom mającym na celu wzmocnienie ochrony,

f) wydzielić kluczowy personel na podstawie zaufania i kompetencji,

g) sprawdzić referencje (opinie) personelu.

3. Proceduralne:

a) ustalić (na piśmie procedury postępowania w następujących przypadkach:

- startu systemu,
- kończenia pracy systemu,
- restatorów,
- kontroli taśm, dysków, kart, tabulogramów,
- identyfikacji użytkowników systemu,
- kontroli dostępu do urządzeń centralnych i terminali,
- zmiany oprogramowania,
- zmiany parametrów systemu,
- konserwacji,
- testowania systemu;

b) ustalić i wprowadzić do praktyki procedury postępowania w przypadkach losowych,

c) odpowiednio przechowywać taśmy i dyski,

d) okresowo konserwować dokumentację,

e) przestrzegać okresów przechowywania dokumentów,

C. Fizyczne i hardware'owe środki ochrony

1. Zabezpieczenie fizyczne:

a) kontrola wstępu (strażnicy, żetony),

b) kontrola dostępu do terminali,

c) zabezpieczenie instalacji przed pożarem,

d) zapewnienie niezawodności źródeł energii elektrycznej i klimatyzacji, redundancja sprzętu,

e) ochrona dokumentacji w zabezpieczonym miejscu,

f) kopie dokumentacji i zbiorów przechowywać poza miejscem przechowywania oryginałów,

g) kontrola dostępu personelu nadzorującego do zastrzeżonych obszarów systemu,

h) minimum dwie osoby powinny być jednocześnie dopuszczone do pracy przy przetwarzaniu danych,

i) objęcie kontrolą i wydanie specjalnych przepustek dla gości, dostawców i programistów.

2. Zabezpieczenie hardware'owe:

a) ochrona pamięci rdzeniowej, rejestry kontroli granic pamięci,

b) na każdy kod operacji powinna być znana odpowiedź,

c) ochrona przed czytaniem i pisaniem,

d) hardware'owa identyfikacja terminali i urządzeń peryferyjnych,

e) sygnalizacja błędów, uszkodzeń i zakłóceń,

f) stosowanie urządzeń szyfrujących i deszyfrujących.

D. Programowe i software'owe środki ochrony

1. Kontrola dostępu:

a) identyfikacja ludzi i terminali przez system:

- hasła i numery identyfikacyjne,
- karty, żetony, przedmioty z magnetycznie zapisaną treścią,
- identyfikacja głosu lub odcisków palców;

b) hasła rozpoznawcze lub procedury wyzwania i odpowiedzi:

- generowanie haseł przypadkowo o dostatecznej długości,
- okresowa zmiana haseł,
- specjalna ochrona przechowywania haseł;

c) system kontroli dostępu powinien być dostatecznie elastyczny.

2. Ochrona danych:

a) jednostki danych powinny być etykietowane,

b) znaczące dane powinny być oddzielone od informacji pozostałych,

c) dostęp do danych nie powinien być bezpośredni, lecz przez katalog właściciela,

d) zastrzeżone pola danych mogą być kasowane na wyjściu,

e) dane i programy mogą być przechowywane w postaci zaszyfrowanej,

f) periodyczna konserwacja systemu, danych i programu,

g) transfery danych powinny być kontrolowane,

h) dane mogą być wartościowane,

i) ładowanie programów i danych powinno być zabezpieczone przez sumy kontrolne,

j) zmiany dokonywane w programie powinny być kontrolowane,

k) modyfikacja danych powinna być odpowiednio zabeupieczona.

3. Kontrola systemowa:

a) wszystkie dostępy i żądania operacji powinny być sygnalizowane,

b) muszą być kontrolowane wszystkie operacje związane z alokacją pamięci, przerwami i trybem operacji,

c) programy użytkowników powinny być kodowane,

d) adresy przesyłane między użytkownikami i systemem powinny być adresami logicznymi; rzeczywiste adresy nie mogą być akceptowane,

e) powinien istnieć mechanizm automatycznego determinowania prawa dostępu do nowo utworzonych danych i programów,

f) przed każdą pracą pamięć i urządzenia peryferyjne powinny być oczyszczone z pozostałości,

g) w razie uzyskania nieprzewidzianych wyników powinno się przerwać operacje,

h) restarty w tych przypadkach powinny nastąpić po ponownym załadowaniu egzekutora.

E. Protekcja systemu ochrony

1. Nie rozpowszechniać informacji na temat braków systemu ochrony.

2. Ustalić ograniczenia na próby powtórnych zgłoszeń dostępu.

3. System powinien wnikać w status użytkownika.

4. Zabezpieczyć przed składowaniem lub wprowadzeniem informacji.

5. Zawartość zbiorów ochrony powinna być zabezpieczona.

6. Programowanie w języku poziomu assemblera powinno być ograniczone lub zabronione.

7. Nie powinno się zezwolić na żadną zmianę tabel ochrony. Zmiany należy dokonywać według specjalnie ustalonej procedury.

F. Kontrola

1. Historia pracy systemu:

a) wszystkie ruchy powinny być rejestrowane,

b) powinna być możliwość rekonstrukcji zapisu historii,

c) konieczny jest program analizy i oceny zapisu historii.

2. Sygnalizacja i rejestracja następujących czynności:

a) wszelkich prac,

b) żądania danych,

c) uzyskania dostępu do zbiorów,

d) dysponowania danymi

oraz należy uwzględnić:

e) dostępy nieautoryzowane,

f) każde specjalne wykorzystanie programu,

g) wszelkie zmiany deskryptorów,

h) zmiany konfiguracji,

i) zmiany w tablicach ochrony i programie zarządzającym,

j) restarty i błędy maszyny,

k) usiłowanie naruszenia pamięci,

l) błędy parzystości.

Po zapoznaniu się z wymaganiami kompleksowego systemu ochrony jasne staje się, że - jak wykazała ankieta opracowana przez Sokołowskiego [25] na temat ochrony zbiorów - oprócz metod organizacyjnych, czyli administracyjnych, inne metody nie są stosowane. Nie biorę pod uwagę zabezpieczenia przez systemy operacyjne, które w rzeczywistości są zwykłą formalnością. Tak liczne wymagania systemu kompleksowego stają się uciążliwe i powodują zmniejszenie skuteczności, gdyż

a) prowadzą do fizycznej niemożności praktycznego i jednoczesnego stosowania wszystkich wymagań,

b) ich mnogość nie tylko, że utrudnia pracę, lecz wprost paraliżuje cały tok pracy ośrodka,

c) kompleksowy system ochrony jest oparty na uczciwości ludzkiej, gdyż decydującym czynnikiem tegoż systemu jest człowiek.

Nic więc dziwnego, że zarówno poszczególne metody, jak i kompleksowy system ochrony nie uzyskały dotychczas prawa obywatelstwa. Nikt nie chce być samobójcą, nikt nie chce i nie dopuści do sparaliżowania pracy ośrodka obliczeniowego przez wprowadzenie (zastosowanie) systemu ochrony. Z tego wynika ograniczenie się do zarządzeń administracyjnych w zakresie ochrony zbiorów.

3.5. Ochrona informacji w państwach zachodnich*

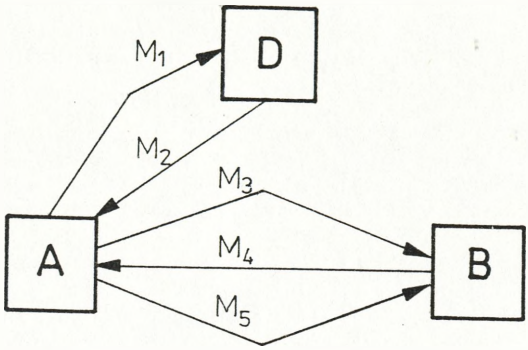
3.5.1. Metoda koncencjonalnych systemów kryptograficznych

Zakładamy, że informacja została przekazana od użytkownika A do użytkownika B. Obaj mają tajmy klucz K_A i K_B. Nadrzędna instancja pośredniczy w przekazywaniu informacji. Głównym elementem tej metody jest identyfikacja obu osób. Identyfikuje je instancja nadrzędna, która posiada odpowiednie dane o dysponentach obu kluczy. Instancję tę nazwijmy dysponentem D. Identyfikację przeprowadza się następująco. Nadawca A przesyła meldunek M_1 do dysponenta D. Podaje swoje nazwisko będące jego identyfikatorem, nazwisko odbiorcy B oraz dodatkowy identyfikator A_1, który ma jednorazową ważność. W odpowiedzi dysponent D ustala - na podstawie posiadanych informacji - dane dotyczące K_A i K_B, które przesyła do A meldunkiem M_2 oraz oblicza tzw. klucz seryjny K_S. Informacja została zaszyfrowana za pomocą klucza K_A, dlatego tylko nadawca A może ją rozszyfrować i być przekonany, że pochodzi on od właściwego nadawcy. Dane o odbiorcy B nadawca A przesyła w meldunku M_3 do B wraz z informacją o kluczu seryjnym K_S oraz identyfikatorze B_1. Wiadomość tę może rozszyfrować jedynie odbiorca B, będący posiadaczem klucza K_B. W ten sposób odbiorca B staje się również posiadaczem klucza seryjnego K_S, wraz z identyfikatorem B_1. Może się rozpocząć bezpieczne przesyłanie informacji w meldunkach M_4 i M_5 pomiędzy A i B. Cbieg informacji według powyższej metody przedstawiono na rys. 3.

Takie poglądy na temat bezpiecznego przesyłania informacji wypowiedzieli w swoich pracach Biegert [1], Ryska i Herda [14]. Autor niniejszej publikacji ma na ten temat odmienne zdanie.

---

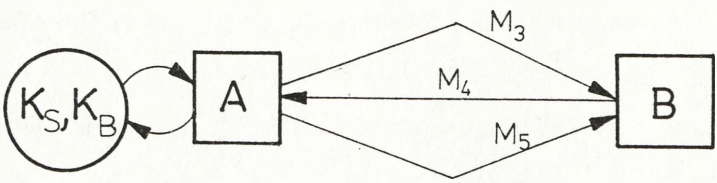
*Niniejszy punkt opracowano na podstawie pozycji [14].



Rys. 3. Metoda inicjacji komunikacji interakcyjnej

3.5.2. Metoda przesyłania informacji w przypadku przechowywania identyfikatora u nadawcy

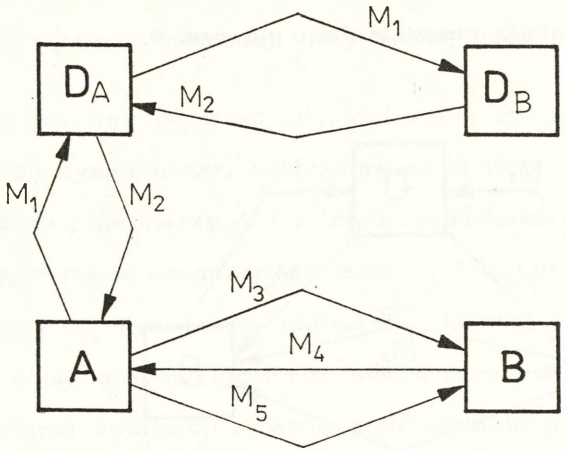
Jeżeli nadawca A regularnie przesyła meldunki do odbiorcy B, to w pamięci komputera przechowuje dane dotyczące kluczy K_S i K_B. Wówczas meldunki M_1 i M_2 stają się zbyteczne, natomiast jest konieczna wymiana informacji o identyfikatorach A_1 i B_1 za pomocą meldunków M_3, M_4 i M_3 (rys. 4).



Rys. 4. Metoda przesyłania informacji w przypadku przechowywania informacji przez nadawcę

3.5.3. Metoda przesyłania informacji w razie istnienia dwóch dysponentów klucza

Metodę tę stosuje się wówczas, gdy zarówno nadawca A, jak i odbiorca B nie mają tego samego dysponenta klucza, tzn. A i B należą do różnych sieci. Wówczas należy wstępnie wymienić informacje pomiędzy dysponentami kluczy DK_A i DK_B. Aby ochronić wymianę informacji pomiędzy dysponentami kluczy, zastosowano klucz specjalny DK_S. Dysponent D_A zna tylko tajmy klucz DK_A, a dysponent D_B - tylko tajny klucz DK_B. Dlatego przed przesyłaniem informacji dysponent D_A jest zmuszony zwrócić się do dysponenta D_B o przekazanie klucza DK_B. Przebieg wymiany informacji przedstawiono na rys. 5.



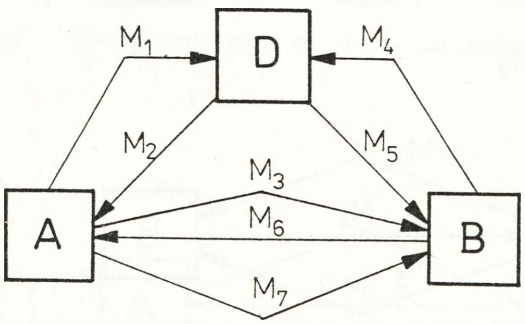
Rys. 5. Metoda wymiany informacji z dwoma dysponentami klucza

3.5.4. Metoda wymiany informacji za pomocą jawnego klucza

Zakładamy, że nadawca A i odbiorca B znają jawny klucz KO (klucz otwarty) i obaj mają jednego dysponenta. W pierwszym meldunku M_1 nadawca A przekazuje żądanie przesłania przez dysponenta D klucza otwartego KO_B. Żądane informacje o kluczu KO_B otrzymuje w meldunku M_2,

przy czym meldunek M_2 zostaje zaszyfrowany prywatnym kluczem KP_3. Dzięki temu użytkownik A został upewniony, że otrzymana informacja w postaci M_2 pochodzi od dysponenta, gdyż tylko on jest właścicielem prywatnego klucza SP_S. Posiadając otwarty klucz KO_B, nadawca A przesyła do B meldunek M_3 zawierający jego nazwisko oraz identyfikator o jednorazowej ważności. Informacja ta może być rozszyfrowana tylko przez odbiorcę B. Podobnie postępuje odbiorca B i otrzymuje od dysponenta D w meldunkach M_4 i M_5 konieczne dane dotyczące klucza KO_A. Wymiana informacji następuje w meldunkach M_6 i M_7.

W razie zastosowania systemów kryptograficznych z otwartym kluczem trzeba informacje wymienić aż siedem razy. Natomiast ta sama procedura w systemach konwencjonalnych wymaga tylko pięciokrotnej wymiany. Wymianę informacji tą metodą przedstawiono na rys. 6

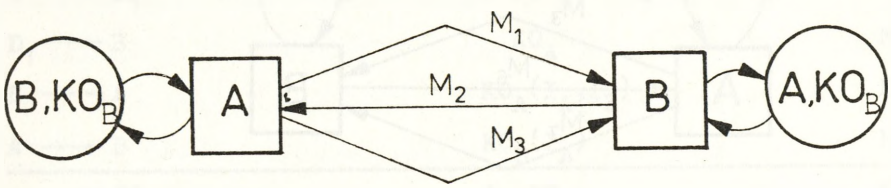


Rys. 6. Metoda inicjowania wymiany informacji w systemach informatycznych z otwartym kluczem

3.5.5. Uproszczona metoda wymiany informacji

Metoda ta polega na tworzeniu w pamięci komputera całej listy kluczy. W liście tej - obok kluczy - są przechowywane nazwiska wszystkich użyt-

kowników sieci. W tym przypadku zarówno nadawcy, jak i odbiorcy korzystają bezpośrednio z listy kluczy, dzięki czemu liczba koniecznych wymienianych informacji maleje z siedmiu do zaledwie trzech (rys. 7).

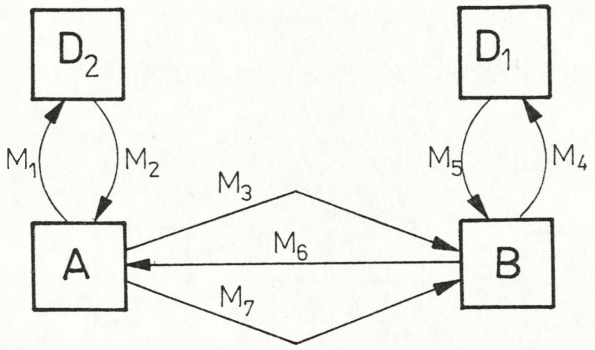


Rys. 7. Uproszczona wymiana informacji

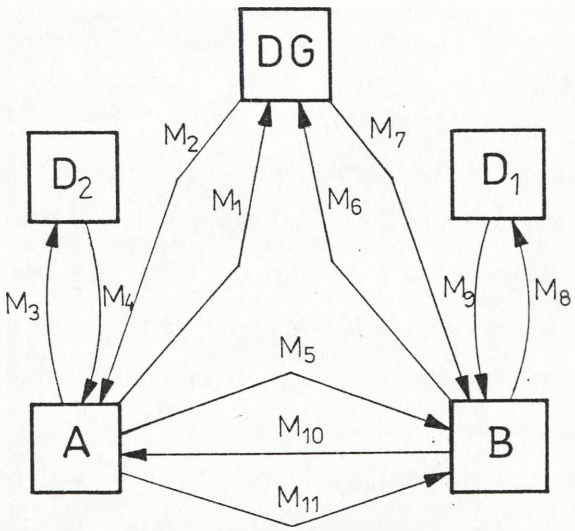
3.5.6. Metoda wymiany informacji przy różnej liczbie dysponentów kluczy

Metoda ta ma trzy odmiany: gdy jest jeden dysponent klucza oraz dwóch i trzech dysponentów. Sformułowano ją według następujących założeń. Jeżeli obaj partnerzy A i B są uczestnikami różnych sieci i mają różnych dysponentów oznaczonych jako D_1 i D_2 oraz partner A zna otwarty klucz KO_B dysponenta klucza D_1, to obaj partnerzy mogą nawiązać między sobą komunikację i rozpocząć przesyłanie informacji. Możliwość przesyłania informacji i nawiązania kontaktu pokazano na rys. 8.

Jeżeli jednak A i B nie znają otwartego klucza należącego do A i B, to musi istnieć nadrzędna instancja, od której obaj partnerzy otrzymują te dane. Wymianę informacji przy tego typu zależnościach przedstawiono na rys. 9.



Rys. 8. Metoda kryptograficzna z dwoma dysponentami klucza



Rys. 9. Metoda kryptograficzna z trzema dysponentami klucza

Przebiegi przesłania informacji (rys. 8 i 9) można zapisać następująco:

	Informacja	Meldunek
$A \longrightarrow D_2$	A, B	M_1
$D_2 \longrightarrow A$	KO_B	M_2
$A \longrightarrow B$	$KO_B(I_A,A)$	M_3
$B \longrightarrow D_1$	B, A	M_4
$D_1 \longrightarrow B$	KO_A	M_5
$B \longrightarrow A$	$KO_A(I_A,I_B)$	M_6
$A \longrightarrow B$	$KO_B(I_A)$	M_7
$A \longrightarrow DG$	A, KO_B	M_1
$DG \longrightarrow A$	KO_B,K_B	M_2
$A \longrightarrow D_2$	A, B	M_3
$D_2 \longrightarrow A$	KO_B, B	M_4
$A \longrightarrow B$	$KO_B(I_A,I_B)$	M_5
$B \longrightarrow DG$	B, KO_A	M_6
$DG \longrightarrow B$	KO_A, K_A	M_7
$B \longrightarrow D_1$	B, A	M_8
$D_1 \longrightarrow B$	KO_A, A	M_9
$B \longrightarrow A$	$KO_A(I_A,I_B)$	M_{10}
$A \longrightarrow B$	$KO_B(I_A)$	M_{11}

Legenda:

DG - dysponent główny kluczy,

D_1,D_2 - dysponenci kluczy,

A,B - użytkownicy sieci komputerowych,

M - przesłane meldunki,

KO - klucz jawny - otwarty,

I_A,I_B - identyfikatory użytkowników sieci,

K_A,K_B - klucze użytkowników sieci.

Przedstawione zasady przesyłania informacji za pomocą metod kryptograficznych są powszechnie stosowane w Stanach Zjednoczonych. Omówione metody (rys. 3-9) stanowią podstawę kształcenia użytkowników sieci komputerowych w stosowaniu metod kryptograficznych podczas przesyłania ważnych informacji. Są to jednak metody przestarzałe i niezmienne od czasów Cezara, od czasu zastosowania jego szyfru. W metodach tych główny element szyfru stanowi KLUCZ. Obowiązują zasady przechowywania i przekazywania klucza przed rozpoczęciem przesyłania informacji. W tym celu utworzono specjalne instytucje w postaci biur dysponentów kluczy. Niewiele zmieniło się więc od najdawniejszych czasów. Jedynie wprowadzono komputer w miejsce dotychczasowych liczydeł.

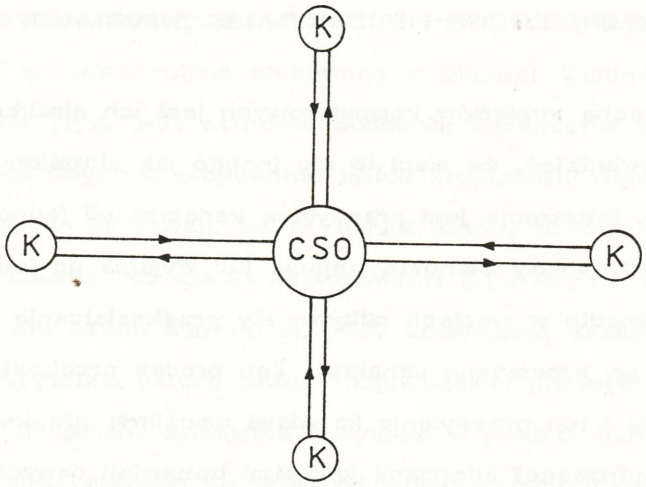
4. SIECI KOMPUTEROWE I PRZESYŁANIE INFORMACJI

Podstawową cechą systemów komputerowych jest ich struktura sieciowa. Ogólnie można powiedzieć, że sieci to nic innego jak określony układ węzłów i kanałów. Informacja jest przesyłana kanałami od jednego węzła do drugiego, dlatego węzły stanowią wejścia lub wyjścia do jednego i do wielu kanałów. Ponadto w węzłach odbywa się przekształcanie informacji w sygnały, które są przesyłane kanałami. Ten proces przekształcania informacji w sygnały i ich przesyłanie kanałami umożliwia przekazywanie odpowiednio zaszyfrowanej informacji kanałami transmisji danych. Zaszyfrowana informacja może być przesyłana kanałami łączącymi węzły, które w zależności od realizowanej funkcji mogą być węzłami pośrednimi lub docelowymi. Zarówno węzeł docelowy, jak i węzeł źródłowy (początkowy), w którym informacja jest szyfrowana, są z zasady wyposażone w systemy obliczeniowe. Natomiast węzeł pośredni może (lecz nie musi) posiadać odpowiedni system obliczeniowy. Zastosowane w węzłach systemy obliczeniowe są nazywane najczęściej komputerami komunikacyjnymi.

