Zofia Nabuda

SPOSOBY ZABEZPIECZENIA TRANSAKCJI W INTERNECIE

Słowa kluczowe: bezpieczeństwo informatyczne, szyfrowanie, system antywirusowy

Wstęp

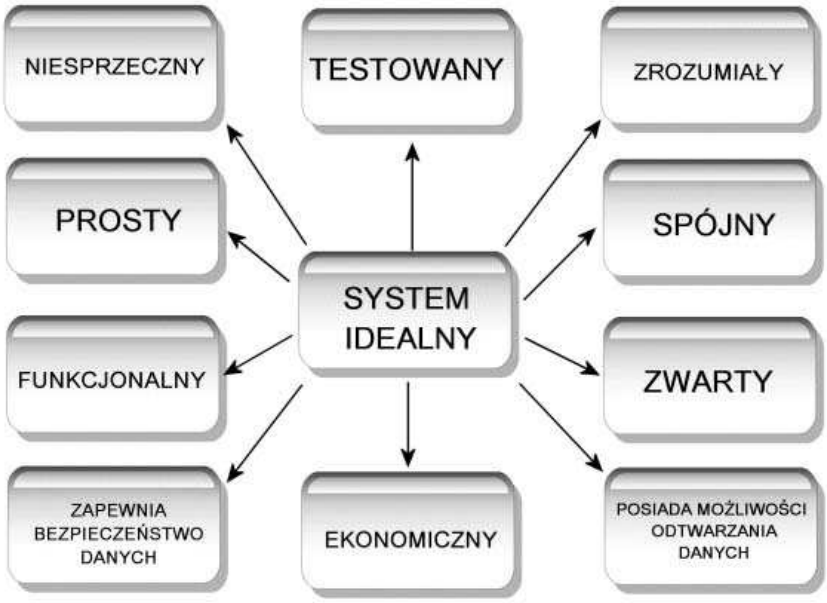
Rozwój handlu elektronicznego wymaga coraz większej uwagi. Jeszcze kilka lat temu handel internetowy był swego rodzaju ciekawostką, nie mającą większego wpływu na życie gospodarcze. Obecnie handel jest najważniejszym składnikiem gospodarki elektronicznej. Liczba klientów korzystających z handlu internetowego wzrasta z dnia na dzień. Dokonują oni coraz większej liczby transakcji internetowych. Handluje się coraz większym zakresem towarów i usług. Internet jest po prostu nowym środkiem do osiągania celów przez firmę (sprzedaż, rozwój). Maleje rola tradycyjnych kanałów dystrybucji, następuje oszczędność czasu, a klienci nie są uzależnieni od godzin otwarcia konkretnej firmy, ponieważ mogą mieć z nią kontakt internetowy przez siedem dni w tygodniu, przez dwadzieścia cztery godziny na dobę. Należy jednak pamiętać, że korzystanie w Internetu może pociągać za sobą także skutki ujemne.

W Internecie, jak w każdym inny przedsięwzięciu, wiążącym się często z dużymi dochodami, mogą pojawiać się i pojawiają się oszuści, hakerzy, złodzieje. Internet nie jest wolny od innych zagrożeń, które należy zidentyfikować i walczyć z nimi.

Sposoby i ochrona systemów informatycznych

System jest zbiorem obiektów rzeczywistych połączonych razem w zorganizowany sposób. System ma cel i zadania do wykonania, wymienia informacje lub obiekty materialne z otoczeniem, ma również pewien czas i cykl życia. System może być zamknięty lub otwarty, może składać się z pewniej liczby podsystemów, między którymi występuje wymiana informacji kontrolnych danych, informacji między którymi występuje współdziałanie lub rywalizacja (Pomykała 2002 s. 37).

System informacyjny jest to wyróżniony przestrzennie i uporządkowany czasowo zbiór informacji, nadawców informacji, kanałów informacyjnych oraz technicznych środków przesyłania i przetwarzania informacji, których funkcjonowanie służy do sterowania obiektem gospodarczym. W większości systemów występuje problem bezpieczeństwa między elementami systemów, podsystemów, sposobu organizacji, ale również bezpieczeństwa danych informacji przechowywanych, używanych lub przesyłanych w systemie. Aby stworzyć system bardzo dobry, powinniśmy próbować nadać mu cechy systemu idealnego. Konstruując system formułujemy ogólną wizję, potem tworzymy analizy i specyfikacje. Po uzyskaniu specyfikacji wymagań rozpoczyna się pracę nad specyfikacją funkcjonalną. Powinna ona określić funkcjonalną stronę systemu, jego strukturę, po czym jest tworzony projekt. Musi on opisywać zachowanie systemu, jego strukturę i architekturę oraz zawierać opis funkcji. Cechy systemu idealnego ilustruje ryc.1.



