ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1981

Seria: GÓRNICTWO z. 112 Nr kol. 697

Ewa PIĘTKA, Irena MAZUREK

WYBRANE PROBLEMY OCHRONY INFORMACJI W SYSTEMACH KOMPUTEROWYCH PRZEMYSŁU WĘGLA KAMIENNEGO

Streszczenie. W artykule wskazano na konieczność rozwoju systemów zarządzania poprzez wdrożenie teletransmisji oraz metody wyeliminowania wzrastającego stąd zagrożenia związanego z nieupoważnionym dostępem do informacji przesyłanej. Podano przykłady technik kryptograficznych wykorzystywanych w systemach o zdalnym dostępie.

1. Wprowadzenie

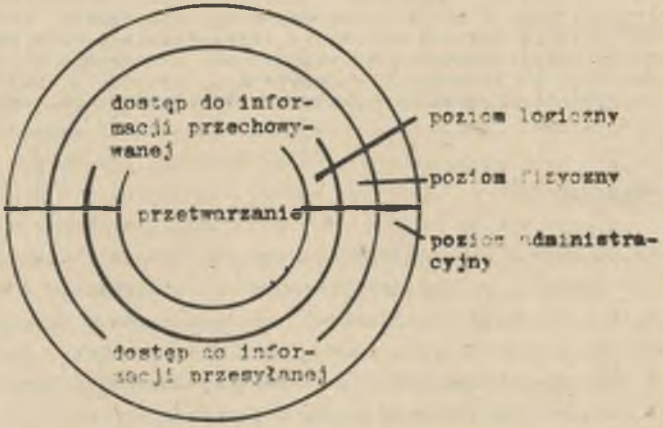
Opracowany w latach sześćdziesiątych projekt "Modelu skomputeryzowanego systemu zarządzania przemysłem węglowym" [1], wdrażany w latach siedemdziesiątych w resorcie, realizowany jest przez sprzęt informatyczny pracujący w oparciu o ujednoliconą technologię przetwarzania. Zadania realizowane są w resortowych ośrodkach informatyki. Obecnie istnieje trójpoziomowa hierarchia organizacyjna służb informatyki:

- Centralny Ośrodek Informatyki Górnictwa (COIG),
- zjednoczeniowe ośrodki informatyki,
- zakładowe ośrodki sterowania i kierowania procesami technologicznymi.

Generowane zbiory wynikowe obejmują różne odcinki działalności gospodarczej kopalń węgla kamiennego, m.in. rozliczanie i analizę procesów produkcyjnych i inwestycyjnych, ewidencję i analizę gospodarki materiałowej, zaopatrzeniowo-magazynowej i środków trwałych, ewidencję i rozliczenia księgowe, zagadnienia planowania i budowy kopalń. Poszczególne etapy prac związanych z przygotowaniem, gromadzeniem, wyprowadzaniem i dostarczaniem do odbiorców arkuszy wynikowych realizowane są w resortowej sieci ośrodków informatycznych. Informacja źródłowa przygotowywana jest i wstępnie przetwarzana w ośrodkach zakładowych. Przetwarzanie i generacja zbiorów wynikowych realizowane są w COIG. Odbiorcami arkuszy wynikowych są służby w kopalniach i zjednoczeniach przemysłu węglowego oraz departamenty Ministerstwa Górnictwa. Łączność pomiędzy ośrodkami, realizującymi poszczególne etapy przetwarzania oraz odbiorcami informacji odbywa się metodami tradycyjnymi. Poszerzenie zakresu użyteczności systemów informatycznych wymaga dalszego rozwoju technicznych środków informacji, dla stworzenia podstaw dalszego doskonalenia stosowanych metod pracy.

W latach osiemdziesiątych zakłada się wdrożenie teletransmisji w jednostkach organizacyjnych przemysłu węglowego. Wprowadzenie końcówek abonenckich u wszystkich użytkowników umożliwi bezpośrednie korzystanie z systemów informatycznych i zapewni automatyczny dostęp do informacji. System zdalnego dostępu znacznie usprawni przepływ informacji w całym przemyśle węglowym, zwiększy jednak zagrożenie wynikające z dostępu osób nieupoważnionych do przechowywanej i transmitowanej informacji. Konieczne stają się więc dodatkowe zabezpieczenia.

Wyróżnić można trzy poziomy zabezpieczeń (rys. 1): logiczny, fizyczny i administracyjny.