4.1. Struktura sieciowa i rodzaje sieci

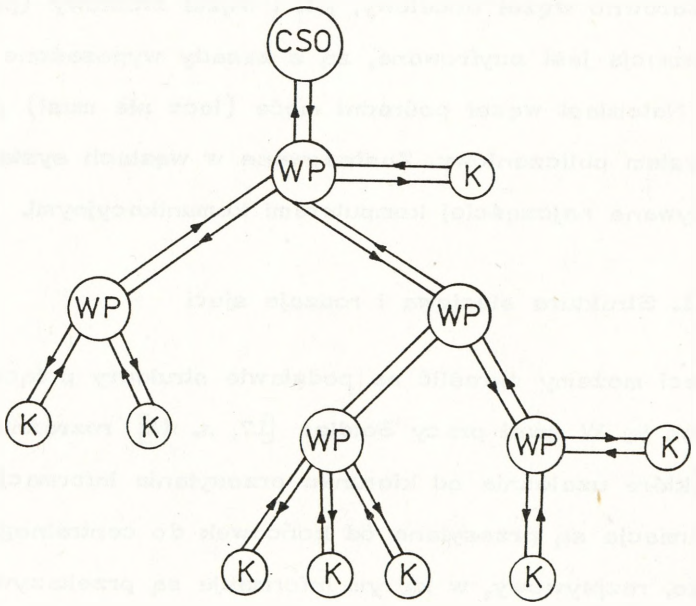
Rodzaj sieci możemy określić na podstawie struktury połączeń kanałów tworzących ją. W swej pracy Seidler [17, s. 41] rozróżnia dwa systemy sieci (które uzależnia od kierunku przesyłania informacji): spływowy, w którym informacje są przesyłane od końcówek do centralnego systemu obliczeniowego, rozpływowy, w którym informacje są przekazywane od centralnego systemu obliczeniowego do licznych końcówek. Może istnieć system spływowo-rozpływowy, który łączy obie funkcje systemów. System spływowo-rozpływowy może mieć układ sieci gwiazdzistej lub drzewiastej (rys. 10).

a)



CSO - centralny system obliczeniowy K - końcówka

b)



WP - węzeł pośredni

Rys. 10. Podstawowe rodzaje sieci

Źródło: [17, s. 42] ; rysunek zmodyfikowany przez autora (Z.T.)

Sieć gwiazdzista jest stosowana rzadziej, ponieważ wymaga dużej liczby kanałów; każdą końcówkę należy oddzielnie połączyć. Tę niedogodność usuwa zastosowanie sieci drzewiastej. Sieć ta jednak wymaga odpowiedniej liczby węzłów pośrednich, do których możemy dołączyć pewną liczbę końcówek.

Innym rodzajem sieci jest sieć pętlowa, którą tworzymy przez nałożenie na siebie sieci gwiaździstej i systemu spływowo-rozpływowego. Sieć pętlową można rozszerzyć przez utworzenie sieci wielopętlowej i pętlowo-hierarchicznej.

4.2. Sieci łączności dla systemów komputerowych

Komputerową sieć teleinformatyczną można określić jako zbiór przestrzennie rozproszonych wielodostępnych systemów komputerowych. Składa się ona z pewnej liczby komputerów głównych połączonych liniami komunikacyjnymi, umożliwiającymi przesyłanie informacji. Jest to więc zbiór wielodostępnych systemów komputerowych, węzłów i kanałów międzywęzłowych.

Istotnym elementem sieci komputerowej jest pojęcie węzła sieci. Skład węzła może być różny. W jego wyposażeniu mogą się znaleźć komputery, multipleksery, modemy itp. Do zadań węzła należy:

1. Zbieranie sygnałów przesyłanych z innych węzłów.

2. Podział zbieranej informacji w postaci sygnałów na dwie grupy: pierwsza zawiera informacje w postaci strumieni o standardowej szybkości 0,6; 2,4; 9,6 oraz 48 kbitów/s. Druga obejmuje informacje przesyłane w postaci pakietów.

3. Kierowanie ruchem otrzymanych sygnałów ciągłych (standardowych), jak i pakietów przez przesyłanie ich do innych węzłów lub końcówek użytkowników.

4. Sterowanie wymianą danych w sieci za pomocą protokołu komunikacyjnego.

Aby w pełni zobrazować pracę węzła, należy wyjaśnić pojęcie "pakietu" oraz "protokołu komunikacyjnego". Wierzbicki podaje następującą definicję pakietu: "Pakiet jest to informacja o specjalnym znormalizowanym formacie, w którym wyodrębnić można dane użytkownika oraz informacje sterujące i adresowane zawarte w tzw. kopercie danych (ramce)" [33, s. 323]. Budowę pakietu pokazano na rys. 11.

Rys. 11. Struktura pakietu danych [33, s. 324] zmodyfikowany przez autora niniejszej pracy

Protokół komunikacyjny jest to zbiór reguł współdziałania poszczególnych elementów sieci, dostępu do zbiorów i sterowania wymianą danych w sieci. Protokóły, w zależności od realizowanych funkcji, można podzielić na liniowe i wirtualne. Protokóły liniowe służą w zasadzie do fizycznych połączeń sieci i mają częstokroć strukturę hierarchiczną. Dzięki tej strukturze protokoły najniższego poziomu stanowią procedury przekazywania danych - terminali do sieci. Protokóły drugiego poziomu przekazują dane

między węzłami. Natomiast protokóły trzeciego poziomu przekazują informacje między komputerami węzłowymi oraz centralnymi.

Na przestrzeni ostatnich 15 lat powstały, szczególnie na Zachodzie, liczne sieci komputerowe i satelitarne. Właśnie sztuczne satelity umożliwiają tworzenie kanałów bardzo dalekiego zasięgu. W obecnych systemach satelitarnych jest stosowany często system z podziałem czasu, np. system INTELSAT-IV. Jest to system umożliwiający łączność z trzema stacjami naziemnymi, z których każda może być połączona z 24 końcówkami telefonicznymi [17, s. 59-61]. Natomiast istniejące na Zachodzie naziemne sieci komputerowe są bardzo rozpowszechnione i często stosowane. Jak podaje Seidler [17], istnieją tam następujące rodzaje sieci:

1. Sieć ARPA zapewniająca łączność między komputerami na terenie Stanów Zjednoczonych i będąca pod auspicjami Agencji Rozwojowej Prac Badawczych Ministerstwa Obrony. Pakiety są przesyłane w sieci przez węzły pomocnicze do węzła docelowego jako niezależne jednostki. Kolejny z węzłów po otrzymaniu pakietu analizuje trasę jego przesyłania do węzła docelowego i wybiera trasę najkorzystniejszą czasowo. Trasa pakietu nie jest z góry ustalona, lecz powstaje przez dołączenie kolejnych segmentów w każdym węźle. Sieć ARPA jest również uruchomiona w Wielkiej Brytanii.

2. Sieć ALOHA powstała z konieczności rozszerzenia sieci ARPA poza obszar północnoamerykański. Do systemu ARPA dołączono kanały radiowe i satelitarne. Uruchomiono go na Hawajach. Specyfika tego systemu polega na tym, że do wspólnego kanału radiowego mogą mieć dostęp jednocześnie wszyscy użytkownicy.

3. Sieć DDS jest siecią należącą do towarzystwa ATT (American Telegraph and Telephon Company) i mającą strukturę hierarchiczną, trójpoziomową. Sygnały kierunkowe są przesyłane od poziomu najniższego

do poziomu najwyższego, a następnie do centralnego. W trakcie przesyłania sygnału następuje jego zwielokrotnienie częstotliwościowe. Dzięki zastosowaniu systemu zwielokrotnienia częstotliwościowego sygnału uzyskano dalekie zasięgi w przesyłaniu informacji. Jednocześnie sieć ma dużą przepustowość, gdyż kanały dalekiego zasięgu mają większą przepustowość niż kanały bliskiego zasięgu. Urządzenie centralne trzeciego rzędu jest połączone kanałami cyfrowymi z urządzeniami pracującymi w kanałach przewodowych. Do sieci DDS jest podobna sieć DATRAN, która ma objąć w przyszłości całe Stany Zjednoczone.

4. Sieci specjalistyczne w USA. Tworzone są różnego rodzaju sieci specjalistyczne, co jest podyktowane następującymi faktami:

- dużą liczbą użytkowników sieci, co bardzo obniża koszt korzystania z sieci przez jednego użytkownika,

- istniejące sieci są już przestarzałe, niejednokrotnie o małej niezawodności i dużych opóźnieniach.

Czynniki te wpłynęły na powstanie licznych sieci specjalistycznych, realizujących określone funkcje. Do nich należą:

a) sieć TYMENT łącząca cztery ośrodki obliczeniowe, posiadające łącznie 26 komputerów; cała sieć składa się z 80 węzłów komunikacyjnych i ma możliwość sprzężenia z innymi sieciami;

b) sieć INFONENT łącząca zaledwie 6 komputerów rozmieszczonych w trzech ośrodkach obliczeniowych; sieć składa się z 25 węzłów, których głównym członem jest jeden komputer komunikacyjny;

c) sieć GENERAL ELECTRIC jest siecią składającą się z kilkudziesięciu komputerów oraz 50 węzłów rozlokowanych w 30 różnych miastach Stanów Zjednoczonych; głównym członem każdego węzła tranzytowego jest komputer Honeywell-416; sieć ma strukturę drzewiastą,

umożliwiającą kierowanie pakietem w sposób uproszczony; ponadto pakiety są mniejsze i nie wymagają "przepakowywania" w węzłach tranzytowych;

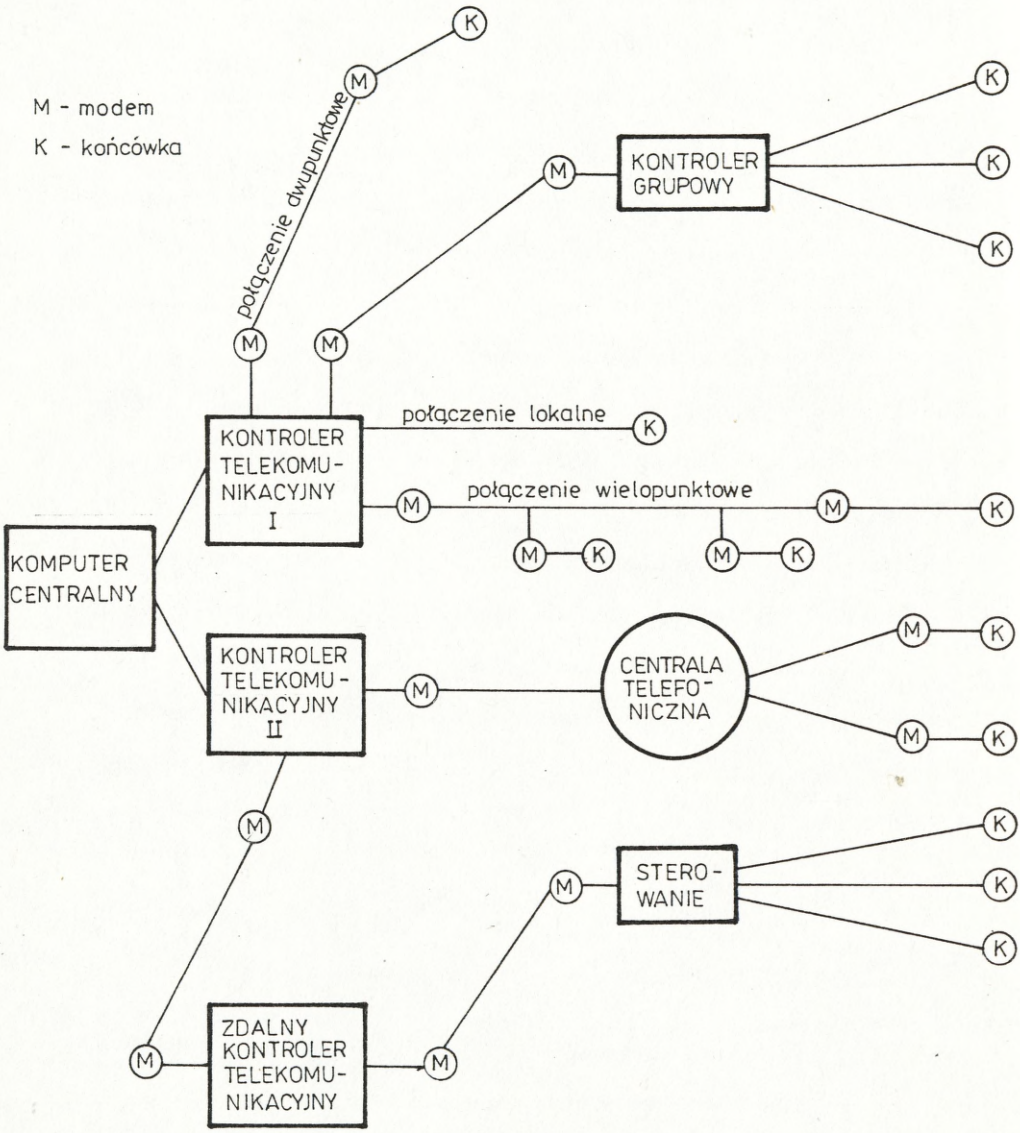
d) sieć NASDAQ jest siecią wyspecjalizowaną w automatyzacji operacji związanych ze sprzedażą i zakupem akcji.

5. Sieci komputerowe w USA mają na celu sprzężenie rozmieszczonych w różnych miejscach komputerów w jeden wielokomputerowy system obliczeniowy. Do tego typu sieci należą: CYBERNET, MERIT, OCTOPUS oraz IBM sprzęgające siedem jednakowych komputerów IBM-360/67.

Niezależnie od wymienionych sieci stosowanych w Stanach Zjednoczonych na podkreślenie zasługują również sieci stosowane w niektórych krajach europejskich. We Francji uruchomiono sieć CADUCE o strukturze gwiaździstej, posiadającej 12 węzłów. Podobna sieć została uruchomiona w Holandii. Szwajcaria posiada sieć ATECO również o strukturze gwiaździstej. Ciekawym rozwiązaniem tej sieci są połączenia kablowe do łączności kontynentalnej oraz radiowe do połączeń zamorskich. W RFN buduje się sieć EDS o liczbie około 30 węzłów, natomiast we Francji sieć komputerową CYCLADES, która ma połączyć ze sobą różne komputery i różne urządzenia WE-WY.

4.3. Sieci terminalowe - protokół komunikacyjny

Typową strukturą sieci terminalowych jest połączenie gwiaździste. Oznacza to, że informacje są przesyłane od komputera do terminali i odwrotnie. Sieć terminalowa składa się najczęściej z komputem centralnego, multipleksera, koncentratora lub procesora telekomunikacyjnego, modemów, łącz komunikacyjnych oraz grupy terminali. Sieć terminalową pokazano na rys. 12. W nowoczesnych maszynach cyfrowych są instalo-



Rys. 12. Sieć terminalowa i jej elementy [13, s. 45] zmodyfikowany przez autora niniejszej pracy

wane multipleksery, które umożliwiają połączenie wielu terminali przez jedno łącze. Warunkiem takiego połączenia jest dostosowanie szybkości działania terminali do szybkości transmisji. Ostatnio stosuje się połączenie mikrokomputera z komputerem centralnym w charakterze procesora telekomunikacyjnego. W takim przypadku spełnia on bardzo istotne funkcje związane z przejęciem większości oprogramowania telekomunikacyjnego, zastąpieniem multipleksera lub koncentratora, sterowaniem oprogramowania całej sieci.

Jednak podstawowym elementem sieci jest protokół telekomunikacyjny. Najprostszym sposobem przedstawienia zapisu protokółu telekomunikacyjnego są grafy skierowane (rys. 13). Przykład dotyczy transmisji danych w układzie dwupunktowym między terminalem a komputerem. Do oznaczenia użyto znaków kodu KOI-8, który omówiono szczegółowo w monografii [26, s. 44]. Na potrzeby transmisji wykorzystano z całego kodu grupę 10 znaków:

SOH - początek nagłówka,

STX - początek tekstu,

ETX - koniec sekwencji znaków w tekście,

ETB - koniec bloku (nie dotyczy bloku ostatniego),

EOT - koniec transmisji danych (przesyłanej informacji),

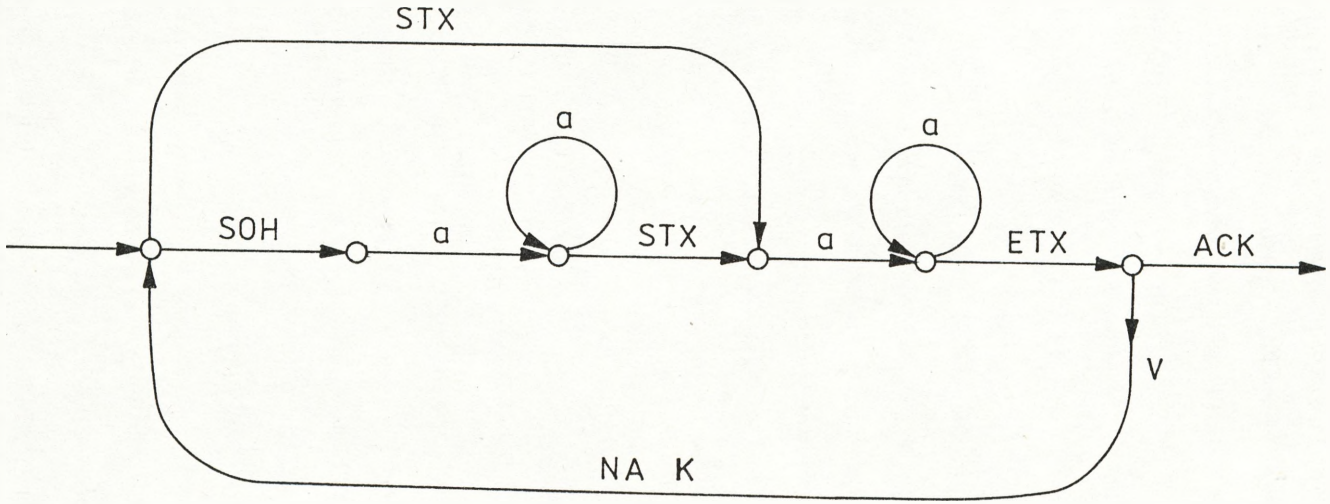
ENQ - zapytanie żądające informacji z terminala o stanie przesyłanych danych lub o identyfikatorze,

ACK - potwierdzenie poprawnego odbioru komunikatu,

NAK - potwierdzenie niepoprawnego odbioru komunikatu,

SYN - znak synchronizujący, zapewniający zgodne działanie urządzeń nadawczych i odbiorczych,

DLE - służy do wprowadzenia dodatkowych znaków kontrolnych,



Rys. 13. Uproszczony graf protokołu komunikacyjnego [13, s. 48] (zmodyfikowany przez autora niniejszej pracy)

v - punkt odwracania kierunku transmisji,

a - znak tekstu nagłówka i kierunku,

x - znak numeru sekwencji komunikatu,

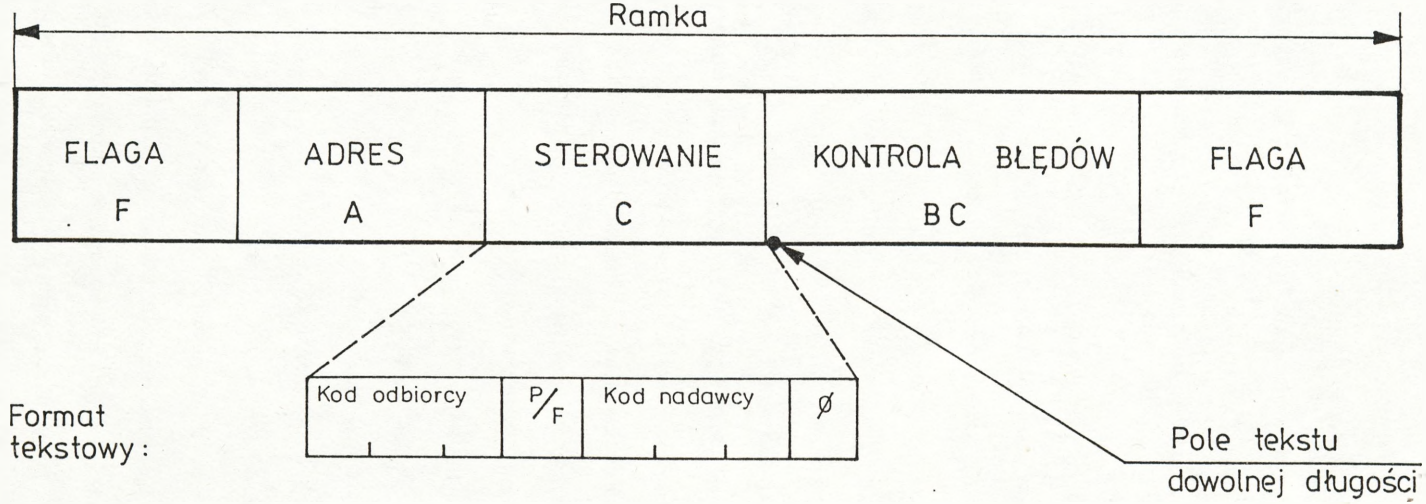
bcc - redundacyjna część komunikatu zawierająca parzystość podłużną lub wielomian generujący.

W myśl przyjętego protokółu ustalono, że struktura komunikatu zawiera trzy pola: 1 - nagłówek, 2 - tekst (zaszyfrowane dane), 3 - pole redundancyjne, które podczas szyfrowania może być pominięte. Bardzo istotnym elementem jest pole pierwsze dotyczące nagłówka, zawierającego numer komunikatu, kod nadawcy i odbiorcy, datę - czas nadania komunikatu oraz priorytet.

Obecnie niektóre firmy zachodnie, produkujące sprzęt komputerowy, wprowadzają protokóły ramowe w miejsce opisanych protokółów standardowych. Protokół ramowy pozwala na definiowanie zadań poszczególnych stacji w sieci, określenie stanów transmisji, kontrolę błędów oraz jednolitości formatu. Każdy komunikat w sieci jest rozpoznawany po tak zwanym "znaku flagowym" umieszczonym w ramce, której ogólny obraz pokazano na rys. 14. Ramka komunikatu ma następującą strukturę [13, s. 52]:

- F - ośmiobitowy znak flagowy,
- A - ośmiobitowe pole adresowe,
- C - ośmiobitowe pole sterujące,
- I - pole tekstu dowolnej długości,
- BC - szesnastobitowe pole kontroli błędów,
- F - ośmiobitowy znak flagowy końca.