Ryc. 1. Cechy systemu idealnego. Źródło: Pomykała J.M., Pomykała J.A.:1999 *Systemy informacyjne: modelowanie i wybrane techniki kryptograficzne*, Mikom,

W każdym systemie informatycznym istnieją zagrożenia związane z błędną lub odbiegającą od przyjętych założeń pracą oprogramowania, zamierzonymi i celowymi destrukcyjnymi działaniami realizowanymi przez wykorzystywane programy komputerowe, próbą dostępu do systemu przez nie-

uprawnionego użytkownika, a także zmianą w sposobie funkcjonowania systemów informatycznych, a w szczególności z pracą odbywającą się w sieci komputerowej.

Powszechnie stosowaną metodą eliminacji błędów w programach jest weryfikacja ich poprawności realizowana w trakcie procesu testowania. Im dłużej wykonywane jest testowanie i im większa jest liczba użytkowników w nim uczestniczyła, tym mniejsze prawdopodobieństwo wystąpienia błędów, ale nigdy nie jest ono całkowicie wyeliminowane. Do źródeł zagrożeń wywołanych nieprawidłową pracą sprzętu komputerowego można zaliczyć awarie sprzętu komputerowego, uszkodzenia informacji zapisanych na nośnikach magnetycznych lub optycznych, przerwy w dostawie energii elektrycznej, wystąpienie niesprzyjających warunków w środowisku zewnętrznym (temperatura, wilgotność, zapylenie, pola magnetyczne i elektroniczne o dużym natężeniu lub wysokiej częstotliwości) (Pomykała 2002 s. 79).

Do programów mogących potencjalnie i w rzeczywistości wyrządzić szkody w systemie informatycznym należy zaliczyć wirusy komputerowe. Wirusem komputerowym nazywa się program, którego charakterystyczną cechą jest zdolność do samopowielania w sposób bezpośrednio niezauważalny dla użytkownika systemu komputerowego. Często celem podejmowania prób dostępu do systemu komputerowego, dokonywanych przez nieupoważnionych użytkowników lub obce osoby jest możliwość zapewnienia sobie dostępu do cennych z różnych względów danych (naruszenie tajności danych), dokonanie modyfikacji wybranych danych przechowywanych w systemie komputerowym, zmniejszenie wydajności systemu, wykonanie zmian w strukturze i w wartościach danych systemowych. Rozbudowa systemów informatycznych, a przede wszystkim zastosowanie technologii sieciowych, powoduje znaczny wzrost wzajemnej złożoności tworzonych systemów, co pociąga za sobą zwiększenie możliwości wystąpienia błędu w oprogramowaniu lub awarii sprzętowej.

Złamanie systemu zabezpieczeń może być dokonywane z zewnątrz systemu (np. podsłuch, przeszukiwanie sieci) lub z wnętrza systemu. W konsekwencji osoby takie jak administratorzy systemu lub osoby pracujące przy projektowaniu i implementacji protokołów kryptograficznych są szczególnie narażone na niebezpieczeństwo takiej implementacji systemu, aby móc w przyszłości pokonać system zabezpieczeń i osiągnąć jakieś korzyści.

Każdy system ochrony składa się z szeregu komponentów, takich jak: algorytmy szyfrowania, metody ograniczania dostępu, metody autoryzacji, itp. Poziom bezpieczeństwa jest zazwyczaj rezultatem współdziałania poszczególnych elementów systemu. Może się zdarzyć, że korzyści wynikające z zastosowania bardzo dobrych algorytmów szyfrowania zostaną zniweczone poprzez zastosowanie złych mechanizmów autoryzacji (Paszczyński 2000 s. 69).