Rys. 1. Poziomy zabezpieczenia informacji

Poziomy te, podzielone na półpierścienie, obejmują: zabezpieczenie dostępu do zbiorów informacyjnych w pamięci masowej oraz ochronę informacji przesyłanej w liniach transmisyjnych.

Poziom logiczny - najbliższy strukturalnie procesom przetwarzania - stanowi zabezpieczanie sprzętowe i systemowe ochraniające przed przypadkowym lub umyślnym ujawnieniem, przekształceniem lub zniszczeniem informacji.

Poziom fizyczny - obejmuje ochronę przed dostępem osób nieupoważnionych do pomieszczeń komputerowych i sprzętu, ochronę linii transmisyjnych oraz ochronę przechowywanych nośników informacji.

Poziom administracyjny - wiąże się z właściwym doborem personelu odpowiednio przeszkolonego. Ważnymi elementami ochrony na tym poziomie są: właściwy nadzór pracy systemu oraz kontrola zapasów magazynowych nośników informacji [2]. Ochrona informacji w procesie przetwarzania oraz dostęp do informacji gromadzonej w zbiorach w pamięci masowej są opisane w pozycjach [2], [3].

Zagadnienia związane z ochroną fizyczną przesyłanej informacji i dostępu do linii transmisyjnej są przedstawione w punkcie 2. Ze względu na niemożliwość całkowitego wyeliminowania niebezpieczeństwa podsłuchu ważną rolę w ochronie informacji odgrywają metody kryptograficzne. Ogólną definicję systemu kryptograficznego oraz typy zabezpieczeń opisano w punkcie 3. Przykłady technik kryptograficznych wykorzystywanych w systemach o zdalnym dostępie, wykorzystywanych przez wielu użytkowników, podano w punkcie 4.

2. Ochrona fizyczna w systemach o zdalnym dostępie

Dostęp do linii transmisyjnej jest teoretycznie możliwy, lecz bardzo trudny do zrealizowania i wymagający dużych nakładów finansowych, specjalnego przygotowania i kosztownego sprzętu. Podłączenie do kabla ziemnego lub napowietrznego jest możliwe, lecz przyniesie zamierzony efekt w przypadku posiadania właściwej dokumentacji połączeń, która umożliwiłaby przyporządkowanie przewodów określonemu abonentowi. Wykorzystanie kabla koncentrycznego przenoszącego kilka tysięcy zwielokrotnionych torów akustycznych lub łącza mikrofalowego zawierającego wiele tysięcy kanałów wymaga wydzielenia wiązki w określonym pasmie częstotliwości. Operacja taka wymaga wyposażenia w bardzo kosztowne urządzenia.

Z powyższego wynika, że dostęp do przesyłanej informacji poprzez podłączenie do kabla transmisyjnego lub przechwycenie pasma łącza mikrofalowego jest bardzo trudne, nie jest jednak niemożliwe. Stosunkowo łatwiejsze jest przyłączenie do zacisków tablic rozdzielczych linii transmisyjnych. Każda para przewodów jest wyraźnie oznakowana, co umożliwia prostą identyfikację i łatwy dostęp. Udaremnienie podsłuchu uzyskuje się przez odpowiednią ochronę tablic rozdzielczych i central telefonicznych oraz wyposażenie ich w system przeciwwłamaniowy.

Jeżeli nie istnieje całkowita pewność, że zastosowane metody ochrony informacji udaremniają podsłuch, należy odwołać się do metod kryptograficznych stanowiących poziom zabezpieczeń logicznych (rys. 1). Wykorzystanie systemów kryptograficznych jest uzasadnione, gdy przesyłana informacja może stać się obiektem zainteresowania osób nieupoważnionych.

3. Systemy kryptograficzne

System kryptograficzny jest parą odwracalnych transformat:

szyfrującej: $T_k(P) = C$,

deszyfrującej: $T_k^{-1}(C) = P$,

gdzie:

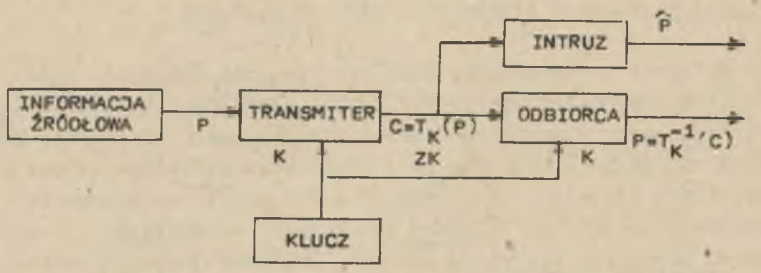
P - informacja źródłowa,

C - zaszyfrowana postać informacji, która zostanie przesłana,

K - klucz sterujący realizacją transformaty.