Pole sterujące C może mieć jeden z trzech formatów: niesekwencyjny, nadzorczy i tekstowy. Format niesekwencyjny jest stosowany do kontroli łączy. Format nadzorczy podaje informacje o stanie zajętości lub gęstości określonego wejścia lub wyjścia. Format tekstowy służy do przekazywania



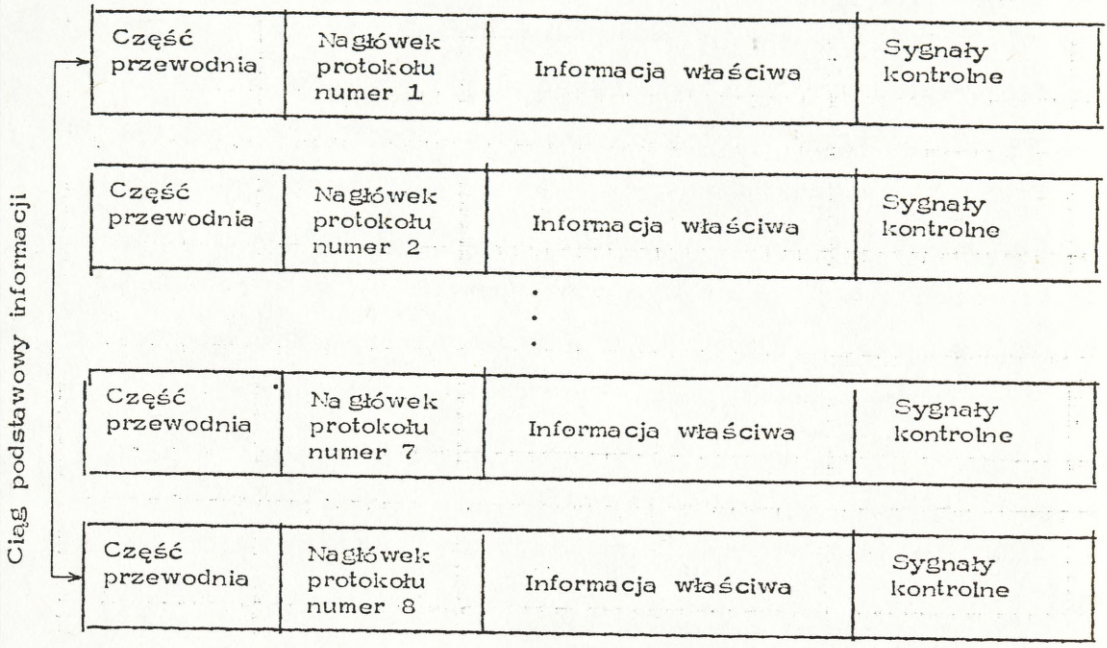
Rys. 14. Ramka komunikatu protokołu ramowego [13, s. 53] (zmodyfikowany przez autora niniejszej pracy)

komunikatu z danymi. Ostatni format jest szczególnie ważny ze względu na szyfrowanie i przesyłanie zaszyfrowanej informacji. Format ten zawiera informacje o numerze odbiorcy zapisane na pierwszych trzech bitach. Bit czwarty, oznaczony jako P, jest wysyłany do terminala podporządkowanego z żądaniem transmisji komunikatu. Natomiast w tej samej pozycji, bit oznaczony jako F, jest wysyłany w odpowiedzi na bit P po zakończeniu nadawania. Kolejne trzy bity tworzą numer nadawcy. Natomiast bit ósmy, ostatni w polu C, jest zawsze zerem (temat ten omówiono w p. 4.4.)

4.4. Transmisja informacji w sieciach komputerowych

Istotnym zagadnieniem w sieciach komputerowych jest przesyłanie informacji. W początkowej fazie sieć ARPA rozwiązała ten problem dość interesująco, chociaż nie uniknięto pewnych błędów. Jak podaje J. Seidler [19], przekazywane w omawianej sieci informacje mają postać ciągu informacji elementarnych. Długość takiego ciągu nie może przekraczać 8096 bitów i ten układ został nazwany ciągiem podstawowym. Informacje zawarte w ciągu podstawowym są umieszczone w pakietach. Długość jednego pakietu nie może przekroczyć 1024 bitów. Dlatego ciąg podstawowy składa się z ośmiu pakietów (rys. 15).

Zasada przesyłania pakietów w sieciach jest z punktu widzenia ochrony przesyłanej informacji dość interesująca. Trasa przesyłania pakietu nie jest znana. W każdym węźle, do którego zostanie skierowany pakiet, jest odczytywany adres węzła docelowego, a z tablicy kierunków wyszukuje się kolejny, wolny węzeł i tam komputer kieruje pakiet. Po drugie obowiązuje zasada, że pakiet przechowuje się w pamięci komputera dopóty, dopóki nie przyjdzie sygnał potwierdzający odbiór pakietu przez węzeł docelowy.



Postać części przewodniej

Nr węzła docelowego	Nr zespołu informacyjnego

Postać nagłówka

Dane z części przewodniej	Numer zespołu informacyjnego	Numer węzła początkowego	Numer pakietu	Numer pakietu poprzedniego	Numer kanału	Sygnały organizacji transmisji

Rys. 15. Struktura pakietów w sieci ARPA [17] (zmodyfikowana przez autora pracy - Z.T.)

Omówiona zasada przesyłania informacji za pomocą pakietów ma pewne wady:

- unikalny kod znakowy ograniczający (a czasami wykluczający) możliwość stosowania innych kodów,

- niejednolitość stosowanej metodyki korekcji błędów,

- konieczność stosowania odrębnych protokołów przy transmisji synchronicznej i start-stopowej,

- wymagana duża ilość informacji sterującej oraz dość duża liczba różnych wersji protokołów.

Te niedociągnięcia wpłynęły decydująco na to, że większość firm zachodnich przechodzi na przesyłanie informacji za pomocą protokołów ramowych rys. 14). Ponieważ system przesyłania informacji za pomocą protokołu ramowego jest korzystny dla szyfrowania informacji, warto zapoznać się z nim bliżej.

Podstawowym elementem protokołu ramowego jest RAMKA ograniczająca długość komunikatu początkowym i końcowym znakiem flagowym. W ramce są przydzielane stałe pola dla poszczególnych części komunikatu (rys. 16). Jednocześnie system stawia wymagania dotyczące wielkości ramki. Nie może być mniejsza od 32 bitów, dlatego każda ramka musi mieć pola F, BC, F. Pole sterujące C decyduje o formacie przesyłanej informacji w sieci. Rozróżniamy trzy formaty komunikatów protokołu ramowego (rys. 14):

1) niesekwencyjny - stosowany do kontroli łączy oraz do nawiązania łączności, uruchomienia terminali, kontroli trybu odezwowego stacji podporządkowanych, zawiadamia o niekorygowalnych błędach,

2) nadzorczy - jest uzupełnieniem formatu tekstowego oraz przenosi informacje o stanie zajętości lub gotowości terminali,

3) tekstowy - służy do przekazywania komunikatu z danymi.

Ponadto pole sterujące C zawiera kod, którego pierwsze trzy bity oraz bity piąty i szósty zawierają różne kody odpowiadające komendom i odezwom pomiędzy komputerami (węzłami). Bit czwarty może przyjmować

R A M K A

Flaga F	Adres A	Sterowanie C	Przesyłanie informacji I	Kontrola błędów BC	Flaga F

Formy komunikatów w zależności od pola C

Niesekwencyjny	Kod	P/F	Kod	1	1
Tekstowy	Zliczanie odbiorcze	P/F	Zliczanie nadawcze	ϕ	
Nadzorczy	Zliczanie odbiorcze	P/F	Kod	ϕ	1

Rys. 16. Protokół ramowy [13] (zmodyfikowany przez autora - Z.T.)

oznaczenie P lub F. P - oznacza przepytywanie i jest wysyłany z żądaniem transmisji komunikatu przez terminal podporządkowany. Bit F oznacza koniec i jest wysyłany przez terminal podporządkowany, po nadaniu komunikatu.

Powyższa zasada przesyłania informacji w sieciach komputerowych za pomocą protokołów ramowych została wykorzystana w Międzyuczelnianej Sieci Komputerowej (MSK). Sieć ta jest pilotową siecią trójwęzłową z następującą lokalizacją węzłów: Centrum Obliczeniowe Politechniki Wrocławskiej, Ośrodek ETO Politechniki Śląskiej oraz Centrum Obliczeniowe Instytutu Podstaw Informatyki PAN w Warszawie. W przyszłości przewiduje się włączenie do sieci uczelnianych ośrodków obliczeniowych w Gdańsku, Toruniu, Poznaniu, Katowicach i Krakowie. W sieci MSK wykorzystano zasadę przesyłania informacji za pomocą protokołu ramowego. Jest ona implementacją protokołu X.25/2 wg CCITT, przy czym ograniczono się jedynie do wersji LAPB, pomijając ustalenia nie mające zastosowania w sieci MSK.

Z wyżej opisanych zasad przesyłania informacji w sieciach komputerowych wynika jeden podstawowy wniosek: dokonano unifikacji metod w zakresie przesyłania komunikatów w sieciach. Jest to nadzwyczaj istotny element w ochronie informacji.

5. ANALIZA NOWOCZESNYCH METOD SZYFROWANIA

Pogląd dotyczący wymagań szyfrowania w sieciach komputerowych jest traktowany dość różnie. Do czasu powstania sieci komputerowych, a raczej do momentu transmisji danych, ochrona informacji była stosunkowo prosta i można ją było uściślić oraz ujednolicić. W tym okresie komputer i ośrodek stanowiły jedną całość. Przetwarzanie odbywało się w ośrodkach obliczeniowych, a wyniki (tabulogramy) użytkownik odbierał bezpośrednio z tegoż ośrodka. Na tym etapie wystarczyło stosowanie określonych metod, najczęściej organizacyjnych, by zabezpieczyć proces przetwarzania danych. Stan ochrony w tym okresie najlepiej przedstawił Sokołowski dotyczącej wyników przeprowadzonej przez siebie ankiety [25]. Autor stwierdził jednoznacznie, że "spośród istniejących metod ochrony, poza metodami organizacyjnymi, stosowane są tylko te metody, których dostarczają producenci komputerów...". Jeśli do tego stwierdzenia dodamy, że metody ochrony dostarczane przez producentów komputerów to nic innego jak zwykła konieczność zabezpieczenia możliwości wieloprogramowej pracy komputera, będziemy mieli pełen obraz "zabezpieczenia" przetworzonych danych w ośrodkach obliczeniowych. Mimo tych faktów należy stwierdzić, że metody ochrony zostały opracowane, czyli były, istniały, chociaż nie zawsze je stosowano.

Oprócz tych metod, już od czasów Cezara, istniały metody związane z szyfrowaniem informacji. Tych metod było dość dużo, jednak do znaczących zaliczamy: metodę Cezara, Viegenera i Vernama. Z tych trzech za wyróżniającą uważa Seidler [18, s. 182] metodę Vernama, gdyż jej entropia rośnie proporcjonalnie do długości ciągu szyfrowego. Rozpatrzmy jeszcze jeden ważny aspekt metod szyfrowania informacji, który szczegó-

łowo przedstawia Sokołowski [23],[24]. Zastanówmy się jednak nad tylko jednym wspólnym elementem wszystkich dotychczasowych metod. Można go opisać, rozpatrując pod tym względem każdą z nich.

Szyfr Cezara

Istotą tego szyfru jest zastąpienie znaków w przesyłanej informacji innymi znakami pochodzącymi z tego samego alfabetu. Zasada szyfrowania jest następująca.

1. Numerujemy kolejne litery alfabetu.

2. Przyjmujemy stałą liczbę, np. 14, która spełnia rolę klucza.

3. Szyfrujemy według schematu: do numeru znaku dodajemy przyjętą wartość klucza (mod N).

Szyfr Viegenera

Szyfr ten, jak i poprzedni, wymaga numerowania liter alfabetu. Następnie przyjmujemy określony klucz, którym z zasady jest słowo. Za pomocą tegoż słowa - klucza, metodą podstawiania, szyfrujemy przesyłaną informację. Literom klucza są również przyporządkowane odpowiednie numery. Szyfrując dodajemy do siebie obie wartości liter. Jest to sama zasada szyfrowania, co poprzednia, z tą różnicą, że kluczem jest słowo zamiast liczby.

Szyfr Vernama

Jest to szyfr różniący się tym od omówionych zasad szyfrowania, że zastosowano odpowiednio długi klucz. Szyfr ten, tak jak i poprzednie, wymaga spełnienia podstawowego warunku: $N \leqslant K$, gdzie: N - długość przesyłanej wiadomości, K - długość klucza. W razie niespełnienia tego warunku następuje systematyczne powtarzanie klucza, co jak stwierdza Seidler [18, s. 182] dostarcza nieprzyjacielowi informacji o kluczu.

Jeden z najnowszych szyfrów amerykańskich, nazwany metodą RSA - jawnego klucza, wykorzystuje również zasady zawarte w poprzednich

metodach. Różnica polega na tym, że zastosowano dwa klucze: jeden do szyfrowania, drugi do deszyfracji (zagadnienie to omówiono szczegółowo w rozdz. 5.1).

Ta krótka analiza, chociaż poprzedzona odpowiednim uzasadnieniem w monografii [27], doprowadza nas do zasadniczego wniosku.

Wszystkie dotychczasowe metody szyfrowania informacji wykorzystują zasadę szyfrowania za pomocą KLUCZA. W tym przypadku deszyfracja polega na jego znalezieniu. Właśnie wykorzystując tę właściwość szyfrów, Polacy deszyfrowali różne meldunki przesyłane przez wojska niemieckie podczas II wojny światowej. Tę podstawową zasadę szyfrowania dotychczasowymi metodami można zdefiniować następująco: informacja jest szyfrowana za pomocą przyjętego klucza, którego postać w każdej metodzie jest odmienna.

Z powyższej analizy wypływa jeszcze jeden wniosek, który dotyczy jakości szyfru. Widać wyraźnie kierunek poszukiwań polegający na udoskonaleniu klucza szyfrowego. Najpierw była nim pewna wartość stała, następnie było słowo, które można było odpowiednio przedłużać, aż wreszcie opracowano metodę dwóch kluczy, którą nazwano metodą jawnego klucza. Ogólnie więc chodziło o znalezienie takiej metody, takiego klucza, który ma dużą moc kryptograficzną. Innymi słowy, wartość metody szyfrowania określano jakością klucza. Dlatego autorzy różnych prac, a szczególnie Sedler [18] i Shannon [20] dokonują oceny jakości szyfru na podstawie liczby kluczy, prawdopodobieństwa dekryptażu oraz entropii klucza. Wymienione metody oceny szyfrów są również dowodem na to, że podstawowym elementem każdego szyfru jest klucz. Dlatego właśnie badania metody ograniczono do badania jakości klucza szyfrowego. Ponieważ do tej pory nie opracowano innych metod oceny jakości szyfru oprócz badań klucza, dlatego autor niniejszej pracy był zmuszony dokonać oceny szyfru

UNITAKOD tymi samymi metodami. Jednocześnie w rozdziałach 7 i 8 zaproponowano inne rozwiązania tego bardzo złożonego problemu.

Przechodząc do wymagań szyfrowania w sieciach komputerowych należy stwierdzić, że sama moc kryptograficzna określonej metody nie wystarcza, aby zastosować ją w sieci. Doszły nowe elementy związane z sieciami kontynentalnymi, a nawet satelitarnymi, dlatego obecne wymagania co do metod szyfrowania muszą również ulec zmianie. Chociaż literatura światowa nadal poszukuje określonego szyfru, to jednak jesteśmy świadkami powstawania przesłanki pierwszych wymagań szyfrów w sieciach komputerowych. Jest to pozytywne zjawisko, którego lekceważyć ani pomijać nie wolno. Opierając się na wcześniejszej analizie tego tematu, można wymagania te ująć następująco.

1. Ochrona komputera (została przedstawiona na rys. 1 oraz omówiona w rozdziale 1 i 3).

2. Ochrona przetwarzanych informacji w komputerze (zaprezentowano ją w monografii [26, s. 30-40, 56-58]). Problem szyfrowania informacji podczas przetwarzania danych w komputerze jest do dziś traktowany zupełnie marginesowo. Jest to oczywiście karygodnym błędem, tym bardziej że jest to problem tak samo ważny jak ochrona samego komputera.

3. Identyfikacja nadawcy i odbiorcy (była dotychczas zupełnie pomijana). W niniejszej pracy ujęto ten problem jako część składową metody UNITAKOD, co uniemożliwia przesyłanie fałszywki w sieciach komputerowych.

4. Szyfrowanie nagłówka jest jednym z najważniejszych problemów przesyłania informacji w sieciach komputerowych. W tym miejscu wypada podkreślić brak takiej możliwości w systemach komputerowych na Zachodzie. O braku możliwości szyfrowania nagłówka Weber w swej pracy pisze: "Zaszyfrowana może być tylko właściwa informacja użytkowa. Nagłówek meldunku z potrzebnymi do sterowania informacji musi być przekazywany otwartym tekstem" [32, s. 52] .

Do wymienionych wymagań stawianych obecnym szyfrom należy dodać (wcześniej omówione) wymaganie dotyczące dużej mocy kryptograficznej zastosowanej metody ochrony.

Zaprezentowana ogólna koncepcja ochrony informacji w systemach komputerowych wymaga odpowiedniego rozwinięcia i uzasadnienia. Dokonajmy w tym celu podsumowania przeprowadzonej analizy szyfrów pod kątem ich wspólnej cechy:

- szyfr Cezara - kluczem jest stała liczba,
- szyfr Viegenera - kluczem jest stałe słowo,
- szyfr Vernama - kluczem jest stałe, długie słowo,
- szyfr RSA - kluczem są stałe liczby pierwsze p oraz q.

Dodając do tego wykazu szyfry macierzowe zauważymy, że i tam określony układ tworzy klucz, za którego pomocą szyfrujemy przesyłaną informację. We wszystkich przypadkach informacja jest szyfrowana za pomocą określonego klucza szyfrowego. Wynika stąd ogólny, lecz niezmiernie ważny, wniosek dotyczący zasad szyfrowania przesyłanej informacji: żadna metoda ochrony informacji oparta na zasadzie klucza szyfrowego nie może być uznana za metodę nowoczesną i wystarczającą w zabezpieczeniu poufności informacji.

5.1. Problemy ochrony informacji wojskowej

Chyba od początku istnienia ludzkości człowiek poszukiwał takiego sposobu przekazywania tajnych informacji, aby nie każdy, lecz tylko ten "upoważniony odbiorca" mógł je po otrzymaniu odczytać. Innymi słowy było to poszukiwanie określonego sposobu szyfrowania informacji. Najprostszy sposób, nazwijmy go "szyfrowaniem", lub "utajnianiem", pochodzi jeszcze z czasów Aleksandra Wielkiego. Aby przekazać informację tajną

przez linię frontu, golono żołnierzowi głowę i informację wypisywano na skórze głowy. Po odrośnięciu włosów żołnierz w przebraniu niewolnika przechodził linię frontu i w ten sposób informacja trafiała do rąk określonego odbiorcy. Dziś taki sposób nie jest do przyjęcia z kilku względów, z których najważniejszym jest czas przekazania informacji. Dziś podstawą przekazywania informacji, szczególnie tajnych informacji wojskowych, jest jej gromadzenie i przetwarzanie. Mimo że do dzisiejszego dnia zakorzenił się pogląd, iż najlepszym zabezpieczeniem jest kłódka, plomba i wartownik, to jednak każdy, kto ma do czynienia z przetwarzaniem danych, będzie musiał zajmować się problemami ochrony przetwarzanej informacji.

Zastosowanie komputerów w wojsku jest powszechne. Wykorzystuje się je w planowaniu działań bojowych, projektowaniu i podejmowaniu decyzji, transportach wojskowych, działaniach kwatermistrzowskich, a nawet w medycynie wojskowej. W pamięciach systemów komputerowych jest przechowywana ogromna ilość ważnych informacji wojskowych. Niejednokrotnie są to informacje ogromnej wagi. Utrata ich lub wykorzystanie niezgodne z przeznaczeniem może wyrządzić niepowetowane szkody wojsku, a nawet naruszyć system obronny państwa. Nie wolno nie zauważać tych poważnych problemów.

Ogólnowojskowy system kierowania bazuje na pionach organizacyjno-funkcjonalnych, wyspecjalizowanych w różnych dziedzinach. Te piony ukształtowały się historycznie w taki sposób, że ich działanie wykazuje wiele cech odrębnych. Jednak organizacyjnie tworzą one jednolity aparat kierowania w wieloszczeblowej strukturze hierarchicznej, podporządkowanej jednoosobowemu dowodzeniu. Natomiast pod względem funkcjonalnym są one w wysokim stopniu autonomiczne. Właśnie zasada jednoosobowego dowodzenia wymaga, aby na określonym szczeblu dowódczym następowała

selektywna integracja informacji w różnych obiektach kierowniczych. Jest to realizowane w różnych układach funkcjonalnych, kierowanych przez osoby o odpowiednim zakresie kompetencji. Dlatego projektowanie systemów informatycznych na potrzeby kierownictwa wojskowego i następnie ich wdrażanie jest ingerencją w dziedzinę niezwykle skomplikowanych układów i zależności. Ta ingerencja musi zdążać w kierunku usprawniania procesów informowania kierownictwa drogą zastosowania zintegrowanego systemu informatycznego. Ta właśnie integracja systemów i jednoosobowe dowodzenie stają się koniecznymi elementami w systemach ochrony informacji.

Z chwilą uzyskania przez użytkownika dostępu do systemu komputerowego pojawiają się pytania, z jakich programów będzie on korzystał i do jakich zbiorów i w jakim zakresie powinien otrzymać dostęp. Jeżeli użytkownik realizuje swój własny program i korzysta z własnych zbiorów danych, rola systemu ochrony ogranicza się do nadzoru, aby użytkownik faktycznie korzystał tylko z własnych zbiorów. Jeżeli jednak programy i zbiory są wykorzystywane przez kilku użytkowników, wówczas każdemu z nich należy przyporządkować pewien poziom zaufania. Poziom ten zazwyczaj jest ustalany na podstawie kodu identyfikacyjnego. Są to jednak zabezpieczenia związane z przetwarzaniem danych w ośrodku obliczeniowym. Sposób tego typu zabezpieczenia przedstawiłem w punkcie 3 oraz w pracach [26, s. 8-11, s. 16-40] oraz [27, s. 29-42]. Jednak w przypadku teleprzetwarzania danych lub teletransmisji informacji zagadnienie ochrony staje się bardziej skomplikowane. Należy zdawać sobie sprawę z następujących faktów.

Ochrona informacji podczas przetwarzania danych w ośrodku obliczeniowym może być ograniczona do zastosowania systemu ochrony w programie zarządzającym lub systemie operacyjnym. Wystarczy wyeliminować z systemu ochrony czynnik ludzki i całe zagadnienie ochrony powierzyć komputerowi. Konieczność zastosowania odrębnego systemu ochrony w programie zarządzającym wynika z tego, że zarówno systemy operacyjne,

jak i programy zarządzające nie mają procedur ochrony. To, co w systemach operacyjnych i programach zarządzających zwykło się nazywać ochroną, w rzeczywistości nie jest niczym innym, jak gwarantem umożliwiającym wieloprogramową pracę komputera.

Jedynym i prawdziwym zabezpieczeniem informacji jest wyłącznie jej szyfrowanie. Daje ono gwarancję, że przypadkowe przechwycenie informacji lub przypadkowy dostęp do niej, odczytanie zawartej w niej treści są praktycznie niemożliwe (zagadnienie to szczegółowo przedstawiłem w punkcie 5.5, oraz 8).

Aby określić działania zarówno wojsk własnych, jak i przeciwnika, należy systematycznie przetwarzać informacje na potrzeby dowodzenia, które jest i być musi procesem ciągłym. Stwarza to potrzebę stosowania komputerów na wszystkich szczeblach dowodzenia, ich pełnego i skutecznego wykorzystania. Jednak współczesne systemy komputerowe są dalekie od bezpiecznego przetwarzania danych i jeszcze długo pozostaną takimi. Dlatego informacje tajne, bez odpowiedniego zabezpieczenia, nie powinny być w komputerach przechowywane, przetwarzane, a tym bardziej przesyłane liniami transmisji danych. Ochrona informacji komputerowej w systemach wojskowych jest absolutną koniecznością i tego lekceważyć nie wolno.

5.2. Analiza ochrony informacji w państwach zachodnich

Ochrona informacji przesyłanych za pomocą sygnałów w sieciach telekomunikacyjnych, przewodowych i radiowych wymaga odpowiedniego zabezpieczenia. Zastosowanie technik informatycznych, wykorzystanie komputerów do gromadzenia, przetwarzania i udostępniania informacji wzmogło zainteresowanie problematyką ochrony. Problem ten dostrzeżono w Stanach Zjednoczonych pod koniec lat pięćdziesiątych. Gromadzona informacja dotyczyła wówczas osób prywatnych i zawierała dane o ich sytuacji rodzinnej,

finansowej, stanie zdrowia, poglądach politycznych, religijnych itp. Informacje te były niejednokrotnie nieaktualne, niepełne, a czasami nieprawdziwe. Podejmowanie - na podstawie tego typu informacji - decyzji dotyczącej niejednokrotnie spraw finansowych było przedsięwzięciem ryzykownym. Zmusiło to władze Stanów Zjednoczonych do wydania odpowiednich aktów prawnych regulujących wykorzystywanie informacji przez różne instytucje.