Szereg funkcjonujących obecnie systemów informatycznych wykorzystuje w celu zabezpieczenia rozwiązania sprzętowe, zazwyczaj karty inteligentne. W oparciu o algorytmy genetyczne powstał cały szereg metod łamania zabezpieczeń tego rodzaju. Oczywiście bezpieczny system informatyczny powinien wykorzystywać do celów ochrony wiele różnorodnych metod, a nie jedną traktowaną jako absolutnie niezawodną. Dla przykładu rozważmy hipotetyczny system informatyczny. Niech funkcjonująca w tym systemie aplikacja nie posiada żadnych zabezpieczeń, a bezpieczeństwo informacyjne niech będzie zapewnione wyłącznie przez narzędzia systemu operacyjnego. System taki nie będzie oczywiście systemem bezpiecznym, a naruszenie jego zasobów może być realizowane na przykład za pomocą koni trojańskich. Nasz system będzie zagrożony także przez błędy występujące w protokołach sieciowych, luki w których mogą być wykorzystane do realizacji potencjalnych włamań. Jeśli sytuacja jest odwrotna, aplikacja dla zwiększenia bezpieczeństwa systemu stosuje np. szyfrowanie, to jego działanie może być zupełnie nieskuteczne, jeśli zabezpieczenia z poziomu sieci czy systemu operacyjnego będą nieszczelne. Z tego właśnie powodu koniecznym jest stosowanie wielopoziomowych, wzajemnie uzupełniających się zabezpieczeń systemu.

Zasady działania Internetu i Intranetu

Współcześnie Internet jest popularna, ogólnoświatową, ogólnodostępną siecią. Składa się on z wielu lokalnych sieci komputerowych, należących między innymi do przedsiębiorstw, klientów, instytucji finansowych i bankowych. Podłączona do Internetu sieć komputerowa w znaczny sposób ułatwia pozyskiwane informacji, a także stwarza nowe możliwości rozwoju handlu elektronicznego z istotnym rozszerzeniem się rynku nie tylko krajowego, ale i obejmującego nawet cały świat. Dziś e-biznes tworzy nową ekonomię, czyli gospodarkę pozbawioną granic państwowych, której towarzyszy z jednej strony stworzona przez sprzedawcę bogata oferta handlowa, z drugiej zaś strony zwiększona liczba klientów realizowanych transakcji elektronicznych i wysokość kwot stanowiących przedmiot tych transakcji (Małachowski 2000 s. 19).

Internet to globalny system informacyjny, który jest logicznym systemem wzajemnych globalnych połączeń przez jednolity, przestrzenny system adresowy opierający się na protokole IP (ang. Internet Protocol) lub jego dalszych rozwinięciach modyfikacjach, jest w stanie wspierać komunikowanie się wykorzystujące zastaw protokołów TCP/IP (ang. Transmission Control Protocol/ Internet Protocol) lub jego dalsze rozwinięcia-modyfikacje i/lub inne protokoły kompatybilne z IP, oferuje, wykorzystuje lub umożliwia pub-

liczne, czy też prywatne świadczenie usług opierających się na komunikacji i pokrewnej infrastrukturze.

Intranet jest rodzajem lokalnej sieci komputerowej, działającej zgodnie z modelem Internetu i stosującej jego charakterystyczne narzędzia, ale w obszarze jednej organizacji gospodarczej. Łączy on technologię lokalnej sieci komputerowej LAN z technologią Internetu oraz jego protokołem transmisji danych TCP/IP, umożliwiając tym samym efektywne korzystanie użytkowników sieci lokalnej w przedsiębiorstwie z Internetem. Bezpieczne dla zasobów danych przedsiębiorstwa połączenie Intranetu z Internetem wymaga zastosowania specjalnego komputera pośredniczącego, chroniącego bazy danych firmy przed niepowołanym dostępem z zewnątrz.

Ochrona informacji i danych

Nasze życie składa się z informacji, które są przechowywane w bazach danych, nasze dane są poufne i możemy sobie zastrzec, że nie wolno ich udostępniać innym, ani sprzedawać na potrzeby reklamy bezpośredniej. Musimy sami zdecydować, czy korzystając z usług zaufamy usługodawcom, że dołożą wszelkich starań by chronić nasze informacje i tym samym zaakceptować niewielkie ryzyko, że jednak mogą one zostać wykorzystane wbrew naszej woli.