Transformatę szyfrującą realizuje nadawca informacji, transformatę deszyfrującą - jej odbiorca.

Konwencjonalne systemy kryptograficzne składają się z trzech części (rys. 2): transmitera, odbiorcy i intruza. Transmiter przetwarza informa-



Rys. 2. Przepływ informacji w konwencjonalnym systemie kryptograficznym

cję z postaci źródłowej na sygnał wysyłany w niezabezpieczonym kanale transmisyjnym. Na żądanie abonenta informacja źródłowa jest szyfrowana zgodnie z zakodowaną transformatą szyfrującą T_k, a szyfrogram przetwarzany jest na sygnał transmisyjny. Zaszyfrowanie zabezpiecza informację przed ujawnieniem oraz uniemożliwia jej odczytanie przez osoby nieupoważnione (intruza). Klucz k jest transmitowany do legalnego odbiorcy informacji zabezpieczonym (autonomicznym) kanałem ZK. Znając postać klucza, odbiorca realizuje procedurę odwrotną T_k^{-1}, otrzymując informację w postaci odpowiadającej informacji źródłowej, tj.:

$$T_k^{-1}(C) = T_k^{-1}(T_k(P)) = P$$

Celem systemów kryptograficznych jest opracowanie tanich w realizacji procedur szyfrowania i deszyfrowania informacji, których analiza jest zbyt droga, aby była opłacalna. Ze względu na opłacalność analizy istnieją dwa typy kryptosystemów. Do pierwszej grupy należą systemy wyposażone w zabezpieczenia, które uniemożliwiają jego rozszyfrowanie bez przekroczenia posiadanych limitów na zasoby komputerowe, np. niewystarczająca pojemność pamięci operacyjnej, zbyt krótki przedział czasu procesora na wymagane obliczenia. Nielimitowanie zasobów pozwoliłoby na rozszyfrowanie systemu. Takie zabezpieczenie systemu nazywamy zabezpieczeniem warunkowym. Drugą grupę stanowią systemy odporne na wszelkiego rodzaju metody

analizy o nieograniczonych zasobach. Zabezpieczenie takie nazywamy zabezpieczeniem bezwarunkowym.

4. Techniki kryptograficzne w systemach wykorzystywanych przez wielu użytkowników

W systemie użytkowanym przez n abonentów jest n^2-n par, które żądają komunikacji. Wymaga to przydzielenia każdej parze użytkowników oddzielnego i niepowtarzalnego klucza. Realizuje się to poprzez podanie wszystkim abonentom n-1 kluczy, po jednym do komunikacji z każdym użytkownikiem. Podłączony do systemu nowy użtykownik musi poznać klucze wszystkich dotychczasowych abonentów oraz przesłać im zdefiniowany przez siebie klucz. Wymaga to wykorzystania zewnętrznego, zabezpieczonego kanału, gdyż informacja przesyłana jest w postaci tekstu źródłowego (nieszyfrowana). Przedstawiona metoda jest droga i niewygodna. Wymaga dodatkowego kanału, w którym podsłuch informacji jest niemożliwy. Wykorzystanie sieci komputerowych powodujących zwiększenie liczby użytkowników pociągnęło za sobą konieczność znalezienia innych, bardziej efektywnych metod kryptograficznych. W sieci komputerowej końcówki abonenckie podłączone są do określonego węzła lokalnego. Użytkownik końcówki zna jeden klucz, który wykorzystuje do komunikacji z danym węzłem. Transmisja pomiędzy abonentami odbywa się za pośrednictwem węzłów. Informacja jest zaszyfrowana przez nadawcę i przesyłana odpowiadającemu mu węzłowi, gdzie jest deszyfrowana, sprawdzany jest adres odbiorcy i ponownie szyfrowana kluczem kolejnego węzła. Proces ten nazywamy szyfrografią łańcuchową. Jeżeli adres w nagłówku informacji odpowiada adresowi abonenta przyłączonego do określonego węzła, informacja jest szyfrowana kluczem odbiorcy i przesyłana do określonej końcówki.