Do pierwszych aktów prawnych można zaliczyć akt normatywny z 1970 r. (Fair Credit Reporting Act), określający zasady obchodzenia się z informacjami osobowymi, wykorzystywanymi przez instytucje kredytowe. Kolejnym aktem była ustawa o ochronie własności prywatnej wydana jako dokument - Privacy Act of 1974. W tych samych latach w Szwecji wydano ustawę o ochronie informacji dotyczącej prywatnej własności. Dwie ustawy o ochronie informacji wydano w 1976 r. w RFN oraz w 1977 r. w Szwajcarii. Niezależnie od ustaw opracowano kompleksowy system ochrony przetwarzania danych, który w praktyce okazał się mało skuteczny, szczególnie przy przetwarzaniu informacji dotyczącej tajemnicy państwowej, służbowej i wojskowej. Dlatego też od wielu lat działa w Stanach Zjednoczonych pokaźna liczba specjalistów w wydziale szyfrów Narodowej Agencji Bezpieczeństwa (National Security Agency), pracując nad znalezieniem właściwego klucza zabezpieczającego w pełni przetwarzaną i przesyłaną informację.

W ostatnich latach ochrona informacji jest przedsięwzięciem pierwszoplanowym. Sytuacja w informatyce zmieniła się radykalnie. Wraz z rozwojem komputeryzacji, tworzeniem sieci komputerowych, wzrasta możliwość infiltracji przechowywanych danych. Jak pisze Weber [32], informatyka przechodzi do mieszkań, a penetracja sieci komputerowych staje się po prostu zabawą. Dla pewnej grupy ludzi przechwytywanie informacji stało się normalnym procederem. Dla nich nie ma nic świętego. Dotyczy to

również sieci komputerowych Amerykańskiego Centrum Badawczego Broni Atomowej w Los Alamos, w którym - jak podaje Weber - dokonano infiltracji danych. W tej sytuacji przetwarzanie, przechowywanie i przesyłanie informacji staje się szczególnie zagrożone. Dotychczasowe metody przestają być skuteczne a nawet tracą sens, natomiast realizm dokonania infiltracji rośnie. Jedyną drogą ochrony danych staje się wyłącznie kryptologia, czyli nauka o kodowaniu (szyfrowaniu) informacji. Ostatnio w literaturze zachodniej pojawiły się takie hasła, jak "tajny kod nie do złamania", "jawny klucz", "bezpieczny i pewny system szyfrowania". Trzeba przyznać, że tego typu hasła, zabarwione smakiem propagandy, pobudzają fantazję ludzką. Pojawienie się haseł o jawności metod, a szczególnie kluczy szyfrowych, które dotychczas stanowiły największą tajemnicę, może pobudzić nawet najspokojniejsze umysły.

Przed kilkoma laty dwaj amerykańscy matematycy Diffie i Hellman [2] opracowali system szyfrowania polegający na stosowaniu dwóch różnych kluczy - jednego do szyfrowania, a drugiego do deszyfracji. Był to początek powstania na Zachodzie nowej metody szyfrowania, opracowanej w 1983 r. przez trzech amerykańskich matematyków: Riverta, Shamira i Adelmana, która została nazwana od pierwszych liter nazwisk "Metodą RSA - jawnego klucza" [15],[16],[19]. Metoda ta zrewolucjonizowała pogląd na temat zasad szyfrowania. Bardzo ważnym elementem jest zastosowanie w niej dwóch różnych kluczy (jednego do szyfrowania, a drugiego do deszyfracji). Ponadto jeśli zastosuje się duże liczby pierwsze (rzędu 150-200 znaków), można w jawny sposób szyfrować bez obawy przed deszyfracją przez osoby nie upoważnione.

Istotnym elementem w ochronie informacji jest uznanie (wyłącznie) szyfrowania za jedyny i w pełni skuteczny element ochrony. Na podkreślenie zasługuje również zastosowanie identyfikacji osoby przekazującej

informację. W dotychczasowych metodach identyfikowano osobę otrzymującą meldunek czy pobierającą informację, a nie interesowano się możliwością przekazania informacji nieprawdziwej, tzw. "fałszywki". Czasami informacja fałszywa może być bardziej szkodliwa niż przechwycona informacja zaszyfrowana. Te dwa elementy, na które obecnie jest zwrócona uwaga państw zachodnich, wydają się uzasadnione w erze sieci komputerowych czy też komputerowych sieci satelitarnych. Jednak w dalszym ciągu mamy do czynienia z kluczem i to kluczem tajnym, który nadal wymaga ochrony.

W sieciach komputerowych obowiązuje zasada szyfrowania nagłówka (adresu) ciągu szyfrowego, której to możliwości (jak już wspomniałem) nie zna metoda RSA. Mimo tego zastosowanie dwóch różnych kluczy szyfrowych oraz identyfikacji odbiorcy i nadawcy skłania nas do bliższego zapoznania się z tą metodą.

5.3. Metoda RSA - jawnego klucza

Aby lepiej zobrazować zasady działania metody RSA, należy rozpatrzyć następujący przykład oparty na kilku publikacjach zachodnich [1], [6], [32]. Zakładamy, że pomiędzy użytkownikami A i B jest przesyłany meldunek składający się z dwóch liter EG. Zakładamy również, że użytkownicy dokonali wyboru i obliczeń i wielkości koniecznych do szyfrowania i deszyfracji takich, jak p, q, u, n, t, b. Jak już wspomniałem, szyfrowanie za pomocą metody RSA - jawnego klucza opiera się w zasadzie na szyfrowaniu za pomocą dwóch kluczy: jawnego klucza szyfrującego i tajnego deszyfrującego. Model matematyczny obu kluczy wyrażamy wzorem:

- jawny klucz szyfrujący:

$$y = z^u \pmod n,$$

- tajny klucz deszyfrujący:

$$y^{*} = y^{b} \pmod{n},$$

gdzie:

z - ciąg znaków przesyłanej informacji,

u - wybrana liczba pierwsza - wartość jawna,

b - obliczona ściśle tajna wartość, będąca podstawą klucza deszyfrującego,

p - wybrana liczba pierwsza - wartość tajna,

q - wybrana liczba pierwsza - wartość tajna,

n = (p * q) - wartość jawna,

t = (p-1) * (q-1) - wartość tajna.

Teraz przystępujemy do szyfrowania przesyłanej informacji. Bierzemy wybrane wielkości p i q oraz u, na których podstawie liczymy wielkość n. Następnie wszystkim znakom maszynowym przyporządkowujemy odpowiednie wielkości liczbowe. Załóżmy, że znakom alfabetu przyporządkowaliśmy następujące liczby:

A = 01	D = 04	G = 09	
B = 03	E = 05	H = 08	
C = 07	F = 10	I = 02	itd.

Szyfrowania dokonujemy na podstawie zasady przesyłania grupy znaków, np. EG. Z tabeli przyporządkowania odczytujemy wartości liczbowe: E = 05 oraz G = 09. Dlatego przesyłany ciąg informacji zapisujemy jako:

$$z = 05 \quad i \quad 09 = 509.$$

Jednocześnie z przeprowadzonych obliczeń otrzymaliśmy wynik dla n = 52961 oraz wybraliśmy liczbę pierwszą u = 131. Wielkości te podstawiamy do wzoru:

$$y = 509^{131} \pmod{52961}.$$

Kolejne potęgi wyrażenia y otrzymujemy według następujących zasad:

509^{1} mod 52961 = 509,

509^{2} -"- = 47237,

509^{4} -"- = 34278,

509^{8} -"- = 41499,

509^{16} -"- = 34164,

509^{32} -"- = 24378,

509^{64} -"- = 11503,

509^{128} -"- = 22431.

Potęgę liczby 131 otrzymujemy z sumy liczb: 128 + 2 + 1:

(128 + 2) 22431 * 47237 (mod 52961) = 35381,

(... + 1) 35381 * 509 (mod 52961) = 2189.

Wielkość tę, jako szyfr wyrażony liczbą: y = 2189, przesyłamy do adresata.

Adresat, po otrzymaniu ciągu szyfrowego 2189, najpierw oblicza ściśle tajną wielkość "b". W wyniku otrzymuje liczbę b = 37271. Znając jawną wielkość "n", przystępuje do deszyfracji:

$$y^{*} = y^{b} \pmod{n},$$

$$y^{*} = 2189^{37271} \pmod{52961},$$

Nie analizując poszczególnych faz obliczeń, które przebiegają zgodnie z wyżej podanym przykładem obliczania kolejnych potęg, adresat otrzymuje w wyniku końcowym wielkość $y^{*} = 509$. Adresat, znając zasadę szyfrowania polegającą na przyporządkowaniu jednemu znakowi dwóch cyfr, odczytuje otrzymany wynik jako: 05 i 09. Następnie za pomocą tablicy przyporządkowania zamienia te wielkości na znaki alfabetu i otrzymuje:
05 = E oraz 09 = G.

Wspomniano na wstępie, że metoda RSA (niezależnie od stosowania dwóch różnych kluczy szyfrowych) ma możliwość identyfikacji nadawcy i odbiorcy. W tym celu przeanalizujemy kolejny przykład identyfikacji osoby

nadającej szyfrogram, aby się upewnić, czy otrzymana informacja nie stanowi fałszywki.

Zakładamy, że informacja jest przesyłana pomiędzy użytkownikami od A do B. Jest ona zaszyfrowana i przed jej deszyfracją należy zidentyfikować nadawcę. Do szyfrowania identyfikacji zostały wybrane następujące liczby:

p = 73 (wybrana liczba pierwsza - wartość tajna),

q = 151 (wybrana liczba pierwsza - wartość tajna),

u = 11 (wybrana liczba pierwsza - wartość jawna),

Obliczamy klucz szyfru b ze wzoru

$$u * b = 1 \pmod t,$$

$$\frac{u * b}{\mod t} = 1,$$

dla wartości: u = 11 oraz t = (73 - 1) (151 - 1) = 10800, dobieramy takie wartości liczb pierwszych, by reszta z dzielenia równała się jedności i otrzymujemy

$$\frac{11 * b}{10800} = 1,$$

stąd

b = 5891.

Identyfikacja nadawcy

Pomiędzy nadawcą A i odbiorcą B ustalono, że wielkością identyfikującą osobę nadawcy będzie cyfra 7. W zaszyfrowanej wiadomości nadawca przesyła w ustalonym miejscu liczbę "9980", która została obliczona ze wzoru

$$y = 7^{11} \pmod n,$$

w którym n = (p * q) = 73 * 151 = 11023.

Dla podanych wielkości poszukujemy resztę z dzielenia

$$y = \frac{7^{11}}{11023}$$

i otrzymujemy y = 9980. Odbiorca deszyfruje. Zna on wielkości: y = 9980, n = 11023, obliczył b = 5891 oraz tajną cyfrę identyfikującą nadawcę 7. Deszyfracja, a tym samym identyfikacja nadawcy, odbywa się na podstawie wzoru

$$y = y^b \pmod n,$$

$$y = 9980^{5891} \pmod{11023}.$$

Po dokonaniu obliczeń otrzymujemy resztę z dzielenia y = 7. Teraz już wiadomo, że przesłana wiadomość pochodzi od właściwego nadawcy i można przystąpić do deszyfracji treści wiadomości.

5.4. Analiza i praktyczna możliwość stosowania metody RSA

Już od dawna matematycy zajmowali się zagadnieniem szyfrów, chociaż w początkowym okresie traktowano to jako zajęcie z dziedziny egzotyki. Początki matematyki w kryptologii wiązały się z przyporządkowaniem literom alfabetu różnych wartości liczbowych, np. A = 01, B = 02,...,Y = 25, Z = 26. To przyporządkowanie literom alfabetu różnych wartości liczbowych jest aktualne po dzień dzisiejszy. Kolejnym krokiem było wprowadzenie wartości modulo, której wielkość zależała od liczby liter alfabetu, w naszym przypadku mod = 26. Dla uzyskania większej mocy kryptograficznej przyjmowano stałą wielkość np. 15, którą dodawano do każdej liczby odpowiadającej określonej literze. Dla przykładu weźmy literę N, której wartość liczbowa wynosi 14. Po dodaniu do liczby 14 stałej 15 otrzymujemy wartość 29, która jest większa od wartości modulo. Dzieląc liczbę 29 przez wielkość modulo 26, otrzymujemy resztę z dzielenia równą 3, która odpo-

wiada literze "C". W ten sposób litera "N" została zamieniona na "C", a liczba 15 na 03. Otrzymaną resztę szyfrowania określamy mianem klucza, który dla każdego szyfru jest wielkością tajną. Chociaż różne mogą być klucze szyfrowe, to jednak zasady ogólne pozostają od lat niezmienione. Tym problemem zajmowali się dwaj amerykańscy matematycy Diffie i Hellman w pracy [2]. Opracowali oni klucz jawny, gdyż deszyfracja następowała według zupełnie innego klucza (co przedstawiono w poprzednim podrozdziale).

Jednocześnie Merkle w swych pracach [11], [12], zaprezentował możliwość zastosowania w metodzie publickey (znanego już w starożytności) problemu dolnych liczb całkowitych. Należy z grupy liczb wyszukać, które dodane do siebie dadzą określoną liczbę "Z". Metodę tę obrazuje podany przykład.

Przykład. Dane jest 10 liczb: 974, 976, 980, 988, 1004, 1036, 1100, 1228, 1484, 1996. Wyszukać te liczby, których suma Z = 4503. Jedynie obecnie znaną metodą rozwiązania tego problemu jest tworzenie wszystkich podzbiorów danego dziesięcioelementowego zbioru liczb, np. (974, 976, 1484) lub (980, 1004, 1996) itd. oraz sprawdzania ich sum. Ponieważ zbiór dziesięcioelementowy ma 2^{10} podzbiorów, dlatego trzeba sprawdzić przynajmniej połowę, czyli 512 możliwych przypadków. Jeśli jednak zamiast 10 liczb wybiera się 30, to liczba podzbiorów wyniesie

$$2^{30} = 1073741824,$$

z czego trzeba przeciętnie sprawdzić połowę, a nie 536870912. Przy tych obliczeniach należy pamiętać, że rząd 30 liczb w zbiorze jest mały.

Metodę tę analizował Shamir [19] i wykazał, na podstawie badań Lenstrów, ojca i syna, oraz Lovasza [8], że metoda Markle'a jest w miarę skuteczna jedynie dla dużych liczb. Dalsze badania doprowadziły do opracowania (przez trzech amerykańskich matematyków: Rieresta, Shamira

i Adelmana [15], [16]) metody RSA, opartej na iloczynie dwóch liczb pierwszych - "p" i "q".

Pomijając samą zasadę szyfrowania według metody RSA, pragnę na podstawie literatury zachodniej dokonać analizy samych liczb pierwszych. Przeanalizujmy wyżej wspomniany problem w oparciu o pracę Biegerta [1]. Pierwszym sukcesem w zakresie możliwości rozkładania liczb pierwszych na czynniki było rozłożenie liczby trzydziestodziewięciomiejscowej. Dokonali tego Morrison i Brillhart [10] za pomocą komputera IBM-360. Kolejnego kroku dokonał w tej dziedzinie Pomerance [16], który zaproponował tzw. kwadratowe sito do rozkładania liczb. Dzięki niemu Morrison i Brillhart rozłożyli tę samą liczbę na tym komputerze w 1982 r. w 90 minut zamiast obliczeń tradycyjnych przez kilka tygodni. Idea sita jest stosunkowo prosta i znana przed ponad 2000 laty, kiedy Erastosthenes podał schemat wyszukiwania liczb pierwszych. Po prostu wykreśla się wszystkie liczby podzielne przez 2,3,5,7,... poza samymi liczbami 2,3,5,7,... - wszystkie nie skreślone liczby są liczbami pierwszymi. W tym zakresie myśl Pomerance'a prowadzi do przeliczenia polegającego na "uproszczeniu" algebry, czyli

$$(a+b)^2 = a^2 + b^2.$$

Przeliczenie to jest oczywiście błędne, lecz brakujący element podwójnego iloczynu (+2ab) staje się praktycznie zerem, jeśli w miejsce "a" i "b" podstawi się liczby pierwsze "p" i "q" i zredukuje za pomocą wzoru $n = p * q$. W takim przepadku otrzymuje się wzór

$$(p+q)^2 = (p^2 + q^2) \mod n,$$

Jeśli uwzględnimy fakt, że każdą liczbę naturalną "x" można napisać w postaci

$$x = kp + 1q,$$

a po podniesieniu do kwadratu otrzymujemy: $x^2 = (kp + 1q)^2 = (k^2p^2 + 1^2q^2) \mod n$ oraz odpowiednio

$$y = \pm kp \pm lq ,$$

z którego to równania otrzymujemy cztery rozwiązania, przy czym prawdopodobieństwo dla każdej z czterech wartości jest równe. Jeżeli w tych przypadkach dla "x" i "y" otrzymamy właściwą kombinację znaków, to liczby (x + y) oraz "n" mają wspólny dzielnik "p" lub "q".

Wyżej opisana zasada, przedstawiona przez Biegerta [1], a dotycząca liczb pierwszych, legła u podstaw metody "public-key". Analizując w dalszym ciągu metodę jawnego klucza dochodzimy do wniosku, że istotnym elementem jest możliwość rozłożenia na czynniki określonego iloczynu liczb pierwszych "n". Davis i Holdvige podają, że w 1984 roku udało się za pomocą komputera CRAY-IS rozłożyć czterdziesiopięciomiejscową liczbę pierwszą w ciągu dwóch godzin. Jednocześnie ci sami autorzy prognozują, że za pomocą największych obecnie komputerów, CRAY-X-MP lub FUJITSU-VP-200, można rozłożyć liczbę o 100 miejscach w przeciągu dwóch lat. Natomiast w 1986 roku Silverman dokonał rozłożenia liczby pierwszej o długości 81 miejsc w ciągu zaledwie 150 godzin. Dokonał tego za pomocą komputerów personalnych PC, które w liczbie ośmiu połączył ze sobą. Prace te zostały opisane przez Biegerta [1].

Z powyższych rozważań wynika jeden podstawowy wniosek, który można sprecyzować następująco: metoda RSA - jawnego klucza wymaga stosowania wyłącznie dużych liczb pierwszych i to powyżej 150 miejsc. Po tym stwierdzeniu należy postawić zasadnicze pytanie: Czy istnieją w rzeczywistości liczby pierwsze powyżej 150 miejsc? Już matematycy grecy twierdzili, że nie ma największej liczby pierwszej. Z tego wynika wniosek, że ciąg liczb pierwszych nie jest skończony. Oto kilka przykładów dotyczących poszukiwań dużych liczb pierwszych. W dniu 5 września 1984 r. znaleziono, za pomocą komputera SIEMENS-7-882, w Centrum Obliczeniowym Uniwersytetu w Hamburgu, liczbę pierwszą o 7067 miejscach.

Dalsze poszukiwania dużych liczb pierwszych przyniosły kolejne rezultaty i liczba znaleziona w Hamburgu zajmuje obecnie 8 miejsce w świecie. W roku 1985 w New Jersey - USA znaleziono dwie kolejne liczby pierwsze o ponad 7067 miejscach, lecz już w tym samym roku znaleziono w Hamburgu kolejną liczbę pierwszą posiadającą 7984 miejsc, której postać przedstawił Biegert. Liczba ta zajmuje obecnie piąte miejsce w świecie. Na pierwszym miejscu jest obecnie liczba pierwsza znaleziona przez Słowińskiego-Chippera Falls, USA, która ma wielkość $2^{216091} - 1$. Jest to olbrzym liczbowy o 65050 miejscach.

Uważam, że przedstawiona powyżej analiza liczb pierwszych jest wystarczającym dowodem na uświadomienie sobie ogromnych trudności w poszukiwaniu dużych liczb pierwszych i jeszcze większych trudności w ich praktycznym wykorzystaniu. Ponieważ metody szyfrowe wymagają możliwości praktycznego stosowania, a co najważniejsze nieutrudniania pracy ani ludziom, ani komputerowi podczas ich stosowania, należy zgodzić się z ogólnym twierdzeniem, że wymagania metody RSA - jawnego klucza można spełnić jedynie teoretycznie. Dokonajmy obecnie analizy metody UNITAKOD.

5.5. Zasady szyfrowania bez klucza - metoda UNITAKOD

Jak wspomniano na początku rozdziału 5, żadna metoda ochrony informacji oparta na zasadzie klucza szyfrowego nie może być uznana za metodę nowoczesną i wystarczającą w zabezpieczeniu poufności informacji. Klucz był, jest i pozostanie tym elementem, który obniża moc kryptograficzną każdej metody. Dlatego w państwach zachodnich poszukiwano różnych kluczy do szyfrowania i do deszyfracji informacji. Wszelkie wyniki idące w kierunku znalezienia "skutecznych" czy też "bezpiecznych" kluczy należy uznać za bezcelowe. W każdym przypadku, niezależnie od

rodzaju metody, deszyfracja polega na znalezieniu określonego klucza. Mając klucz szyfrowy, można bez trudu dokonać deszyfracji dowolnego ciągu szyfrowego. W dodatku można dokonać deszyfracji bez pozostawienia śladu nielegalnej działalności. Ten fakt można porównać z wchodzeniem i wychodzeniem z mieszkania za pomocą klucza; czynność ta nie pozostawia po sobie śladu w postaci uszkodzenia drzwi. Historia uczy nas, że żadna z metod ochrony nie była skuteczna, jeśli informacje szyfrowano za pomocą klucza. Najlepszym tego dowodem jest system ENIGMA-ULTRA z czasów II wojny światowej, który stał się jedną z przyczyn klęski armii hitlerowskiej.

Wychodząc z powyższych zasad szyfrowania informacji, opracowano nową metodę zwaną UNITAKOD. Ponieważ, jak wspomniałem, klucz jest najsłabszym punktem we wszystkich metodach szyfrowania, postanowiono pominąć go i opracować algorytm oparty na układzie tablic. Ponadto z całym naciskiem należy podkreślić, że w algorytmie szyfrowania udział bierze sam ciąg szyfrowy jako część składowa algorytmu, jako suma współrzędnych tablicy kodów i tablicy wierszy oraz kolumn przesyłanej informacji. Dlatego poszukiwanie treści ciągu szyfrowego, a tym bardziej klucza, mija się z celem.

Podstawowym elementem algorytmu jest tablica kodów kryptograficznych (rys. 17). Tablicę opracowano na podstawie 60 znaków kodu maszyn cyfrowych seria ICL-1900. Pominięto w niej litery małe alfabetu oraz trzy znaki, które są stosowane w działaniu urządzeń peryferyjnych. Zawiera ona 60 wierszy i 60 kolumn. W każdym wierszu umieszczono 60 identycznych znaków emc z tym, że układ poszczególnych znaków w wierszu przesunięto w lewo o jeden znak. W ten sposób zapisana tablica kodów tworzy jednolity, wyjściowy układ do tworzenia kolejnych jej permutacji. Podstawową zasadą tworzenia kolejnych układów tablic jest dokonywanie permutacji w poszczególnych wierszach, bez prawa przenoszenia znaków

RAMKA		1	2	. . .	59	60
		A	B	. . .	:	?
1	A	A	B	. . .	:	?
2	B	B	C	. . .	?	A
:	:	:	:	TABLICA WŁAŚCIWA	:	:
59	:	:	?	. . .	<	=
60	?	?	A	. . .	=	:

LICZBA KLUCZY - PERMUTACJI :

$L_1 = (Z_w\ !)^2$ — ZMIENIAMY UKŁAD RAMKI

$L_2 = (Z_w\ !)^w$ — ZMIENIAMY UKŁAD TABLICY WŁAŚCIWEJ

$L_3 = (Z_w\ !)^2 * (Z_w\ !)^w$ — ZMIENIAMY UKŁAD CAŁEJ TABLICY KODÓW

GDZIE :

W - LICZBA WIERSZY

Z_w - LICZBA ZNAKÓW ELEMENTARNYCH W WIERSZU.