Identyfikacja (inaczej uwierzytelnienie) i autoryzacja to krytyczne elementy bezpiecznej komunikacji. Ustala ona tożsamość nadawcy i/lub odbiorcy informacji. Często przy dokonywaniu transakcji polega na podaniu numeru karty kredytowej. Natomiast autoryzacja to sprawdzanie czy zgłaszający się użytkownik może korzystać z systemu. Często stosuje się wykazy dostępów oraz dostęp grupowy, użytkownicy mogą mieć możliwość czytania pliku, i/lub pisania w liku, i/lub wykorzystywania pliku. Autentyczność jest to potwierdzenie, czy deklarowana osoba inicjująca transakcję jest rzeczywiście tą osobą za którą się podaje. W internetowej bankowości będzie to spełnione np. przy użyciu poufnego kodu PIN w połączeniu z użyciem jednorazowego identyfikatora transakcji TAN. Integralność informacji to właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany. Zawartość dokumentu nie może zostać zmieniona podczas transmisji. Jest to jeden z warunków zaufania do wykorzystywanego kanału transakcji, a także podstawowy warunek prowadzenia transakcji finansowych za pośrednictwem Internetu. Natomiast poufność polega na zagwarantowaniu, ze informacje przechowywane w systemie komputerowym i informacje przesyłane mogą zostać odczytane tylko przez uprawnione osoby. W szczególności chodzi o drukowanie, wyświetlanie i inne formy ujawniani, w tym ujawnianie istniejącego obiektu (Adams 2002 s. 61).

Podstawowymi metodami dotyczącymi uwierzytelniania, autoryzacji, autentyczności i poufności są enkrypcja, biometria i zapory ogniowe. Pierwsze to nic innego jak system przetwarzania danych w kod, który może zostać odczytany tylko przez osobę dysponującą kluczem do jego odszyfrowania. Do kodowania można użyć światowego standardu systemu Data Encryption Standard (DES). Koduje on każdą wiadomość używając trzech różnych kluczy następujących po sobie. Enkrypcja jest częściej stosowana do ochrony danych zawartych w kartach kredytowych. Biometria to potencjalnie najbezpieczniejszy system ochrony wiadomości. Angażuje on unikatowe cechy organizmu ludzkiego, takie jak odciski palców, rozpoznawanie głosu, czy weryfikację tęczówki. Biometria jest nadal w fazie rozwoju, ale w kolejnych latach spodziewamy się ulepszenia w zakresie oprogramowania. Program oceniałby szybkość składnia podpisu oraz kształty linii, co pozwalałoby na szybką weryfikację. Ze względu na swą nadzwyczajną prostotę biometria znajdzie miejsce w świecie elektronicznym.

Firewall są instalowane miedzy sieciami w celu wymuszenia kontroli dostępu między nimi. Inaczej mówiąc zabezpieczają przed nieautoryzowanym dostępem z zewnątrz do sieci lokalnej. Pożyteczną cechą Firewall jest możliwość wykorzystania ich do rejestrowania śledzenia wszelkich przychodzących pakietów (ang. auditing). Dobrze skonstruowana zapora ogniowa zabezpiecza niemal całkowicie przed atakami z zewnątrz, potrafi zapobiec podsłuchiwaniu i podszywaniu się nieuprawnionych, blokuje penetrację sieci wewnętrznej oraz potrafi ochronić przed znanymi wirusami i końmi trojańskimi.

Zapora ogniowa na poziomie sieci jest to router lub specjalny komputer, który kontroluje adresy pakietów i decyduje o tym, czy przepuścić pakiet do sieci lokalnej czy go zatrzymać. Zazwyczaj blokowanie pakietów dokonuje się za pomocą pliku zawierającego adresy IP określonych ośrodków. Router będzie wtedy blokował wszystkie pakiety pochodzące z tych ośrodków lub zmierzające do nich. W momencie, gdy odnajduje on pakiet zawierający zastrzeżony adres IP, zatrzymuje go uniemożliwiając mu przedostanie się do sieci lokalnej.