Opisana metoda posiada ważną zaletę - nie wymaga transmisji kluczy pomiędzy użytkownikami. Wadą jej jest konieczność wielokrotnego szyfrowania i deszyfrowania informacji w poszczególnych węzłach sieci. Przedstawiona poniżej technika zabezpieczania informacji jest kompromisem pomiędzy opisanymi dwoma metodami.

Zakłada się istnienie małej liczby m węzłów sieci, wykorzystanych jako węzły podziału klucza. Każdy użytkownik posiada m kluczy, z których każdy służy do komunikacji z jednym z m węzłów. Każdy węzeł podziału kluczy pamięta n kluczy (n jest liczbą użytkowników). Jeżeli abonenci A i B zamierzają zainicjować komunikację, wybierają m-ty węzeł podziału liczby, który przydziela im parę losowo wybranych kluczy. Przed udostępnieniem kluczy system sprawdza, czy para ta nie została przydzielona innym użytkownikom. Jeżeli odpowiedź jest negatywna, klucze są przesyłane użytkownikom w postaci zaszyfrowanej za pomocą klucza służącego do komunikacji określonego abonenta końcówki z danym węzłem.

Wprowadzenie tablicy kluczy w każdym węźle umożliwia jednoczesną utajnioną komunikację wielu abonentom. Metoda ta pozwala również na stwierdzenie autentyczności odbiorcy informacji poprzez zaszyfrowanie klucza transmisji pomiędzy użytkownikami kluczem wykorzystywanym w komunikacji odbiorcy i węzła podziału.

Przedstawiona metoda wymaga jednokrotnego szyfrowania deszyfrowania informacji dokonywanych odpowiednio przez nadawcę i odbiorcę informacji. Wyeliminowana została więc wada szyfrografii łańcuchowej, w której każde przejście przez węzeł wymagało realizacji procedur szyfrujących i deszyfrujących.

5. Zakończenie

Dotychczasowy rozwój wyposażenia komputerowego resortu górnictwa umożliwił względnie sprawną eksploatację stale rozwijających się systemów komputerowych. Wzrastająca liczba użytkowników oraz wdrażanie nowych systemów informatycznych wymagają zwiększenia mocy obliczeniowej resortowej sieci ośrodków przetwarzania danych. Rozszerza się zakres stosowanych systemów powodując wzrost ilości przetwarzanej informacji oraz częstotliwość dostępu do zbiorów bazy danych. Wymaga to szerszego wdrożenia systemów zdalnego dostępu. Ze względu na charakter przysałanej informacji konieczne jest jej zabezpieczenie przed nieupoważnionym odczytem lub niezauważoną zmianą.

Zaproponowane metody ochrony przesyłanej informacji, wykorzystane przez projektantów systemów teletransmisji, rozszerzą zakres możliwości i zastosowań systemów informatycznych oraz umożliwią użytkownikowi wybór abonenta, upoważnionego do odczytu wysłanej przez niego informacji.

LITERATURA

[1] Lisowski A., Pawełczyk E.: Zastosowanie komputerów oraz metod statystyki i ekonometrii w zarządzaniu branżą na przykładzie górnictwa węgla kamiennego. GIG - COIG, Katowice 1977.

[2] Idźkiewicz A.: Ochrona informacji w procesie przetwarzania. PWE, Warszawa 1979.

[3] Martin J.: Security, Accuracy and Privacy in Computer Systems. Prentice - Hall. Inc., Englewood Cliffs, New Jersey 1973.

Recenzent: Doc. dr inż. Józef Bendkowski

Wpłynęło do Redakcji 2.02.1981 r.

Выбранные проблемы хранения информации в системах вычислительных машин каменноугольной промышленности

Р е з ю м е

В статье указана необходимость развития систем управления путем внедрения дальней связи для передачи данных, а также метода устранения увеличивающейся отсюда опасности, связанной с неуполномоченным доступом к передаваемой информации. Представлены примеры криптографической техники используемой в системах с доступом дальнеуправления.

Selected problems of information protection in computer systems of hard coal industry

S u m m a r y

The article points to the necessity of developing the system of management by means of data transmission implementation and to the methods of eliminating imminence increasing from that, which is connected with unauthorized access to the sent information. The examples of cryptographig techniques used in the systems of remote access, have also been given.