Rys. 17. Tablica kodów kryptograficznych

w kolumnach. Tablica kodów składa się z dwóch części: z ramki, w której dokonujemy oznakowania kolumn i wierszy, i z tablicy właściwej. W ramce znajduje się dwa razy po 60 znaków kodu KOI-8, służących do oznakowania kolumn i wierszy. Tablica właściwa składa się z 60 wierszy, z których każdy zawiera 60 znaków wspomnianego kodu. Tak zbudowaną tablicę można wykorzystać do szyfrowania informacji w trojaki sposób:

a) zmieniając układ ramki; przy nie zmienionym układzie tablicy właściwej otrzymujemy liczbę kombinacji

$$L_k = (W_z!)^2,$$

gdzie: W_z - liczba znaków elementarnych w jednym wierszu;

b) zmieniając układ tablicy właściwej; przy nie zmienionym układzie ramki otrzymujemy liczbę kombinacji

$$L_k = (W_z!)^W,$$

gdzie: W - liczba wierszy tablicy;

c) zmieniając jednocześnie układ ramki i tablicy właściwej, otrzymujemy liczbę kombinacji

$$L_k = (W_z!)^2 (W_z!)^W.$$

Układ tablic

$$\text{Szyfr} = \left(\boxed{\text{tablica kodów kryptograficznych}} + \boxed{\text{ciąg szyfrowy}} \right) \pmod M$$

Tablica kodów kryptograficznych - wartość stała
Ciąg szyfrowy - wartość zmienna

Model matematyczny szyfru

$$S_{wk} = \boxed{(a_{xz} + b_{ij}) \pmod M} \qquad (1)$$

S_{wk} - element ciągu szyfrowego dla
wiersza = $(x + i) \pmod M$
kolumny = $(z + j) \pmod M$

a_{xz} - znak z tablicy kodów kryptograficznych dla określonej permutacji, gdzie x = nr wiersza, z = nr kolumny

b_{ij} - znak z układu tablic zmiennych dla każdego znaku w określonym wierszu i kolumnie.

Model matematyczny deszyfracji

$$a_{xz} = S_{wk} - b_{ij} \qquad (2)$$

Uwaga: Przy wartościach zerowych i ujemnych dodać mod M.

Drugim elementem algorytmu jest przesyłana informacja - sam ciąg szyfrowy. Długość ciągu szyfrowego może być dowolna. W algorytmie cały ciąg szyfrowy podzielono na wiersze i kolumny. Liczba znaków w wierszu może wynosić od 1 do 120. Tworzą one jednocześnie liczbę kolumn. Liczba wierszy jest uzależniona od długości ciągu szyfrowego i przyjętej liczby znaków w wierszu. Na przykład jeżeli ciąg szyfrowy zawiera 100 znaków i przyjęto, że jeden wiersz zawiera 5 znaków, to w tablicy będzie 20 wierszy i pięć kolumn. Jeżeli jednak przyjmiemy 100 znaków w wierszu, to ten sam ciąg szyfrowy będzie się składał tylko z jednego wiersza i 100 kolumn.

Trzecim elementem jest tablica czasu. W tablicy czasu podane są lata, miesiące, dni, godziny i minuty. Służy ona dla opracowania odpowiedniej permutacji tablicy kodów kryptograficznych i rozpoczęcia szyfrowania. Służy ona również do umieszczania odpowiednich informacji w tzw. pilocie koniecznym do deszyfracji ciągu szyfrowego.

Metody UNITAKOD nie należy rozpatrywać wyłącznie jako metody szyfrowania informacji (chociaż to jest jej głównym celem). Metoda ta łączy zespół elementów składających się na całość. Do nich zaliczamy:

1. Ochronę komputera. Zarówno literatura zachodnia, jak i krajowa w zasadzie nie poruszają tego tematu podczas omawiania metod szyfrowania informacji. Najczęściej w literaturze fachowej znajdujemy wzmianki dotyczące ochrony komputera za pomocą metod organizacyjnych. Metoda UNITAKOD pomija tego typu ochronę z powodu jej małej skuteczności.

Jednocześnie przewiduje się zastosowanie systemu ewidencji i kontroli w programie zarządzającym (systemie operacyjnym), co przedstawiono w pracy [26].

2. Ochronę przetwarzanych informacji w komputerze, lub inaczej przetwarzanie zaszyfrowanej informacji. Problem ten jest dotychczas traktowany marginesowo i nie znalazł nawet teoretycznych rozwiązań. Metoda UNITAKOD przewiduje również zabezpieczenie informacji podczas jej przetwarzania. Zagadnienie to zostało szczegółowo przedstawione w dwóch monografiach [26], [27].

3. Identyfikacja nadawcy i odbiorcy. Problem ten jest ściśle związany z przesyłaniem informacji w sieciach komputerowych. Ten element szyfru jest jednym z głównych zagadnień metody UNITAKOD. Po raz pierwszy identyfikacja nadawcy i odbiorcy jest rozpatrywana w metodzie RSA - jawnego klucza, natomiast w metodzie UNITAKOD została zastosowana w 1987 roku. Identyfikacja wiąże się ściśle z szyfrowaniem nagłówka (adresu), co wymaga jednoczesnego stosowania dwóch rodzajów szyfrów (zagadnienie to zostanie omówione poniżej).

4. Szyfrowanie nagłówka (adresu) podczas przesyłania szyfrogramów w sieciach komputerowych. Możliwość ta wynika z następujących zasad metody UNITAKOD:

- stosowania trzech różnych tablic: zerowej, wyjściowej i szyfrowej,
- stosowania pilota zmieniającego swą postać szyfrową w zależności od czasu i zasad szyfrowania za pomocą tablicy zerowej lub wyjściowej.

Tablica zerowa jest tablicą kodów kryptograficznych, opracowaną przez generator permutacji, a stanowiącą podstawę generowania tablicy wyjściowej. Postać tablicy zerowej jest uzależniona od czasu pracy generatora. Liczbę tablic zerowych można określić wzorem $(W_k!)^{Ww}$, gdzie: W_k - liczba kolumn w jednym wierszu tablicy, W_w - liczba wierszy

w tablicy. Dzięki tej ogromnej liczbie różnych permutacji tablic zerowych otrzymujemy - przy zastosowaniu tego samego programu - różne permutacje tablic wyjściowych.

Tablica wyjściowa jest tworzona w momencie szyfrowania na podstawie modelu matematycznego:

$$S_{wk} = \left(a_{xz} + b_{ij} \right) \bmod M \qquad (3)$$

opisanego powyżej,

gdzie: $w = (x + i) \bmod M,$ (4)

$k = (z + j) \bmod M.$ (5)

W powyższym modelu matematycznym dokonano zapisu tablicy kodów kryptograficznych oraz tablicy ciągu informacji. Model ten pozwala na tworzenie trzech różnych tablic opisanych powyżej, gdyż możemy go zapisać jako sumę współrzędnych dla wartości x i y i wówczas model matematyczny przyjmuje postać:

$$SZYFR = (T_{xy} + W_{xy}) \bmod M,$$

gdzie: T_{xy} - współrzędne tablicy kodów kryptograficznych,

W_{xy} - współrzędne tablicy przesyłanej informacji.

Ponieważ zapisy (4) i (5) wyrażają sumę wartości dla x i y, dlatego po podstawieniu do wzoru (3) otrzymujemy

$$SZYFR_x = \left(T_x + W_x \right) \bmod M \qquad (6)$$

$$SZYFR_y = \left(T_y + W_y \right) \bmod M. \qquad (7)$$

Dzięki tak zastosowanej zasadzie posługiwania się wzorem (3) uzyskujemy możliwość:

a) jednoczesnego stosowania dwóch różnych szyfrów, a mianowicie: szyfru nr 1 do szyfrowania treści informacji - wzory (6) i (7) oraz szyfru nr 2, stosowanego do szyfrowania adresu, dla którego $W = \phi$;

b) wykorzystania metody UNITAKOD do przesyłania informacji w sieci komputerowej za pomocą protokołu ramowego (rys. 16). W protokole

ramowym zachodzi konieczność stosowania dwóch rodzajów szyfrów jednocześnie, co uzyskujemy stosując szyfr nr 1 do szyfrowania informacji w polu I oraz szyfr nr 2 do szyfrowania adresu w polu A;

c) identyfikacji nadawcy i odbiorcy za pomocą PILOTA przesyłanego w polu I i szyfrowanego za pomocą szyfru nr 2.

Tablica szyfrowa jest sumą obu tablic: wyjściowej tablicy kodów kryptograficznych i tablicy przesyłanej informacji. Zasada szyfrowania za pomocą tej tablicy jest ujęta we wzorach (1) i (2).

6. SKUTECZNOŚĆ METOD OCHRONY INFORMACJI

Metody ochrony mają gwarantować bezpieczną eksploatację informacji i zabezpieczyć je przed dostępem osób nie upoważnionych. Miarę tego zabezpieczenia nazywamy skutecznością zastosowanego algorytmu. Przez skuteczność rozumiemy stopień, w jakim dana metoda zabezpiecza zbiory informacji przed infiltracją. Wszystkie dotychczasowe obliczenia skuteczności określonej metody nie odzwierciedlają rzeczywistości, gdyż nie uwzględniono decydującej roli czynnika ludzkiego, co wykazano w pracy [29]. Dlatego skuteczność poszczególnych metod ochrony możemy rozpatrywać jako

- skuteczność teoretyczną,
- skuteczność rzeczywistą (praktyczną).

6.1. Teoretyczna skuteczność metody ochrony zbiorów

Użyteczność przedmiotu czy urządzenia jest podstawą ich zastosowania w praktyce. Przedmiot, który nie jest użyteczny, lub nie ma zabezpieczenia gwarantującego bezpieczeństwo jego użytkowania, staje się całkowicie nieprzydatny lub wręcz niebezpieczny w użyciu. Zbiory informatyczne mają swoisty rodzaj zabezpieczenia w postaci metod ochrony. [28].

Na podstawie sumy prawdopodobieństw zdarzeń przeciwnych można określić prawdopodobieństwo ochrony. Po rozpatrzeniu prawdopodobieństwa ochrony i prawdopodobieństwa infiltracji jako zdarzeń przeciwnych można zapisać:

$$P_o + P_i = 1,$$

gdzie P_o - prawdopodobieństwo ochrony zbiorów, P_i - prawdopodobieństwo infiltracji zbiorów.

Dlatego prawdopodobieństwo ochrony zbiorów wynosi $P_o = 1 - P_i$. Ze wzoru wynika, że należy określić prawdopodobieństwo infiltracji, aby znaleźć wielkość prawdopodobieństwa ochrony. Można tego dokonać, przeprowadzając n wykluczających się doświadczeń, które potwierdzą wystąpienie m przypadków infiltracji. Wówczas prawdopodobieństwo infiltracji wyniesie $P_i = m/n$. Podstawiając wartości P_i do wzoru określającego prawdopodobieństwo ochrony, otrzymujemy $P_o = 1 - m/n$.

Na podstawie powyższych rozważań dokonano obliczeń skuteczności programowych metod ochrony, które w ostatecznym rozrachunku wyrażają się liczbą bliską jedności: $P_o = 0{,}984$ oraz dla metod technicznych $P_o = 0{,}9997$.

Przytoczone obliczenia są bez wątpienia prawidłowe. Jeśli tak, to zachodzi pytanie dlaczego wobec tak dużej skuteczności różnych metod ochrony nie są one powszechnie stosowane [25] (odpowiedź na to pytanie jest zawarta w p. 6.2).

6.2. Rzeczywista skuteczność metod ochrony zbiorów

Metody ochrony ograniczają dostęp do systemu i nielegalne korzystanie z informacji. Żadna z tych metod nie występuje w praktyce w czystej postaci, gdyż wówczas byłaby mniej skuteczna. Dlatego jest konieczne stosowanie kompleksowego systemu ochrony, który jest uciążliwy i paraliżuje proces przetwarzania danych. Ponadto system kontroli, oparty tylko na uczciwości pracowników ośrodków obliczeniowych, może wpływać ujemnie na skuteczność zastosowanej metody ochrony.

Zaprezentowane w omawianym rozdziale metody ochrony zbiorów informatycznych zawierają dodatkowy składnik, który w dotychczasowych obliczeniach nie był uwzględniany. Po dokładnym przeanalizowaniu po-

szczególnych metod stwierdzamy, że każda z nich kryje w sobie c z y n n i k l u d z k i, który nie tylko, że istnieje, lecz spełnia w niej d e c y d u j ą c ą r o l ę. Czynnika tego nie należy bagatelizować, a tym bardziej nie wolno go pomijać, ponieważ odgrywa on szczególną rolę w określaniu rzeczywistej skuteczności zarówno poszczególnych metod, jak i kompleksowego systemu ochrony.

Nie uwzględniany do tej pory czynnik ludzki występujący we wszystkich metodach ochrony, nie ma określonego prawdopodobieństwa ochrony. Trudność polega na tym, że nie można podzielić ludzi na pewnych i niepewnych lub pewnych, mniej pewnych, niepewnych itp.

Rozpatrując jednak zagadnienie ochrony zbiorów informatycznych, jesteśmy zmuszeni określić jednoznacznie prawdopodobieństwo ochrony czynnika ludzkiego. W tym celu wykorzystujemy ponownie twierdzenie, że suma prawdopodobieństwa zdarzeń przeciwnych równa się jedności. Otrzymujemy wzór:

$$S_p + S_n = 1,$$

w którym S_p - skuteczność ochrony człowieka pewnego, S_p - skuteczność ochrony człowieka niepewnego,

stąd

$$S_p = S_n - S = 0,5.$$

Po podstawieniu otrzymanej wartości do dotychczasowych wzorów określających skuteczność mamy

$$P_o = 0,5(1 - P_i),$$

a wówczas rzeczywista skuteczność stosowanych metod ochrony będzie zawarta w granicach

$$\left[0,4 < P_o < 0,5\right].$$

Powyższy wzór jest słuszny wtedy, gdy mamy do czynienia z jedną metodą lub z jednym sposobem. Jednak stosując kilka sposobów lub

kompleksowy system ochrony, powinniśmy jego skuteczność określić funkcją trzech zmiennych. Wówczas skuteczność rzeczywista tegoż systemu zostanie wyrażona wzorem*:

$$f(x,y,z) = \frac{0,5}{n+m+t}\left[\sum_{i=1}^{n} a_i x_i + \sum_{j=1}^{m} b_j y_j + \sum_{k=1}^{t} c_k z_k\right],$$

w którym:

a_i - skuteczność ochrony zbiorów przy zastosowaniu i-tej metody organizacyjnej dla $i = 1,2,...,n$,

b_j - skuteczność ochrony zbiorów przy zastosowaniu j-tej metody technicznej dla $j = 1,2,...,m$,

c_k - skuteczność ochrony zbiorów przy zastosowaniu k-tej metody programowej dla $k = 1,2,...,t$,

przy ograniczeniach:

$$x_i = \begin{cases} 0 - \text{i-ta metoda (sposób) nie została użyta,} \\ 1 - \text{i-ta metoda (sposób) została użyta,} \end{cases}$$

$$y_j = \begin{cases} 0 - \text{j-ta metoda (sposób) nie została użyta,} \\ 1 - \text{j-ta metoda (sposób) została użyta,} \end{cases}$$

$$x_k = \begin{cases} 0 - \text{k-ta metoda (sposób) nie została użyta,} \\ 1 - \text{k-ta metoda (sposób) została użyta.} \end{cases}$$

Powyższe rozważania nad dotychczasowym określeniem skuteczności metod ochrony zbiorów, bez uwzględniania czynnika ludzkiego, są odpowiedzią na postawione na początku pytanie, dlaczego metody ochrony zbiorów, wobec tak dużej ich skuteczności, nie są powszechnie stosowane. Obliczenia rzeczywistej skuteczności tych metod gwarantują bezpieczeństwo zbiorów zaledwie w 50%, a nie jak wykazano w rozważaniach teoretycznych - w 99,9% [28], [29].

---

*Wzór został opracowany przez M. Nycz i A. Pieniążek w Instytucie Organizacji i Zarządzania PWr., a następnie uzupełniony o czynnik ludzki przez autora książki.

6.3. Ocena jakości szyfrowania

Informacje można utajnić zasadniczo dwoma sposobami: za pomocą kodowania i za pomocą szyfrowania. System szyfrowy polega na zastosowaniu algorytmów matematycznych tworzących procedury kryptograficzne. Są to operacje przyporządkowania danej informacji x_i szyfrogramów y_i za pomocą odwzorowania szyfrującego f_k, a zatem

$$y_i = f_k(x_i).$$

Operacją odwrotną do szyfrowania jest odczytywanie wiadomości x_i na podstawie szyfrogramu y_i za pomocą odwzorowania odwrotnego do szyfrowania, czyli f_k^{-1}. Operację taką nazywamy deszyfracją i zapisujemy jako

$$x_i = f_k^{-1}(y_i).$$

Zastanówmy się nad kryteriami jakości metod szyfrowania i ich mocą kryptograficzną. Shannon podał pięć kryteriów jakości metod szyfrowania:

1) tajność metody,

2) długość stosowanego klucza,

3) odporność metody na błędy w kanale oraz w urządzeniach szyfrujących i deszyfrujących,

4) wprowadzona przez szyfrowanie nadmiarowość,

5) prosta realizacja metody szyfrowania.

Ad 1) Zgodnie z kryterium tajności metody należy przyjąć założenie wprowadzone do kryptologii jeszcze w XIX wieku przez Augusta Kerckholla, że nieprzyjaciel zna metodę szyfrowania, deszyfrowania i zbiór kluczy. Przyjmuje się także inne założenia dotyczące nieprzyjaciela, a mianowicie, że zna on również język, w którym są zapisane wiadomości i typ szyfrowanych wiadomości (wojskowe, gospodarcze itp.), zna budowę urządzeń kryptograficznych, budowę i organizację komputerów oraz ich

oprogramowanie, dysponuje komputerem o odpowiedniej szybkości. Gdy metoda szyfrowania jest wszystkim znana, a nieprzyjaciel przechwycił pewien szyfrogram i nie zna wiadomości przesyłanej przez szyfrogram ani klucza, za pomocą którego zaszyfrowano wiadomość, to aby określić szyfrogram przy znanej metodzie, musi znać klucz. Tak więc informacja jest zabezpieczona jedynie przez utrzymanie w tajemnicy jednego z kluczy wybranego z całego zbioru. A zatem z punktu widzenia użytkowników systemu przesyłania wiadomości z szyfrowaniem byłoby dobrze, gdyby prawdopodobieństwo przechwycenia lub osiągnięcia klucza było jak najmniejsze. Im liczniejszy będzie zbiór kluczy, tym trudniej będzie nieprzyjacielowi złamać dany system kryptograficzny. W związku z tym liczność zbioru kluczy bywa nazywana mocą kryptograficzną systemu utajniania i stanowi jeden z najważniejszych parametrów charakteryzujących systemy kryptograficzne.

Ad 2) Kryterium długości klucza uwzględnia szczególnie warunki nałożone na kanał "klucza", który powinien być trudno dostępny dla nieprzyjaciela i co najmniej tak "szybki", jak kanał szyfrogramu. Jednoczesne spełnienie tych dwóch warunków prowadzi do tego, że nazwa kanał "klucza" jest umowna, tzn. nie jest to kanał telekomunikacyjny. Mając taki kanał telekomunikacyjny trudno dostępny dla nieprzyjaciela można by go wykorzystać do przesyłania wiadomości, nie klucza. W praktyce realizacja takiego "kanału" wygląda w ten sposób, że nadawca wiadomości i jej odbiorca mają wykazy kluczy. Wykorzystuje się je w ten sposób, że nadawca i odbiorca wiadomości wiedzą, od którego klucza zaczyna się przekazywanie wiadomości i co jaki czas zmienia się klucz (np. co godzinę, po 100 przesłanych znakach wiadomości itp.).

Długość klucza, obok liczby kluczy, stanowi ważny parametr charakteryzujący system kryptograficzny. Im klucz jest dłuższy, tym trudniejszy jest proces dekryptażu, który polega na odtworzeniu klucza. Bardzo długie

klucze, tzw. klucze "nieskończone", można otrzymać za pomocą stosunkowo prostych algorytmów np. wykorzystując generator znaków pseudolosowych.

Ad 3) Kryterium odporności metody na błędy jest istotne z tego powodu, że w danym systemie telekomunikacyjnym nie występują zakłócenia. W każdym rzeczywistym systemie błędy takie występują i trzeba się z nimi liczyć przy projektowaniu urządzeń szyfrujących. Metoda szyfrowania nie może wprowadzać zbytniej zależności między poszczególnymi wiadomościami elementarnymi w szyfrowaniu, aby błąd w jednej z nich nie powodował błędu odczytania innych wiadomości lub nawet uniemożliwiał ponowne ich odczytanie.

Ad 4) Kryterium nadmiarowości jest istotne ze względu na czas i koszt nadawania szyfrogramu. Dąży się do tego, aby stosowana metoda nie wprowadzała zbyt dużej nadmiarowości, która również może być źródłem informacji o wiadomości, a tym samym może ułatwić odczytanie szyfrogramu przez nieprzyjaciela.

Ad 5) Kryterium prostoty metody jest ściśle związane z trudnymi warunkami, w jakich często pracują urządzenia szyfrujące. Jest ono związane z kosztami tych urządzeń i z częstą zmianą stosowanego w czasie pracy klucza, a nawet metod szyfrowania. Im prościej realizuje się szyfrowanie, tym lepsza i tańsza jest dana metoda.

6.4. Kryteria jakości systemów utajniania

Moc kryptograficzna systemów utajniania jest mierzona różnymi wielkościami, m.in. za pomocą liczby wariantów klucza, tj. liczbą kluczy, za pomocą prawdopodobieństwa złamania klucza szyfru, czyli tzw. dekryptażu lub przez entropię klucza. Wartość tego kryterium jakości szyfrowania znalazła swoje potwierdzenie w rozważaniach teoretycznych Shannona i Sedlera.

Kryteria jakości systemów utajniania można podzielić na dwie grupy:

a) teoretyczne, które wywodzą się z analizy systemów kryptogragicznych metodami teorii informacji i statystycznej teorii podejmowania decyzji; zaproponowali je Shannon i Seidler,

b) praktyczne, oparte na ocenie ilości pracy i środków, które musi zastosować kryptoanalityk, aby złamać szyfr. Jako praktyczne kryterium jakości przyjmuje się eksperymentalnie określoną liczbę operacji matematyczno-logicznych, które są konieczne do złamania systemu lub - przy założeniu mocy obliczeniowej, jaką dysponuje kryptoanalityk - równoważny czas łamania systemu. Kryteria te noszą nazwę kryteriów ilości pracy.