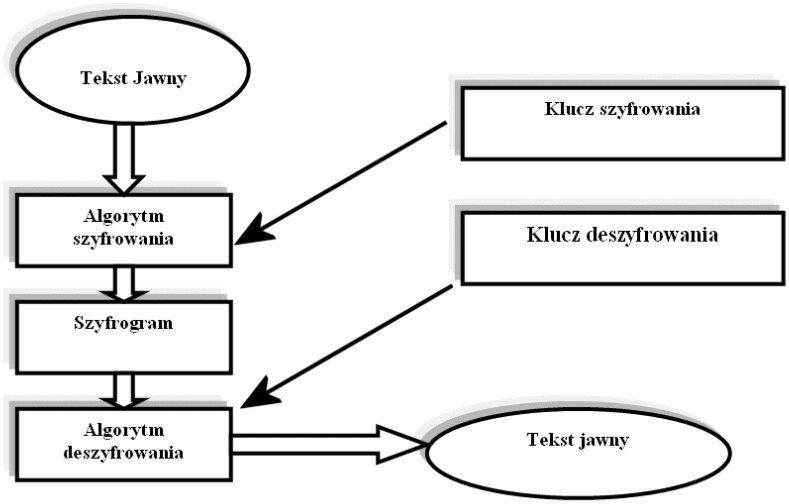
Zapora ogniowa na poziomie aplikacji jest to zazwyczaj komputer główny z uruchomionym programem zwanym oprogramowaniem serwera Proxy. Rolą serwera Proxy jest transmitowanie odizolowanych kopii pakietów jednej sieci do drugiej. Ten typ zapory skutecznie maskuje źródło połączenia i chroni sieć lokalną przed dostępem użytkowników Internetu, którzy mogą usiłować zdobyć o niej informacje. Zapory ogniowe na poziomie aplikacji fizycznie oddzielają sieć lokalną od Internetu, dzięki czemu dobrze pełnią funkcje ochronne. Trzecia to zapora na poziomie transmisji, jest podobna do systemów na poziomie aplikacji. Różnica między nimi jest taka, że systemy działające na poziomie transmisji nie wymagają specjalnych aplikacji typu klient obsługujących protokoły Proxy. Zapory takie

tworzą obwód łączący komputer-klient z serwerem i nie wymagają żadnej aplikacji do kontrolowania określonej usługi. Ich zaletą jest możliwość obsługiwania wielu protokołów, których stosowanie w systemach działających na poziomie aplikacji wymaga używania odpowiedniej aplikacji dla każdej usługi (Adams 2002 s. 75).

Szyfrowanie informacji

Techniki szyfrowania zyskują szczególne znaczenie w kontekście przesyłania danych. Zadaniem kryptografii jest zagwarantowanie tajności danych. Bez wątpienia każda osoba i każda organizacja mają prawo do ochrony swoich danych przed niepowołanym dostępem. Sprawdzone i odporne na złamanie techniki kryptograficzne charakteryzują się przede wszystkim tym, że ich algorytmy zostały opublikowane i są powszechnie znane. Odczytanie zaszyfrowanej wiadomości bez znajomości klucza jest mało realne w możliwym do przyjęcia czasie i za pomocą będących do dyspozycji środków.

Obecnie najczęściej są stosowane systemy szyfrowania wykorzystujące przekształcenia matematyczne. Można do nich zaliczyć dwa typy algorytmów szyfrujących: algorytmy z kluczem prywatnym, w których tego samego klucza używa się do szyfrowania i odszyfrowania informacji (tzw. szyfrowanie symetryczne) i algorytmy z kluczem publicznym, w których używa się klucza publicznego do zaszyfrowania informacji, a klucza prywatnego do jej odszyfrowania (tzw. szyfrowanie asymetryczne).



Ryc. 2. Szyfrowanie i deszyfrowanie z wykorzystaniem dwóch kluczy.

Źródło: Martyniak Z., 2000, *Zarządzanie informacją i komunikacją – zagadnienia wybrane*, Wydawnictwo Akademii Ekonomicznej w Krakowie, Kraków

Szyfrowanie symetryczne jest najczęściej używane do ochrony danych zapisanych na dyskach komputerowych lub do szyfrowania informacji przesyłanych między dwoma komputerami. Dzieli się je na tzw. szyfry strumieniowe i szyfry blokowe. Przy szyfrowaniu niesymetrycznym posługuje się dwoma różnymi kluczami, jeden z nich to prywatny, a przynależny do niego algorytm to algorytm deszyfrujący. Drugi klucz jest publiczny, a odpowiedni algorytm – to algorytm szyfrujący. Ważne, że nie można na podstawie znajomości klucza publicznego wygenerować klucza prywatnego. Dlatego klucz publiczny można udostępnić bez żadnego ryzyka, Służy on osobom trzecim do szyfrowania wiadomości, które mogą być odszyfrowane tylko przez posiadacza odpowiedniego klucza prywatnego. Schemat szyfrogramu i de szyfrogramu z wykorzystaniem dwóch kluczy obrazuje ryc.2.