6.5. Moc kryptograficzna według C.E. Shannona

Shannon wprowadził dwa teoretyczne kryteria jakości systemów kryptograficznych, tj. a) średnią entropię warunkową klucza H(K/Y) i b) wiadomości H(X/Y). W obu przypadkach warunkiem jest znajomość szyfrogramu o długości N. Najpierw określił on "szyfr doskonały" i na tej podstawie przyjął - jako kryterium jakości metody szyfrowania - entropię warunkową zmiennej losowej, reprezentującej prawdopodobieństwo odgadnięcia klucza przy warunku przechwycenia określonego szyfrogramu. Entropia w teorii szyfrów oznacza miarę nieokreśloności zdarzeń zachodzących w określonym stanie między pewnymi zjawiskami wzajemnie wykluczającymi się. Jest ona - według Shannona - związana z liczbą uzyskanej informacji, dzięki której zmniejsza się stopień nieokreśloności.

Przyjmijmy, że jesteśmy nieprzyjacielem i znamy metodę szyfrowania zastosowaną przez system łączności, który podsłuchujemy. Wówczas z naszego punktu widzenia zastosowanie określonego klucza przez nadajnik może być opisane za pomocą zmiennej losowej. Znając metodę szyfrowania, możemy określić a priori prawdopodobieństwo pojawienia się po-

szczególnych kluczy. Gdy przechwycimy szyfrogram, to chcielibyśmy doprowadzić do takiej sytuacji, w której prawdopodobieństwo zastosowania jednego z kluczy jest równe jedności, zaś prawdopodobieństwo zastosowania pozostałych kluczy jest równe zero. Wynika z tego, że na podstawie szyfrogramu można jednoznacznie określić klucz, a tym samym przechwycić przesłaną wiadomość. Widać zatem, że bardzo interesującym wskaźnikiem jakości mogłoby być prawdopodobieństwo otrzymania klucza przy warunku przechwycenia szyfrogramu.

Dla użytkownika takiego systemu łączności byłoby dobrze, gdyby przechwycenie szyfrogramu nie dawało możliwości innego rozkładu prawdopodobieństwa kluczy niż rozkład a priori. Za szyfr "doskonały" Shannon uznał taki szyfr, dla którego prawdopodobieństwo otrzymania klucza przy warunku przechwycenia szyfrogramu jest równe prawdopodobieństwu pojawienia się a priori poszczególnych kluczy. Przy badaniu takiego prawdopodobieństwa interesuje nas w zasadzie tylko jego nieokreśloność, która jest tym większa, im rozkład ten jest bliższy rozkładowi a priori, i tym mniejsza, im lepiej możemy określić poszukiwany klucz. Syntetyczną miarą tak rozumianej nieokreśloności rozkładu jest średnia entropia warunkowa klucza, którą oznaczmy jako $\overline{H}(K/Y)$.

Dla dostatecznie dużych N, a więc dla odpowiednio dużej próbki nieokreśloność klucza jest równa lub bliska zeru, co oznacza że klucz jest znany. Wynika z tego (podstawowy wniosek Shannona), że każdy szyfr można złamać, jeśli się zna metodę szyfrowania i dysponuje dostatecznie dużą liczbą szyfrogramów. Systemy kryptograficzne, dla których $\overline{H}(K/Y)$ i $\overline{H}(X/Y)$ nie zmierzają do zera przy $N \to \infty$, a klucze mają nieskończoną długość, są nazywane idealnymi. Gdy nie przechwycono szyfrogramu, tzn. dla $N = 0$, mamy $\overline{H}(K/Y = H(K)$ i wówczas system nazywamy ściśle idealnym. Z powyższej definicji wynika, że dla systemu ściśle idealnego ilość

informacji o kluczu, których dostarczono kryptoanalitykowi szyfrogram $I(K:Y) \stackrel{df}{=} H(K) - \overline{H}(K/Y)$ jest równa zeru niezależnie od długości szyfrogramu.

Wielkość $H(K)$ to entropia prawdopodobieństwa a priori kluczy. Przy założeniu, że klucze są równo podobne, entropia ta jest tym większa, im więcej jest możliwych kluczy, a więc gdy większa jest moc kryptograficzna szyfru.

6.6. Moc kryptograficzna według J. Seidlera

Inną metodę podejścia do zagadnienia zaproponował Seidler. Przy założeniu, że nieprzyjaciel zna sygnał nadawany i zasadę przyporządkowania go kluczowi i wiadomości, klucz jest dla niego nie znanym zniekształceniem. Zniekształcenie to można traktować jako przypadkowe o rozkładzie prawdopodobieństwa bądź znanym a priori, bądź wyznaczonym za pomocą teorii gier, jako rozkład najbardziej pesymistyczny. Zatem dla nieprzyjaciela zaszyfrowany sygnał ma taki sam charakter jak sygnał, który uległ w kanale przypadkowym bardzo silnym i skomplikowanym zniekształceniom. W takiej sytuacji jako kryterium jakości systemu kryptograficznego Seidler proponuje przyjąć ryzyko optymalnej resuły decyzyjnej stosowanej przez nieprzyjaciela (kryptoanalityka), który klucz traktuje jako przypadkowe zniekształcenie.

Przy założeniu, że dla zbiorów wiadomości, szyfrogramów i kluczy można określić rozkłady prawdopodobieństwa, Seidler wprowadził następującą zależność, która określa ilość informacji o wiadomości dostarczonej kryptoanalitykowi przez szyfrogram:

$$I(X:Y) = H(Y) - \overline{H}(Y/X) = H(Y) - \overline{H}(Y/K) + \overline{H}(Y/K) - \overline{H}(Y/X).$$

Korzystając z zależności przedstawionych poniżej, Seidler przekształcił wzór do postaci

$$I(X : Y) = I(K : Y) + H(X) - H(K) + n_k ,$$

w której:

$I(X:Y)$ - ilość informacji o wiadomości dostarczonej kryptoanalitykowi przez szyfrogram,

$I(K:Y)$ - ilość informacji statystycznej o kluczu niesionej przez szyfrogram

$$I(K:Y) = H(Y) - \overline{H}(Y/K),$$

$H(X)$ - entropia rozkładu prawdopodobieństwa wiadomości,

$H(K)$ - entropia rozkładu prawdopodobieństwa klucza,

$\overline{H}(Y/K)$ - średnia entropia warunkowa szyfrogramów, gdy jest ustalony klucz.

Biorąc pod uwagę, że średnia entropia warunkowa pary X, K przy warunku ustalonej informacji X równa się entropiii klucza K

$$\overline{H}(X, K/X) = H(X)$$

mamy $\overline{H}(Y/K) = \overline{H}(Y, K/K) = \overline{H}(X, K/K) = H(X)$.

Jest to zależność oczywista: jeżeli jest ustalony klucz, to nieokreśloność szyfrogramów jest spowodowana jedynie przez nieokreśloność wiadomości, a przy tym klucz i szyfrogram określają jednoznacznie informację

n_k - oznacza wskaźnik niewykorzystania kluczy, który charakteryzuje efektywność wykorzystania kluczy:

$$n_k \geqslant 0,$$

$\overline{H}(Y/X)$ - średnia entropia warunkowa szyfrogramu, gdy ustalona jest wiadomość,

$$\overline{H}(Y/X) = \overline{H}\left[f(X,K)/X\right] \leqslant \overline{H}\left[(X,K)/X\right] = H(K).$$

Tak więc entropia szyfrogramów Y przy warunku, że jest ustalona informacja X, nie jest większa od entropiii klucza. Wniosek ten przy założeniu, że w kanale nie ma szumu, jest oczywisty. Mianowicie nieokreśloność szyfrogramu Y przy ustalonej wiadomości jest spowodowana jedynie przez nieokreśloność klucza. W skrajnym przypadku, gdy szyfrogramu nie uzależniamy od klucza, mielibyśmy

$$\bar{H}(Y/X) = 0.$$

Stąd właśnie parametr

$$n_k = H(K) - \bar{H}(Y/X)$$

określa niewykorzystanie klucza w szyfrowaniu.

Jako użytkownicy systemu telekomunikacyjnego chcielibyśmy, aby szyfrogram nie niósł nieprzyjacielowi żadnej informacji o wiadomości, czyli chcielibyśmy, aby

$$I(X : Y) = 0.$$

Z tego warunku wobec $n_k \geqslant 0$ otrzymujemy

$$H(X) + I(K:Y) - H(K) \leqslant 0$$

$$H(X) \geqslant 0 \quad \text{i} \quad I(K : Y) \geqslant 0.$$

A więc entropia rozkładu prawdopodobieństwa kluczy $H(K)$ musi być jak największa, aby była spełniona wymagana nierówność. Stwierdzenie to jest jednoznaczne z warunkiem, aby moc kryptograficzna szyfru była jak największa, bowiem nie ma wpływu na oba dodatnie składniki analizowanej sumy.

Tak więc warunkiem koniecznym, aby szyfr był idealny, tzn. do tego, aby $I(X:Y) = 0$, jest

$$H(X) \leqslant H(K),$$

a więc warunkiem, by szyfrogram nie dostarczał informacji statystycznej o wiadomości jest nie mniejsza entropia klucza niż entropia informacji.

Z przeprowadzonej analizy jakości metod szyfrowania wynika, że o jakości szyfru decydują następujące czynniki:

1) liczba kluczy,

2) prawdopodobieństwo dekryptażu,

3) entropia klucza.

Wymienione trzy parametry jakościowej oceny szyfrów są ściśle ze sobą związane i żaden z nich nie może być pominięty przy ocenie szyfru.

6.7. Skuteczność nowoczesnych metod ochrony informacji

Jak wspomniano w poprzednim rozdziale, zarówno kryteria ocen, jak i zasady dotyczące liczby kluczy oraz entropia klucza nie mogą być stosowane w ocenie nowoczesnych metod ochrony. Wynika to z tej prostej przyczyny, że podczas szyfrowania za pomocą komputera, w oparciu o różne modele matematyczne, mamy do czynienia z pominięciem klucza jako elementu szyfrującego. Również amerykańska metoda RSA przewiduje zastosowanie innego klucza do szyfrowania a innego do deszyfracji. Fakt ten trudno jest nazwać stosowaniem klucza szyfrującego, tym bardziej że metoda opiera się na określonym modelu matematycznym. Znając ogólne zasady oceny szyfrów, zastanówmy się nad mocą kryptograficzną nowoczesnych metod szyfrowania.

Amerykańska metoda "RSA - jawnego klucza" została oparta na liczbach pierwszych "p" i "q", które stanowią grupę liczb tajnych oraz na ich iloczynie "n", którego wartość jest jawna. Dlatego do złamania klucza zastosowanego w metodzie RSA konieczna jest znajomość wartości "p" i "q". Znając iloczyn "n" tych liczb, można obliczyć w dwojaki sposób ich wartość.

1) Mnoży się kolejne liczby pierwsze (na zasadzie każda z każdą), aby znaleźć liczby pierwsze przy znanej wartości ich iloczynu "n", aż do otrzymania określonego iloczynu "n". Jest to metoda najdłuższa i nie zawsze prowadzi do celu.

2) Pobiera się kolejne liczby pierwsze i dzieli iloczyn przez liczbę pierwszą aż do otrzymania wyniku bez reszty. Wówczas dzielnik przyjmujemy jako jedną, a wynik dzielenia jako drugą liczbę pierwszą. Ta metoda, chociaż jest dość długa, daje jednak lepsze rezultaty.

Autorzy metody RSA uważają jednak, że znalezienie wartości "p" i "q",

czyli klucza metody, jest niemożliwe przy dużych wartościach tych liczb. Szkopuł w tym, że duże liczby pierwsze sprawiają spore kłopoty podczas szyfrowania, dlatego nie zawsze i nie wszędzie mogą być stosowane. Ze względu na możliwość łamania szyfru w metodzie RSA błędem byłoby stosowanie wprost jednego z wyżej podanych sposobów. Poznanie zasad szyfrowania w metodzie RSA umożliwiło podjęcie licznych prób znalezienia klucza szyfrowego. Jest to trzeci sposób, który pragnę opisać dokładniej.

Z przeprowadzonej analizy liczb pierwszych wynikają następujące wnioski:

- końcówki liczb pierwszych (ostatnie ich cyfry) są zawsze cyfrą nieparzystą, pomijając cyfrę 2,

- iloczyn liczb pierwszych, chociaż nigdy nie jest liczbą pierwszą, ma zawsze końcówkę nieparzystą,

- cyfrę 2, która jest zaliczana do liczb pierwszych, należy zdecydowanie odrzucić z metody szyfrowania, gdyż iloczyn dwójki z dowolną liczbą pierwszą będzie zawsze liczbą parzystą. Rozszyfrowanie klucza jest w tym przypadku dziecinnie proste,

- cyfra 5, zaliczana również do liczb pierwszych, występuje również w grupie tych liczb jeden raz (można tej wartości nie brać pod uwagę),

- z analizy liczb pierwszych i ich iloczynów wynika:

a) w przypadku iloczynu "n" kończącego się cyfrą 5, jesteśmy pewni, że jedna liczba ma końcówkę 5, a druga 7,

b) każda wartość "n" może mieć wyłącznie jedną z końcówek 1, 3, 7 i 9,

Wartości końcówek liczb pierwszych i ich iloczynu:		
Wartość końcówki "n"	Możliwość kombinacji końcówek: p	q
1	1	1
	3	7
	9	9
3	1	3
	7	9
7	1	7
	3	9
9	1	9
	3	3
	7	7

c) określona końcówka "n" ma ściśle określone końcówki liczb pierwszych "p" oraz "q" (patrz wartości końcówek liczb pierwszych i ich iloczynu),

- analiza zbioru wszystkich liczb wykazała, że procentowa zawartość zbioru liczb pierwszych w całym zbiorze liczb, z którego one pochodzą stanowi średnio 10,6%. Ponadto końcówki liczb pierwszych 1, 3, 7 i 9, są rozłożne w zbiorze równomiernie i stanowią po około 25% zbioru,

- z analizy posiadanych informacji wynika, że nie przyjmuje się różnych długości liczb pierwszych dla "p" oraz "q". Istotą szyfru jest stosunkowo duży rząd wartości "n". Aby ten warunek był spełniony, nie należy łączyć np. jednej liczby pierwszej posiadającej trzy cyfry z drugą siedmiocyfrową, gdyż w takim przypadku wartość "n" może zawierać również tylko siedem cyfr. Najlepiej jest przyjmować wartość "n" czternastocyfrową. Ta uwaga ma istotne znaczenie przy łamaniu klucza.

Podsumowując dotychczasową analizę liczb pierwszych oraz posiadane informacje na temat szyfru RSA, możemy napisać ogólny wzór na

obliczanie wartości "p" i "q" przy znanej wartości ich iloczynu "n":

$$n/x = y,$$

w którym: n - iloczyn "p" i "q",

x - liczba pierwsza z określoną końcówką,

y - znalezione wartości długiej liczby pierwszej.

Dla uściślenia wzoru dokonajmy analizy liczby "x" oraz wypiszmy wzory, którymi należy posługiwać się w określonych przypadkach.

Przypadek pierwszy: gdy liczba "n" ma końcówkę jeden, wówczas stosujemy wzór:

a) $y = n/x_1$, c) $y = n/x_9$,

b) $y = n/x_3$,

w którym: x_1 oznacza liczbę pierwszą z końcówką jeden.

Przypadek drugi: gdy liczba "n" ma końcówkę trzy, wówczas stosujemy wzór:

a) $y = n/x_1$,

b) $y = n/x_7$.

Przypadek trzeci: gdy liczba "n" ma końcówkę siedem, wówczas stosujemy wzór:

a) $y = n/x_1$,

b) $y = n/x_3$.

Przypadek czwarty: gdy liczba "n" ma końcówkę dziewięć, wówczas stosujemy wzór:

a) $y = n/x_1$,

b) $y = n/x_3$,

c) $y = n/x_7$.

W oparciu o powyższą analizę systemu RSA pragnę podać kilka przykładów obliczania wartości "p" i "q" dla znanej "n".

Przykład 1

n = 5959, dlatego dla końcówki $n_k = 9$ stosujemy wzór

$$y = 5959/x_9$$

i otrzymujemy p = 59 oraz q = 101.

Przykład 2

n = 23.711, dlatego dla końcówki $n_k = 1$ stosujemy wzór

$$y = 23.711/x_1$$

i otrzymujemy p = 131 oraz q = 181.

Przykład 3

n = 114.137, dlatego dla końcówki $n_k = 7$ otrzymujemy wzór

$$y = 114.137/x_1$$

i otrzymujemy p = 311 oraz q = 367.

W punkcie 5.2 pokazano sposób deszyfracji i identyfikacji bez analizy możliwości znalezienia wartości klucza "b". Również w tym punkcie pokazano, że klucz otrzymujemy ze wzoru $u * b = 1 \pmod t$. Taka możliwość znalezienia klucza zachodzi wówczas, gdy jawna wartość "u" jest identyczna z tajną wartością "x", czyli u = x. W każdym innym przypadku ściśle tajny klucz "b" znajdujemy ze wzoru

$$b * x = 1 \pmod t,$$

czyli

$$\frac{b * x}{\mod t} = 1,$$

gdzie: x - ściśle tajna wartość służąca do znalezienia klucza "b", na podstawie wzoru $x = u \pmod t$.

Podstawiając wzór dla "x" do wzoru dla określenia klucza "b" otrzymujemy

$$b = \frac{t}{x}.$$

Ponieważ $x = u \pmod t$, co możemy zapisać jako: $x = \frac{u}{t}$, a po podstawieniu do wzoru $b = \frac{t}{x}$, otrzymujemy

$$b = \frac{1}{x} .$$

Podsumowując powyższą analizę, otrzymujemy dwa wzory na znalezienie ściśle tajnego klucza "b"

$$x = u \pmod t$$

w którym: $t = (p - 1)(q i 1)$, które to wartości podstawiamy do wzoru końcowego $b = \frac{1}{x}$.

Kolejną metodą nowoczesnego szyfrowania informacji jest metoda UNITAKOD, w której pominięto zasadę szyfrowania za pomocą klucza. Do szyfrowania wykorzystano model matematyczny będący sumą dwóch czynników, zmieniających się w zależności od czasu. Jest to metoda szyfrowania dynamicznego w odróżnieniu od dotychczasowych metod statycznych. Zastosowaną sumę dwóch czynników można zapisać jako

$$SZYFR = A_{xy} + B_{xy},$$

oraz

$$SZYFR_{(x)} = A_x + B_x,$$

$$SZYFR_{(y)} = A_y + B_y.$$

Dzięki zastosowaniu sumy dwóch czynników można jednocześnie otrzymać różne szyfry:

$$SZYFR_1 = A_{xy} + B_{xy}$$

$$SZYFR_2 = A_{xy} + \phi$$

$$SZYFR_3 = \phi + B_{xy}.$$

Możemy również określić liczbę tablic zerowych. Ponieważ tablica kodów kryptograficznych składa się z odpowiedniej liczby wierszy "W" oraz odpowiedniej liczby znaków w wierszu W_z, dlatego liczbę permutacji dla jednego wiersza wyznacza wzór $(W_z!)$. Uwzględniając ramkę tablicy oraz ilość wierszy tablicy, otrzymujemy wzór na liczbę tablic zerowych określonych liczbą permutacji tablicy:

$$L_p = (W_z!)^2 * (W_z!)^W.$$

Każda permutacja tworzy tablicę zerową, która jest podstawą do utworzenia odpowiedniej liczby tablic wyjściowych, dlatego otrzymujemy wzór końcowy dla liczby tablic (permutacji) wyjściowych:

$$L_{pw} = \left[(W_z!)^2 * (W_z!)^W\right]^2 .$$

Podstawiając wielkości liczbowe tablicy kodów kryptograficznych, otrzymujemy:

$$L_{pw} = \left[(256!)^2 * (256!)^{256}\right]^2 .$$

Wzór powyższy dotyczy wyłącznie określenia liczby permutacji tablic wyjściowych. Niezależnie od tej ogromnej liczby permutacji należy uwzględnić jeszcze tablicę przesyłanej informacji. Przyjmując średnią liczbę 120 znaków druku w wierszu oraz 10.000 wierszy przesyłanej informacji (firma IBM przyjmuje maksymalną liczbę stron druku w programach standardowych 9999, po 60 wierszy na stronie, co równa się 599.940 wierszy), otrzymujemy liczbę znaków równą $L_z = 120 * 10.000$. Ponieważ generator permutacji określa dowolnie (w zakresie wielkości L_z) liczbę znaków w wierszu, która odpowiada liczbie kolumn, natomiast długość meldunku i wygenerowana liczba kolumn określa liczbę wierszy, otrzymujemy liczbę permutacji tablicy przesyłanej informacji. Połączenie obu możliwych permutacji daje ogólną kombinację wszystkich permutacji związanych z szyfrowaniem za pomocą metody UNITAKOD.

Uważam, że dokładne obliczenia tych wielkości są zbędne, a chyba i niemożliwe. Jednak aby zobrazować czas konieczny do rozszyfrowania przechwyconego szyfrogramu zaszyfrowanego metodą Vernama, warto przytoczyć obliczone przez Sokołowskiego [23, s. 89-90] dane dotyczące liczby kluczy $504.7 * 10^{18}$. Dla tej liczby kluczy deszyfracja na komputerze o szybkości 1.000.000 operacji na sekundę trwałaby aż $265 * 10^6$ lat. Ponieważ liczba permutacji w metodzie UNITAKOD jest wielokrotnie większa, prowadzenie dalszych dowodów na moc kryptograficzną tej metody należy uznać za zbędne.

7. JAWNOŚĆ W METODACH OCHRONY

Przed analizą zagadnienia jawności metod ochrony należałoby rozstrzygnąć, jakie są różnice pomiędzy poufnością i bezpieczeństwem, bezpieczeństwem i tajnością oraz tajnością i nienaruszalnością. Na wstępie podano definicję wymienionych pojęć bez analizy powiązań między nimi. Problem poufności nie jest związany z komputerem i nie powstał wraz z maszyną cyfrową. Poufność dotyczy człowieka, dotyczy prawa człowieka, który decyduje jakimi informacjami chce się podzielić z innymi ludźmi. Natomiast bezpieczeństwo dotyczy zabezpieczenia środków technicznych i programów przed dostępem nie upoważnionych osób. Nie ma bezpośredniego związku pomiędzy poufnością a bezpieczeństwem. Gdyby ktoś skonstruował doskonale bezpieczny komputer, mógłby on pracować samodzielnie i to z pogwałceniem wszelkich praw poufności.

W codziennym życiu traktuje się zagadnienie tajności i bezpieczeństwa jako pojęcia równoznaczne. Łączenie tych dwóch pojęć jest podstawowym błędem. Tajność jest pojęciem dotyczącym danych. Jest ono atrybutem opisującym stopień ochrony, której podlegają dane. Przez poufność rozumie się, że nie ujawniony system zapewni maksymalną jego odpomość na infiltrację. Siła tego rozumowania opiera się na konieczności poszukiwania dróg dojścia do systemu ochrony. Słabą jego stroną jest niedocenianie przeciwnika, który potrafi prędzej wybrać słaby punkt systemu ochrony, nawet przy maksymalnym zabezpieczeniu, niż wykazują to analitycy i krytycy systemu. Można stwierdzić, że tajność - a raczej utajnianie - systemu ochrony nie gwarantuje bezpieczeństwa.

Trzeci problem to tajność i nienaruszalność. Oba te pojęcia dotyczą danych. Często mylimy je z pojęciem wykradania informacji lub bezprawnego odczytywania. Otóż tajność opisuje stan ochrony danych, natomiast

nienaruszalność oznacza pewną cechę danych, która gwarantuje, że dane są wiernią kopią informacji zawartej w dokumentach źródłowych.

Przy opracowaniu systemu ochrony informacji można próbować utrzymać w tajemnicy zastosowane zabezpieczenie. Lepiej jednak przeprowadzić jego wszechstronną analizę, ujawnić braki i błędy, a następnie dokonać odpowiednich korekt i dopiero wdrożyć system. Jeżeli jednak po wdrożeniu systemu nie można go podać do publicznej wiadomości, to znaczy, że nie zabezpiecza on wystarczająco informacji. Jeżeli natomiast projekt jest dobry, wówczas można go opublikować w całości (z wyjątkiem danych wejściowych i generatorów znaków losowych). W świetle tych kilku uwag dokonajmy analizy metod ochrony.

W stosowanych metodach organizacyjnych opracowuje się tak zwany plan ochrony systemu komputerowego, który przewiduje analizę potrzeb ochrony, opis ośrodka obliczeniowego i zakładu, opis obiegu dokumentów, czas realizacji poszczególnych systemów komputerowych, wykaz osób upoważnionych do przetwarzania danych określonego systemu, wykaz personelu obsługującego system, wykaz osób współpracujących i przygotowujących dane do systemu itd. Wszystkie wymienione elementy są najczęściej ściśle tajne i podlegają odpowiedniemu zabezpieczeniu. Obok tajnych, systemów informatycznych tworzy się tajną dokumentację systemu ochrony.

Inna metoda to zabezpieczenie techniczne. W zasadzie układy zabezpieczające dotyczą identyfikacji osoby upoważnionej za pomocą kart, żetonów czy tasiemki papierowej a nawet magnetycznej, znaków przy urządzeniach końcowych oraz systemów alarmowych. Wszystkie te elementy mają odpowiednią tajną ewidencję, tajne instrukcje oraz odpowiednią tajną instrukcję ochrony zabezpieczeń technicznych.

Metody programowe zawierają najczęściej odpowiednie procedury wymagające podania przez użytkownika hasła, informacji początkowej umożliwiającej dostęp do zbiorów itp. Dpracowane tego typu programy zabezpieczające wymagają odpowiedniej ewidencji rejestracji i dodatkowego zabezpieczenia. Wszystkie powyżej wymienione metody wchodzą w skład kompleksowego systemu ochrony, dlatego pomijam całą analizę tego systemu. Ogólnie można stwierdzić, że dotychczasowe systemy ochrony wymagają odpowiedniej rejestracji, dokumentacji i ścisłego utajniania. Jest to czynnik tworzący dodatkowy system utajniania samych metod ochrony informacji. Nic więc dziwnego, że metody ochrony informacji nie znalazły praktycznego zastosowania, gdyż - z jednej strony - były mało skuteczne, a z drugiej paraliżowały pracę całego ośrodka obliczeniowego.

Po zapoznaniu się z zasadami jawności w metodach ochrony, zastanówmy się nad jawnością w metodach szyfrowania informacji. Do znanych metod należy zaliczyć: szyfr Cezara, szyfr Viegenera, szyfr Vernama, metodę RSA - jawnego klucza oraz metodę UNITAKOD. Rozpatrzmy kolejno każdą z metod pod względem możliwości ujawnienia zasad szyfrowania.

SYSTEM CEZARA polega na zastępowaniu znaków alfabetu, innymi znakami tegoż alfabetu. Zasada szyfrowania polega na tym, że znakom alfabetu przyporządkowuje się liczby, przy czym numerację możemy rozpocząć od dowolnie wybranej litery. Następnie przyjmujemy dowolnie obraną wartość N, którą systematycznie dodajemy do liczby określonego znaku. Otrzymany wynik obliczamy według wartości modulo M. Z podanych zasad szyfrowania żadna nie może być ujawniona. Znając wielkość N, można stosunkowo łatwo dokonać deszyfracji, gdyż liczba permutacji dwudziestu czterech znaków alfabetu wynosi 24!. Dlatego metoda wyma-

gała utajnienia w całości, a konkretne zasady szyfrowania trzymane były w tajemnicy.

SZYFR VIEGENERA polega również na numerowaniu znaków alfabetu, do których dodaje się, według modulo M, odpowiednie wielkości klucza. Mamy tu do czynienia z kluczem, którego treść wymaga odpowiedniej ochrony. Deszyfracja w tym przypadku polega na poszukiwaniu treści klucza. Kluczem jest zawsze określone słowo, dlatego wraz z długością ciągu szyfrowego rośnie liczba powtórzeń klucza. To systematyczne powtarzanie się klucza dostarcza przeciwnikowi informacji o samym kluczu. Dlatego Seidler [18] uważa, że szyfr Viegenera nie może być uznany za szyfr doskonały. Nie można tu mówić nawet o jawności metody, gdyż przy pełnym jej utajnieniu, ona sama się deszyfruje w miarę częstotliwości i długości przesyłanych szyfrogramów.

SZYFR VERNAMA jest w zasadzie podobny do szyfru Viegenera z tą różnicą, że zastosowano w nim odpowiednio długi klucz. Jest to szyfr dla ciągów o długości N, dla których musi być spełniony warunek N K, gdzie: N - długość ciągu szyfrowego, K - długość klucza. Jeśli warunek ten nie zostanie dotrzymany, występuje zjawisko zachodzące w szyfrach Viegenera, czyli powtarzanie się klucza. Również przy zastosowaniu szyfru Vernama obowiązuje zasada tajności klucza.

We wszystkich metodach szyfrowania za pomocą klucza obowiązuje zachowanie ścisłej tajemnicy kluczy. Natomiast deszyfracja lub tak zwane łamanie szyfru polega na znalezieniu klucza. Odmiennie przedstawia się to zagadnienie w nowoczesnych metodach szyfrowania. Rozpatrzmy jawność w metodzie, która się nazywa metodą jawnego klucza.

METODA RSA - JAWNEGO KLUCZA. Co prawda nazwa jej sugeruje jawność klucza, w rzeczywistości ani metoda, ani klucz nie są jawne

(metodę RSA i zasady szyfrowania omówiono w p. 5.3). Obecnie przeanalizujemy tę metodę pod względem jawności i możliwości ujawniania poszczególnych jej elementów. Na ogólną liczbę siedmiu elementów stosowanych w metodzie aż pięć to elementy tajne. Do elementów jawnych zaliczamy następujące wartości: u - wybraną liczbę pierwszą, n - iloczyn dwóch liczb "p" i "q". Do wielkości tajnych zaliczamy: z - ciąg znaków informacji, p - wybraną liczbę pierwszą, q - wybraną liczbę pierwszą, t - obliczoną wartość ze wzoru (p-1) (q-1) oraz b - obliczoną wartość ściśle tajną, stanowiącą klucz deszyfracji. Trudno tu mówić o jawności metody czy jawnym kluczu. Właściwy klucz, służący do szyfrowania informacji, jest zawarty w liczbach pierwszych "p" i "q", których iloczyn jest znany. Znana jest również wielkość wybrana "u", która służy do obliczenia klucza deszyfrującego "b". Kluczem zasadniczym metody RSA są tajne liczby "p" i "q" (możliwość znalezienia obu tych wielkości omówiono w p. 6.7). Ponieważ dwie liczby pierwsze kilkudziesięcioznakowe są niemożliwe do praktycznego stosowania, musimy stosować wyłącznie liczby małe, które nie gwarantują skuteczności metody. Natomiast wielkości "n" oraz "u" muszą (podkreślam muszą) być podawane jawnie, gdyż są one podstawą obliczenia wielkości "b" służącej jako klucz do deszyfracji otrzymanego szyfrogramu. Bez jawnego przesyłania tych dwóch wielkości nie jesteśmy w stanie dokonać deszyfracji, a jawność tych dwóch liczb bardzo obniża wartość metody.

Rozpatrzmy obecnie metodę UNITAKOD przedstawioną w p.p. 5.4 i 6.4. Po analizie dotychczasowych metod szyfrowania, które są stosowane w praktyce lub przechodzą próby laboratoryjne, dokonajmy oceny omówionej w poprzednich rozdziałach metody UNITAKOD. Metoda ta jest szyfrem dynamicznym, opartym na układzie tablic zmieniających się w zależności od czasu i położenia wierszy oraz kolumn przesyłanej wiado-

mości. Jest to metoda szyfrowania bez stosowania klucza. Proces szyfrowania jest oparty na dwóch różnych algorytmach, z których jeden służy do szyfrowania, a drugi do deszyfracji. Ponieważ do dziś nie ma metody oceny szyfru bez klucza, a szczególnie szyfru, który przesyłaną informację traktuje jako część składową algorytmu szyfrującego, należy ocenić metodę UNITAKCD za pomocą konwencjonalnych wzorów podanych w pracach [18], [20]. W tym celu przyjmijmy za liczbę kluczy minimalną wartość permutacji tablicy kodów i przesyłanej informacji, która będzie podstawą dalszych obliczeń. W tym przypadku otrzymamy.

1. Liczba permutacji obu tablic

$$L_p = (W_z!)^2 * (W_z!)^W * (W_w * K_w),$$

gdzie: W - liczba wierszy w tablicy kodów kryptograficznych,

Z_w - liczba znaków w wierszu tablicy kodów kryptograficznych,

W_w - liczba wierszy w przesyłanej wiadomości,

K_w - liczba kolumn w przesyłanej wiadomości.

2. Prawdopodobieństwo dekryptażu

$$P_d = \frac{1}{L_k}.$$

3. Współczynnik dekryptażu

$$W_d = L_k * X,$$

gdzie: X - współczynnik zależny odwrotnie proporcjonalnie do szybkości pracy urządzenia deszyfrującego.

4. Entropia klucza

$$E_k = \log_2 W + \log_2 Z_w + \log_2 W_w + \log_2 K_w.$$

Entropia klucza została określona przez Shannona [20] jako suma logarytmów prawdopodobieństwa, gdzie prawdopodobieństwo przyjęcia przez zmienną losową X określonej wartości wynosi x_i. Gdy wszystkie prawdopodobieństwa są sobie równe i wynoszą 1/n, wielkość entropii przyjmuje wartość maksymalną, określoną równaniem $E = \log_2 n$.

Z powyższych wzorów wynikają następujące wnioski, które zastosowano w algorytmie szyfrowania.

1. Jakość szyfru rośnie wraz z liczbą kluczy, gdyż wówczas rośnie liczba możliwości, które musi przeanalizować kryptoanalityk, aby doprowadzić do dekryptażu. Dlatego liczba kluczy może i powinna być zastąpiona "kluczem nieskończonym" lub układem tablic i ich nieskończenie wielką liczbą permutacji.

2. Określona liczba kluczy służy do obliczenia prawdopodobieństwa dekryptażu, współczynnika dekryptażu i entropii klucza. Ważnym parametrem w tym układzie jest współczynnik dekryptażu, określający czas jaki musi upłynąć, aby kryptoanalityk na pewno zaszyfrował przechwycony szyfrogram.

Po zastosowaniu powyższych wzorów do metody UNITAKOD otrzymano maksymalną liczbę kluczy, czyli permutacji tablicy kodów i przesyłanej informacji, którą można wyrazić jako

$$L_p = (256!)^{256} * (256!)^2 * 120 * 10.000 ,$$

gdzie:

- wyrażenie w pierwszym nawiasie kwadratowym dotyczy liczby permutacji tablicy kodów kryptograficznych,

- wyrażenie w drugim nawiasie kwadratowym dotyczy stosowanych w praktyce średnich długości przesyłanych informacji, które są stosowane w wydawnictwach standardowych programów ICL.

Ponieważ liczba permutacji L_p jest dużo większa od liczby kluczy w metodzie Vernama, należy uznać za zbyteczne obliczanie czasu potrzebnego na deszyfrację informacji. Na podkreślenie zasługuje - i jest to najistotniejszy element metody UNITAKOD - pojawienie się w czasie szyfrowania trzech różnych tablic kodowych (co szczegółowo podano w p. 5.5):

1) tablicy zerowej, którą tworzy się za pomocą specjalnego generatora. Talica ta stanowi podstawę do dalszej pracy podczas szyfrowania. Liczba

tablic zerowych równa się liczbie permutacji tablicy kodów kryptograficznych. Dlatego jeden i ten sam program szyfrujący, dokonujący szyfrowania w tym samym czasie, wygeneruje różne kody w zależności od wygenerowanej i przyjętej tablicy zerowej;

2) tablicy wyjściowej, którą tworzymy za pomocą generatora na podstawie wybranej wcześniej tablicy zerowej. Jej liczba równa się liczbie tablic kodowych z tym, że jeden i ten sam generator opracowuje zupełnie inną tablicę wyjściową dla różnych tablic zerowych;

3) tablicy kodowej, którą tworzy się z tablicy wyjściowej i z tablicy wierszy i kolumn przesyłanej informacji. Tablica ta została opisana za pomocą wzoru (1), p. 5.4.

W metodzie UNITAKOD zasługuje jeszcze jedno na podkreślenie. Otóż w metodach klasycznych zachodzi konieczność spełnienia warunku, by długość ciągu szyfrowego była mniejsza lub równa długości klucza. To wymaganie w szyfrowaniu dynamicznym metody UNITAKOD po prostu traci sens. Jedynie warunek szyfru idealnego podany przez Seidlera [18, s. 182], wyrażony we wzorze $N_x/N \log_2 K$, w którym N odnosi się do długości przesyłanej informacji, ma w metodzie UNITAKOD możliwość zastosowania. Podstawiając do powyższego wzoru wartości metody UNITAKOD, otrzymano

$$\frac{Z_w}{K_w * W_w} \leqslant \log_2 (Z_w * W).$$

Ponieważ wartości Z_w oraz $(Z_w * W)$ dla określonego szyfru są wartościami stałymi, a jedynie może się zmieniać długość ciągu szyfrowego (przesyłanej informacji) wyrażonej wzorem $(K_w * W_w)$, przedstawiony warunek staje się bardziej oczywisty wraz ze wzrostem długości przesyłanej informacji.

Niezależnie od powyższych zalet metody UNITAKOD należy wymienić najważniejszą: jest nią całkowita jawność! Metoda, ta mimo swej prostoty w praktycznym stosowaniu, ma tak wielką liczbę niewiadomych, że bez obawy można publikować jej możliwości i zasady zastosowania. Dla przykładu rozpatrzmy urywek ciągu szyfrowego w postaci: 021F95X... Przystępując do deszyfracji, lub jak kto woli, do łamania szyfru, należy sobie odpowiedzieć na następujące pytania:

"Czy zaszyfrowane wartości są ujęte w znakach: 02, 021, 1F, 21F, F9 itd., czy też może w innych układach?

Jeżeli ustalimy, że zaszyfrowany znak ma postać $\phi 2$, to wówczas należy ustalić:

- jaki jest udział w liczbie $\phi 2$ czynnika A (tablicy kodów kryptograficznych), a jaki czynnika B (tablicy przesyłanej informacji),
- czy wartość 02 jest wynikiem szyfru nr 1 (SZYFR=A+B), czy też szyfru nr 2 (SZYFR = A + ϕ),
- czy wynik powstał w rezultacie zastosowania wielkości mod M, czy też nie,
- jaka była wygenerowana postać tablicy zerowej,
- jaka była wygenerowana postać tablicy wyjściowej,
- jaka była wygenerowana postać tablicy przesyłanej informacji,
- jaki był czas przesyłania meldunku, na podstawie którego dokonywano generowania poszczególnych tablic itd.

Ta ogromna liczba niewiadomych, których znajomość jest konieczna dla dokonania deszyfracji, upoważnia nas do określenia metody UNITAKOD jako metody szyfrowania bez klucza, której zasady szyfrowania są całkowicie jawne.

Zaprezentowana w niniejszym opracowaniu metoda UNITAKOD jest jednak niemożliwa do wdrożenia i praktycznej eksploatacji bez zastoso-

wania generatora znaków losowych, a raczej generatora permutacji. Jest to jeden jedyny element w metodzie UNITAKOD, który po wdrożeniu należy utrzymać w tajemnicy. Możliwości opracowania i zastosowania generatora przedstawiono w pracy [30], jednak dokładne zasady pracy i wymagania stawiane generatorowi permutacji, przedstawiono w p. 8.

8. GENERATORY ZNAKÓW LOSOWYCH I PERMUTACJI

Generatory liczb losowych są ściśle związane z teorią prawdopodobieństwa. Rozróżniamy dwa rodzaje generatorów liczb losowych:

- fizyczne,
- programowe.

Do generatorów fizycznych zaliczamy w zasadzie dwa typy. Pierwszy z nich to moneta, a drugi urna z ponumerowanymi kartkami lub kulkami. Rzucanie monetą daje możliwość losowego otrzymania orła lub reszki z prawdopodobieństwem 1/2, czyli zmienna losowa ma rozkład dwupunktowy i przyjmuje wartości ϕ lub 1. Urnę wraz z ponumerowanymi kartkami będziemy także nazywali generatorem liczb losowych o rozkładzie równomiernym. Oba generatory fizyczne dają możliwość otrzymywania liczb losowych, lecz właśnie dlatego nie mogą być stosowane w ochronie zbiorów, a szczególnie w szyfrowaniu informacji. Jeśli zastosujemy rzeczywiste generatory liczb losowych, tracimy możliwość deszyfracji ciągu szyfrowego.

Obecnie, przy szerokim zastosowaniu maszyn cyfrowych, a szczególnie przy przesyłaniu informacji w sieciach komputerowych, jesteśmy zmuszeni korzystać z innego typu generatorów. Są nimi programowe generatory liczb losowych, które powszechnie otrzymały miano generatorów programowych. Nazwa ta nie jest zupełnie ścisła i nie odpowiada prawdzie. Otrzymywane liczby z generatorów programowych powstają w wyniku stosowania odpowiedniej procedury rachunkowej, dlatego nie są to liczby losowe w takim sensie, jak liczby otrzymywane z generatorów fizycznych. Takie generatory należałoby określić mianem generatorów liczb pseudolosowych. Należy w posługiwaniu się nazwą generatory programowe pamiętać, że generowane przez nich wartości są wartościami pseudolosowymi, które umożliwiają deszyfrację ciągu szyfrowego. Dzięki tym właściwościom

mogą być stosowane w zabezpieczeniu informacji przed dostępem osób nie upoważnionych.

8.1. Generatory programowe

Istotnym problemem związanym z generatorami fizycznymi jest ich stabilność, a raczej brak stabilności. W pracach [21] i [34] można znaleźć wiele przykładów generatorów fizycznych, jednak dominującą rolę odgrywają generatory programowe. Są to generatory wykonane jako odpowiednie programy dla maszyn cyfrowych. Generatory tego typu, ze względu na dużą stabilność, mogą i są wykorzystywane w ochronie informacji, szczególnie w jej szyfrowaniu.

Generatory programowe, które stosuje się w praktyce, a które wyparły wszelkie inne generatory, przyjmuje następującą postać:

$$x_{n-1} = a_o x_n + a_1 x_{n-1} + \dots + a_k x_{n-k} + b \pmod N, \qquad (8)$$

gdzie wszystkie wartości a_i, b oraz x_i są liczbami całkowitymi z przedziału (0 - N). Są to tak zwane generatory liniowe. Szczególną ich postacią są generatory multyplikatywne, których ogólna postać jest wyrażona wzorem

$$x_{n+1} = cx_n \pmod N. \qquad (9)$$

Jest jeszcze jedna grupa generatorów mieszanych, którymi nie będziemy się zajmowali ze względu na małą ich przydatność praktyczną (obecnie). Szczególnie przydatnym (w naszym przypadku) jest generator określony wzorem (9). Należy zwrócić uwagę, że każdy ciąg (x_n), n = 0,1,2,... jest zbudowany ze skończonej liczby różnych znaków (liczb). Każda liczba w tym ciągu powtarza się dokładnie jeden raz, natomiast długość tego ciągu określa liczba K, zwana jego okresem. Jeżeli w określonym ciągu x_n jest spełniony warunek K = N, to każda liczba ciągu pojawia się w określonej kolejności i ciąg ten staje się po prostu permutacją liczb

(0, 1, 2,..., N - 1). Jeżeli K N, to pojawiają się tylko niektóre liczby ciągu. Na uwagę zasługuje przypadek, gdzie we wzorze (9) zachodzi zjawisko K = N. Spełnienie tego warunku jest konieczne do otrzymania określonej permutacji ciągu, koniecznej w czasie szyfrowania informacji (zagadnienie to zostanie rozwinięte w p. 8.2).

8.2. Generator permutacji

W metodzie UNITAKOD zastosowano tablicę kodów kryptograficznych, która ma możliwości szyfrowania informacji w oparciu o trzy rodzaje tablic: zerową, wyjściową i szyfrową. Każda tablica wymaga utworzenia odpowiedniej generacji za pomocą określonego generatora. Dlatego jest wymagana możliwość generowania permutacji ciągów ($::_n$), dla K = N, w których każda liczba (znak) pojawi się wyłącznie jeden raz. Tablica kodów kryptograficznych może mieć rozmiary:

- 34 znaki, w tym 24 litery alfabetu łacińskiego oraz 10 cyfr,
- 60 znaków stosowanych w maszynach cyfrowych,
- 145 znaków stanowiących wersję międzynarodowego kodu KOI-8,
- 256 znaków stanowiących maksymalną liczbę możliwych kombinacji kodu KOI-8.

Wartość liczbowa N mieści się w przedziale (34 - 256).

Niezależnie od powyższego wymogu w metodzie UNITAKOD musi być spełniony warunek możliwości wygenerowania odpowiedniej liczby permutacji wyrażonej wzorem: $(W_z!)^W$, gdzie W_z - liczba zastosowanych znaków z przedziału (34 - 256), W - liczba wierszy w tablicy. Gdy $W_z = W = 256$, otrzymujemy maksymalną liczbę permutacji: $P = (256!)^{256}$. Jest to podstawowy warunek decydujący o zastosowaniu określonego generatora permutacji.

Zastosowany w metodzie UNITAKOD programowy generator permutacji oparto na ogólnych zasadach generatora multyplikatywnego (9), w którym dokonano niezbędnych zmian. Pierwsza dotyczy stałej wartości "c", a druga wartości "N". Stała wartość "c" jest niezmiernie istotnym elementem wzoru (9). W generatorach multyplikatywnych jej wartość jest praktycznie obojętna, ale muszą to być liczby całkowite z przedziału (0 - N) [34, s. 29]; jest to warunek. Dla przykładu rozpatrzmy wyniki otrzymane dla wartości: c = 4, oraz ciągu liczb: 1, 2, 3, ..., 10. Z tego N = 10. Po podstawieniu tych danych do wzoru (9) otrzymujemy:

$x_1 = 4 \times 1 \pmod{10} = 4,$

$x_2 = 4 \times 2$ -"- $= 8,$

$x_3 = 4 \times 3$ -"- $= 2,$

$x_4 = 4 \times 4$ -"- $= 6,$

$x_5 = 4 \times 5$ -"- $= 0,$

$x_6 = 4 \times 6$ -"- $= 4,$

$x_7 = 4 \times 7$ -"- $= 8,$

$x_8 = 4 \times 8$ -"- $= 2,$

$x_9 = 4 \times 9$ -"- $= 6,$

$x_{10} = 4 \times 10$ -"- $= 0.$

W wyniku otrzymaliśmy:

1) $x_1 = x_6 = 4,$

2) $x_2 = x_7 = 8,$

3) $x_3 = x_8 = 2,$

4) $x_4 = x_9 = 6,$

5) $x_5 = x_{10} = 0.$

Nie otrzymaliśmy natomiast liczb 1, 3, 5, 7, 9, które występują w ciągu x_n. Podobnie dla c = 6, gdzie ciąg otrzymanych wartości wynosi: 6, 2, 8, 4,

0, 6, 2, 8, 4, 0. Z tych krótkich przykładów można wyciągnąć następujące wnioski.