Podsumowanie

Bezpieczeństwo systemu informatycznego jest pojęciem zbyt szerokim i pojemnym, by można było mówić o konkretnych rozwiązaniach bez określenia warunków brzegowych – określenia kluczowych zasobów i ich wartości, określenia poziomu dopuszczalnego ryzyka czyli poziomu bezpieczeństwa i wreszcie określenia środowiska technicznego.

W złożonym systemie na poszczególne elementy działa wiele zagrożeń, którym trzeba przeciwstawiać prewencję i zwalczać je. Trzeba pamiętać, że dbanie o bezpieczeństwo to proces, który nigdy się nie kończy. Stale trzeba uaktualniać systemy za pomocą najnowszych programów korygujących luki w zabezpieczeniach, wdrażać najlepsze systemy zabezpieczeń, na jakie firma może sobie pozwolić.

Bezpieczeństwo nigdy nie jest pełne, trzeba stale stosować i testować nowe procedury, aby poziom zabezpieczenia był możliwie jak najwyższy. W przypadku systemu informatycznego zaufanymi muszą być administratorzy sieci, którzy będą dbać i czuwać nad bezpieczeństwem systemu, kontrolować dane oraz działanie wewnętrznej infrastruktury informatycznej. Należałoby podkreślić również bardzo ważną rolę użytkowników systemu, nawet najlepszy system zabezpieczający zawiedzie, gdy użytkownicy nie będą ściśle przestrzegać zasad jego użytkowania.

Streszczenie

Niniejsza praca dotyczy zagadnień związanych z bezpieczeństwem informatycznym organizacji (firmy, przedsiębiorstwa, organizacji). Bezpieczeństwo to polega na ochronie zasobów organizacji przed naruszeniem poufności, dostępności i integralności. Aby prawidłowo zaprojektować system bezpieczeństwa należy zidentyfikować zasoby informacyjne firmy, określić

podatność na zagrożenia oraz dopuszczalny poziom ryzyka. Ta faza analizy poprzedza powstanie założeń do projektu polityki bezpieczeństwa, który powinien zawierać podział na sfery, strategię ochrony tych sfer a także wskazywać na narzędzia sprzętowe i programowe (szyfrowanie, ściana ogniowa, system antywirusowy).

TRANSACTION SAFETY IN THE INTERNET

Key words: informatics safety, Codes, antivirus system

Summary

Present paper refers to informatic safety in the organization (company, establishment or institutions). This safety is related to protection information rescources of the organization from infringement in confidentiality, accessibility and integrity. In order to design system of protection correctly this resources should be identified, susceptibility to threats and permissible risk should be determined. This analysis precedes foundations of the project of safety policy. This project should include zoning and strategies of protection of each zone and should mention programme and equipment instruments (Codes, firewall, antivirus system).

Literatura

1. Adams C., Lloyd S. (2002), *Podpis elektroniczny – klucz publiczny,* Wydawnictwo ROBOMATIC.
2. Małachowski A. (red.), (2000), *Komunikacja gospodarcza. Rynek transakcji elektronicznych,* Wydawnictwo Akademii Ekonomicznej im. Oskara Langego we Wrocławiu, Wrocław.
3. Martyniak Z. (2000), *Zarządzanie informacją i komunikacją – zagadnienia wybrane*, Wydawnictwo Akademii Ekonomicznej w Krakowie, Kraków.
4. Paszczyński S.(red.), (2000), *Systemy komputerowe i sieci. Projektowanie, zastosowanie, eksploatacja. Tom I,* Wydawnictwo Wyższej Szkoły Informatyki i Zarządzania, Rzeszów.
5. Pomykała J.M., Pomykała J.A. (1999), *Systemy informacyjne: modelowanie i wybrane techniki kryptograficzne*, Mikom.
6. Stallings W.(1997), *Ochrona danych w sieci i intersieci W teorii i praktyce*, Wydawnictwo Naukowo-Techniczne, Warszawa.