1) W obu przypadkach otrzymaliśmy liczby parzyste zamykające się okresem:

- dla c = 4 : 4, 8, 2, 6, 0,
- dla c = 6 : 6, 2, 8, 4, 0;

2) Nie otrzymaliśmy liczb nieparzystych.

3) Nie został spełniony warunek pojawienia się każdej liczby tylko jeden raz.

Ta krótka analiza świadczy o tym, że generator (9) nie może być stosowany dla parzystej wartości "c".

Rozpatrzmy działanie generatora dla liczb nieparzystych, np. c = 9. W wyniku otrzymujemy: 9, 8, 7, 6, 5, 4, 3, 2, 1, 0. Jest to układ malejący w odwrotnej kolejności, od 9 do 0. Jeśli podstawimy wartości c = 15, otrzymujemy: 5, 0, 5, 0, 5, 0, 5, 0, 5, 0, 5, 0. Jeżeli dla tej samej wartości "c" podstawimy N = 20, otrzymamy w wyniku: 15, 10, 5, 0, 15, 10, 5, 0, 15, 10. We wszystkich przypadkach otrzymujemy układ liczb zmieniających się w okresach. Jednak w żadnym z wymienionych przypadków nie uzyskaliśmy pożądanego wyniku i tym samym nie zostały dotrzymane warunki określone we wstępie.

Jeżeli nie zostały spełnione warunki przy podstawieniu parzystych i nieparzystych wartości "c", rozpatrzmy działanie generatora permutacji dla liczb pierwszych. Podstawmy dla wartości "c" kolejne liczby pierwsze: 3, 7, 11, 13, 17 i dokonajmy obliczeń dla N = 10, 20 oraz 24.

Przykład 1

Przyjmujemy ciąg x_n = 1, 2, 3, ..., 10 oraz N = 10.

c \ x_n	1	2	3	4	5	6	7	8	9	10
3	3	6	9	2	5	8	1	4	7	0
7	7	4	1	8	5	2	9	6	3	0
11	1	2	3	4	5	6	7	8	9	0
13	3	6	9	2	5	8	1	4	7	0
17	7	4	1	8	5	2	9	6	3	0

Na podstawie analizy wyników zestawionych tabelarycznie należy stwierdzić, że wszystkie warunki zostały spełnione. Ciąg x_n przyjmuje zróżnicowaną postać uzależnioną od wartości "c". Każda liczba ciągu jest prezentowana jeden raz, a cały ciąg kończy się wartością zerową.

Przykład 2

Przyjmujemy ciąg x_n = 1, 2, 3, ..., 20, oraz N = 20, dla tych samych wartości "c".

Również i w tym przykładzie wszystkie wartości ciągu x_n zostały zaprezentowane jeden raz i każdy z ciągów kończy się zerem. Powyższe przykłady dotyczyły jednak nietypowych wartości N, gdyż żadna z nich nie reprezentowała wielkości obowiązujących w metodzie UNITAKOD. Rozpatrzmy najmniejszą wartość N, jaka może być zastosowana w praktyce. Jest to wielkość N = 24, czyli obejmuje cały alfabet łaciński stosowany w maszynach cyfrowych.

Przykład 3

Przyjmujemy ciąg x_n = 1, 2, 3, ..., 24 oraz N = 24, dla tych samych wartości "c".

Z analizy zestawionych wyników można wnioskować, że tylko wartość c = 3, podstawiona do wzoru nie spełnia warunków obowiązujących ge-

x_n / c	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
3	3	6	9	12	15	18	1	4	7	10	13	16	19	2	5	8	11	14	17	0
7	7	14	1	8	15	2	9	16	3	10	17	4	11	18	5	12	19	6	13	0
11	11	2	13	4	15	6	17	8	19	10	1	12	3	14	5	16	7	18	9	0
13	13	6	9	12	5	18	11	4	17	10	3	16	9	2	15	8	1	14	7	0
17	17	14	11	8	5	2	19	16	13	10	7	4	1	18	15	12	9	6	3	0

Tablica do przykładu 2

nerator permutacji. Obliczenia dla N = 60 potwierdzają to samo. Zastanówmy się nad przyczyną zaistniałych faktów.

Jak stwierdzono na początku niniejszego rozdziału, metoda UNITAKOD wymaga, by liczba "c" była tak dobraną liczbą pierwszą, ażeby można było otrzymać kolejną permutację ciągu x_n dla okresu równego N. Według Sierpińskiego [21, s. 171] wykładnik, do którego jakakolwiek liczba należy według modułu pierwszego "p" jest zawsze dzielnikiem liczby p - 1. Te liczby, które należą według modułu pierwszego "p" do wykładnika p - 1 nazywamy pierwiastkami pierwotnymi liczby pierwszej "p". Zgodnie z powyższym twierdzeniem rozpatrzmy pierwiastek pierwotny liczby 2 dla N = 23. Mówiąc inaczej: zbadajmy, czy liczba 2 jest pierwiastkiem pierwotnym liczby 23.

$2^1 = 2 \pmod{23}$, $2^2 = 4 \pmod{23}$, $2^3 = 8 \pmod{23}$, $2^4 = 16 \pmod{23}$, $2^5 = 9 \pmod{23}$, $2^6 = 18 \pmod{23}$, $2^7 = 13 \pmod{23}$, $2^8 = 3 \pmod{23}$, $2^9 = 6 \pmod{23}$, $2^{10} = 12 \pmod{23}$, $2^{11} = 1 \pmod{23}$.

Stwierdzamy, że liczba 2 należy modulo 23 do wykładnika 11, przeto nie jest pierwiastkiem pierwotnym liczby 23.

Rozpatrzmy jeszcze jeden przykład dla liczby 5 modulo 23.

$5^1 = 5 \pmod{23}$, $5^2 = 2 \pmod{23}$,..., $5^{21} = 14 \pmod{23}$ oraz

$$5^{22} = 1 \pmod{23}.$$

W tym przypadku liczba 5 należy modulo 23 do wykładnika 22, czyli jest pierwiastkiem pierwotnym liczby 23.

Analizę dotyczącą pierwiastków pierwotnych liczb pierwszych przeprowadzono zgodnie z zasadami podanymi przez Sierpińskiego w pracy [21, s. 169-181]. Powyższe zasady zostały wykorzystane przez R. Zieleniewskiego w pracy [34, s. 38 i 39] oraz zastosowana do generatora multiplikatywnego opracowanego przez Lehmana, a wyrażonego wzorem: $X_{n+1} = C X_n \pmod{M}$.

C	N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
3	20	3	6	9	12	15	18	21	0	3	6	9	12	15	18	21	0	3	6	9	12	15	18	21	0
7	24	7	14	21	4	11	18	1	8	15	22	5	12	19	2	9	16	23	6	13	20	3	10	17	0
11	24	11	22	9	20	7	18	5	16	3	14	1	12	23	10	21	8	19	6	17	4	15	2	13	0
13	24	13	2	15	4	17	6	19	8	21	10	23	12	1	14	3	16	5	18	7	20	9	22	11	0
17	24	17	10	3	20	13	6	23	16	9	2	19	12	5	22	15	8	1	18	11	4	21	14	7	0

Warunki nie zostały spełnione tylko dla C = 3.

Tablica do przykładu 3

W metodzie UNITAKOD wykorzystano omówioną wyżej analizę, jednak zastosowanie praktyczne wymaga dodatkowych uściśleń. Metoda UNITAKOD stawia nieco odmienne wymagania generatorowi permutacji, którego postać można wyrazić następująco:

$$P = C X_n \pmod N,$$

gdzie: C - określona liczba pierwsza,

N - określona liczba znaków zastosowana w tablicy kodów,

X_n - ciąg liczb całkowitych.

Wymagania związane z zastosowaniem generatora permutacji w metodzie UNITAKOD można ująć w dwóch punktach.

I. Liczba N musi być stałą i określoną wartością dla danego szyfru, z przedziału liczb 24 - 256. Najczęściej będą to wielkości związane z międzynarodowym kodem i tak:

a) 24 - liczba znaków alfabetu,

b) 34 - liczba znaków alfabetu i cyfr,

c) 60 - minimalna liczba znaków stosowanych w komputerach,

d) 145 - międzynarodowa wersja kodu ośmiobitowego,

e) 256 - maksymalna liczba możliwych kombinacji w kodzie międzynarodowym.

II. Liczba C musi być określoną liczbą pierwszą spełniającą poniższe trzy warunki:

a) $C * X_i \neq \phi \pmod N$ dla $i = 1, 2, \ldots, N-1$,

b) $C * X_i = \phi \pmod N$ dla $i = N$,

c) $C * X_i \pmod N \neq C * X_j \pmod N$, jeżeli $X_i \neq X_j$.

Spełnienie podanych powyżej dwóch warunków jest niezbędne do zastosowania generatora permutacji w metodzie UNITAKOD. Całość można ująć w następującym wzorze końcowym:

$$S_{wk} = (a_{xz} + b_{ij}) \pmod{M},$$

gdzie: a_{xz} - tablica kodów kryptograficznych tworzona za pomocą generatora permutacji: $P = C\,X_n \pmod{N}$,

M - liczba znaków zastosowanych w określonych zasadach szyfrowania, którą następnie podstawiamy w miejsce liczby N.

Pozostałe wartości podane w powyższym wzorze omówiono w p. 5.4.

Poszukiwania wartości C dla generatora permutacji przy różnych wielkościach N ilustrują poniższe zestawy.

Generator permutacji: $X = C X_n \pmod N$ Część 1

C	N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
7	34	7	14	21	28	1	8	15	22	29	2	9	16	23	30	3	10	17
13	34	13	26	5	18	31	10	23	2	15	28	7	20	33	12	25	4	17
19	34	19	4	23	8	27	12	31	16	1	20	5	24	9	28	13	32	17
7	60	7	14	21	28	35	42	49	56	3	10	17	24	31	38	45	52	59
13	60	13	26	39	52	5	18	31	44	57	10	23	36	49	2	15	28	41
19	60	19	38	57	16	35	54	13	32	51	10	29	48	7	26	45	4	23
7	145	7	14	21	28	35	42	49	56	63	70	77	84	91	98	105	112	119
13	145	13	26	39	52	65	78	91	104	117	130	143	11	24	37	50	63	76
19	145	19	38	57	76	95	114	133	7	26	45	64	83	102	121	140	14	33

C	N	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
7	34	24	31	4	11	18	25	32	5	12	19	26	33	6	13	20	27	0
13	34	30	9	22	1	14	27	6	19	32	11	24	3	16	29	8	21	0
19	34	2	21	6	25	10	29	14	33	18	3	22	7	26	11	30	15	0
7	60	6	13	20	27	34	41	48	55	2	9	16	23	30	37	44	51	58
13	60	54	7	20	33	46	59	12	25	38	51	4	17	30	43	56	9	22
19	60	42	1	20	39	58	17	36	55	14	33	52	11	30	49	8	27	46
7	145	126	133	140	2	9	16	23	30	37	44	51	58	65	72	79	86	93
13	145	89	102	115	128	141	9	22	35	48	61	74	87	100	113	126	139	7
19	145	52	71	90	109	128	2	21	40	59	78	97	116	135	9	28	47	66

C	N	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
7	60	5	12	19	26	33	40	47	54	1	8	15	22	29	36	43	50	57
13	30	35	48	1	14	27	40	53	6	19	32	45	58	11	24	37	50	3
19	60	65	24	43	2	21	40	59	18	37	56	15	34	53	12	31	50	9
7	145	100	107	114	121	128	135	142	4	11	18	26	33	40	47	54	61	68
13	145	20	33	46	59	62	75	88	101	114	127	140	18	31	44	57	70	83
19	145	85	104	123	142	16	35	54	73	92	111	130	4	23	42	61	80	99

C	N	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68
7	60	4	11	18	25	32	39	46	53	0								
13	60	16	29	42	55	8	21	34	47	0								
19	60	28	47	6	25	44	3	22	41	0								
7	145	75	82	89	96	103	110	117	124	131	138	144	6	13	20	27	34	41
13	145	96	109	122	135	3	16	29	42	55	68	81	94	107	120	133	1	14
19	145	118	137	11	30	49	68	87	106	125	144	18	37	56	75	94	113	132

C	N	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85
7	145	48	55	62	69	76	83	90	97	104	111	118	125	132	139	1	8	15
13	145	27	40	53	66	79	92	105	118	131	144	12	25	38	51	64	77	90
19	145	6	25	44	63	82	101	120	139	13	32	51	70	89	108	127	1	20

C	N	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102
7	145	22	29	36	43	50	57	64	71	78	85	92	99	106	113	120	127	134
13	145	103	116	129	142	20	23	36	43	62	75	88	101	114	127	140	8	21
19	145	39	58	77	96	115	134	8	27	46	65	84	103	122	141	15	34	53

C	N	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119
7	145	141	3	10	17	24	31	38	45	52	59	66	73	80	87	94	101	108
13	145	34	47	60	73	86	99	112	125	138	6	19	32	45	58	71	84	97
19	145	72	91	110	129	3	22	41	60	79	98	117	136	10	29	48	67	86

C	N	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136
7	145	115	122	129	136	143	5	12	19	26	33	40	47	54	61	68	75	82
13	145	110	123	136	4	17	30	43	56	69	82	95	108	121	134	2	15	28
19	145	105	124	143	17	36	55	74	93	112	131	5	24	43	62	81	100	119

C	N	137	138	139	140	141	142	143	144	145
7	145	89	96	103	110	117	124	131	138	0
13	145	41	54	67	80	93	106	119	132	0
19	145	138	12	31	50	69	88	107	126	0

Dla wartości C = 7, 13, 19 oraz N = 34, 60, 145, warunki postawione dla generatora permutacji $X = CX_n \pmod N$ zostały spełnione.

Generator permutacji: $X = CX_n \pmod N$, dla N = 60, gdzie: C - kolejne liczby pierwsze od 7 do 59, n = 1,2,3,...,N.

Część 1

C	N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
7	60	7	14	21	28	35	42	49	58	3	10	17	24	31	38	45	52	59	6	13	20	17	34	41	48	55	2	9	16	23	30	37	44	51	58	5
11	60	11	22	33	44	55	6	17	28	39	50	1	12	23	34	45	56	7	18	29	40	51	2	13	24	35	46	57	8	19	30	41	52	3	14	25
13	60	13	26	39	52	5	18	31	44	57	10	23	36	49	2	15	29	41	54	7	20	33	46	59	12	25	38	51	4	17	30	43	56	9	22	35
17	60	17	34	51	8	25	42	59	16	33	50	7	24	41	58	15	32	49	6	23	40	57	14	31	48	5	22	39	56	13	30	47	4	21	38	55
19	60	19	38	57	16	35	54	13	32	51	10	29	48	7	26	45	4	23	42	1	20	39	58	17	36	55	14	33	52	11	30	49	8	27	46	5
23	60	23	46	9	32	55	18	41	4	27	50	13	36	53	22	45	8	31	54	17	40	3	26	49	12	35	58	21	44	7	30	53	16	39	2	25
29	60	29	58	27	56	25	54	23	52	21	50	19	48	17	46	15	44	13	42	11	40	9	38	7	36	5	34	3	32	1	30	59	28	57	26	55
31	60	31	2	33	4	35	6	37	8	30	10	41	12	43	14	45	16	47	18	49	20	51	22	53	24	55	26	57	28	59	30	1	32	3	34	5
37	60	37	14	51	28	5	42	19	56	33	10	47	24	1	38	15	52	29	6	43	20	57	34	11	48	25	2	39	16	53	30	7	44	21	58	35
41	60	41	22	3	44	25	6	47	28	9	50	31	12	53	34	15	56	37	18	59	40	21	2	43	24	5	46	27	8	49	30	11	52	33	14	55
43	60	43	26	9	52	35	18	1	44	27	10	53	36	19	2	45	28	11	54	37	20	3	46	29	12	55	38	21	4	47	30	13	56	39	22	5
47	60	47	34	21	8	55	42	29	16	3	50	37	24	11	58	45	32	19	6	53	40	27	14	1	48	35	22	9	56	43	30	17	4	51	38	25
53	60	53	46	39	32	25	18	11	4	57	50	43	36	29	22	15	8	1	54	47	40	33	26	19	12	5	58	51	44	37	30	23	16	9	2	55
59	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25

C	N	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
7	60	12	19	26	33	40	47	54	1	8	15	22	29	36	43	50	57	4	11	18	25	32	39	46	53	0
11	60	36	47	58	9	20	31	42	53	4	15	26	37	48	59	10	21	32	43	54	5	16	27	38	49	0
13	60	48	1	14	27	40	53	6	19	32	45	58	11	24	37	50	3	16	29	42	55	8	21	34	47	0
17	60	12	29	46	3	20	37	54	11	28	45	2	19	36	53	10	27	44	1	18	35	52	9	26	43	0
19	60	24	43	2	21	40	59	18	37	56	15	34	53	12	31	50	9	28	47	6	25	44	3	22	41	0
23	60	48	11	34	57	20	43	6	29	52	15	38	1	24	47	10	33	56	19	42	5	28	51	14	37	0
29	60	24	53	22	51	20	49	18	47	16	45	14	43	12	41	10	39	8	37	6	35	4	33	2	31	0
31	60	36	7	38	9	40	11	42	13	44	15	46	17	48	19	50	21	52	23	54	25	56	27	58	29	0
37	60	12	49	26	3	40	17	54	31	8	45	22	59	36	13	50	27	4	41	18	55	32	9	46	23	0
41	60	36	17	58	39	20	1	42	23	4	45	26	7	48	29	10	51	32	13	54	35	16	57	38	19	0
43	60	48	31	14	57	40	23	6	49	32	15	58	41	24	7	50	33	16	59	42	25	8	51	34	17	0
47	60	12	59	46	33	20	7	54	41	28	15	2	49	36	23	20	57	44	31	18	5	52	39	26	13	0
53	60	48	41	34	27	20	13	6	59	52	45	38	31	24	17	10	3	56	49	42	35	28	21	14	7	0
59	60	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

WNIOSKI KOŃCOWE

1. Na obecnym etapie przetwarzania informacji i przesyłania jej za pomocą linii transmisji, zabezpieczenie jej poufności musi być oparte na odpowiednich systemach szyfrowania danych.

2. Eliminacja czynnika ludzkiego z systemu ochrony informacji jest decydującym elementem jego wysokiej skuteczności.

3. Skuteczny system szyfrowania informacji musi się składać z kilku elementów szyfrujących, wchodzących w skład modelu matematycznego. Model ten nie może w żadnym przypadku być monolitem, który w określonych warunkach daje ten sam wynik, gdyż ułatwia to deszyfrację ciągu szyfrowego przez osoby nie upoważnione.

4. Im większa jawność metody ochrony informacji, tym większa jej skuteczność.

5. Klucz jest czynnikiem obniżającym skuteczność metod ochrony informacji, dlatego jego eliminacja z procesu szyfrowania staje się koniecznością.

6. Szyfrowanie bez klucza powinno być oparte na modelu matematycznym, który spełni podstawową zasadę idealnego systemu ochrony: "metoda powinna być tak zaprojektowana, aby jej autor, mając zaszyfrowany i rozszyfrowany tekst, nie był w stanie określić zasad tworzenia ciągu szyfrowego, a tym samym nie był w stanie dokonać deszyfracji innego ciągu szyfrowego".

SPIS LITERATURY

[1] Biegert W., Moderne Chiffrierverfahren, FHT - Stuttgart - 87.

[2] Diffie, Hellman - New Directions in Cryptography, IEEE Trans. Inf. Theory, 1976.

[3] Goldman S., Teorija informaciji, Moskva 1957.

[4] Hoffman L.J., Poufność w systemach informatycznych, WNT, Warszawa 1982.

[5] Jaglom M., Verojatnost' i informacija, Moskva 1960.

[6] Karhausen M.O., Müller P.J., Datenbank, Datentransparenz und Datenschutz. Nachrichten Dokumentation 1972/4.

[7] Kulikowski J.L., Organizacyjne i techniczne aspekty ochrony danych w systemach informatycznych, t. 1, z. 2, TNOiK, Wrocław 1976.

[8] Lenstra, Lenstra, Lovasz, Factoring Polynominals with Rational Coefficients, Math. Annalen, 261, 1982.

[9] Miszczak M., Problemy ochrony systemów komputerowych, referat na konferencji naukowej "Prawne problemy systemów informatycznych, Wrocław 1976.

[10] Morrison, Brillhart , A method of factoring and the Factorization of F_7, Math. Comp. 29, 1975.

[11] Merkle, Secure Communications Over Insecure Channels, Comm. ACM, 21, 1978.

[12] Merkle, Hellman - Hiding, Information and Signatures in Trapdoor Knapsack, IEEE Trans. Inf. Theory, 24, 1978.

[13] Niemczyk L., Oprogramowanie teleprzetwarzania maszyn jednolitego systemu, Warszawa, WNT, 1979.

[14] Ryska H., Herda J., Kryptographische Verfahren in der Datenverarbeitung, Springer, 1980.

[15] Sandia Report - Factorization Using the Quadratic Sieve Algorithm, United States Department of Energy, 1983.

[16] Sandia Report - Most Wandet Factorizations Using the Quadratic Sieve, United States Department of Energy- 1984.

[17] Seidler J., Analiza i synteza sieci łączności dla systemów teleinformatycznych, PWN, Warszawa 1979.

[18] Seidler J., Teoria kodów, PWN, Warszawa 1965.

[19] Shamir L., A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem, IEEE Trans. Inf. Theoriy, 1982.

[20] Shannon, C.E., Communication Tcony of Secrecy Systems BSTJ-49.

[21] Sierpiński W., Arytmetyka teoretyczna, PWN, Warszawa 1969.

[22] Slovar spravocnik, Matematika i kibernetika v ekonomike, Moskva 1971.

[23] Sokołowski A., Materiały i studia, nr 59, Warszawa, WAP, 1976.

[24] Sokołowski A., Ochrona informacji w systemach informatycznych, Warszawa, WAP, 1983.

[25] Sokołowski A., Skuteczność metod ochrony, Informatyka 1976 nr 1.

[26] Topolewski Z., Analiza i synteza ochrony informacji w procesach przetwarzania i teletransmisji danych, Pr. nauk. Inst. Org i Zarządz. PWr., nr 10, Wrocław 1985.

[27] Topolewski Z., Ochrona informacji w procesach przetwarzania i teletransmisji danych, Pr. nauk. Inst. Org. i Zarządz. PWr., nr 46, Wrocław 1988.

[28] Topolewski Z., Ochrona zbiorów informatycznych w systemach przetwarzania danych, Inst. Org. i Zarządz. PWr., Raport serii PRE nr 29, Wrocław 1979.

[29] Topolewski Z., Próba określenia rzeczywistej skuteczności dotychczasowych metod ochrony zbiorów informatycznych, Inst. Org. i Zarządz. PWr, Raport serii PRE nr 138, Wrocław 1980.

[30] Topolewski Z., Zastosowanie generatora znaków losowych w teleprzetwarzaniu bad danych, Inst. Org. i Zarządz. PWr, Raport serii PRE nr 306, Wrocław 1981.

[31] Wasserman J., Plugging the leaks in computer security, Hardvard Business Review 1977.

[32] Weber F., Der Traum von der perfekten Verschlüsselungsmethode, Technische Rundschau 32/85.

[33] Wierzbicki T., Informatyka w zarządzaniu, PWN, Warszawa 1986.

[34] Zieliński R., Generatory liczb losowych, WNT, Warszawa 1979.

Spis treści

Wydrukowano w 15 egz.
Egz. 1 - 15 - ASG WP
Wykonał: Z. Topolewski
Poz. .....