# ANALIZA PROTOCOALELOR REȚELELOR DE TELECOMUNICAȚII

*Claudia HLOPEANICOV*

*Academia Militară a Forţelor Armate „Alexandru cel Bun” mun. Chişinău, Republica Moldova*

***Rezumat:*** *Analiza cerințelor pentru sistemele și rețelele moderne de telecomunicații, în special analiza cerințelor privind indicatorii de calitate ai transmisiei de date în sistemele informatice de uz special. Sunt luate în considerare protocoalele de securitate a rețelelor celor mai comune rețele IP de telecomunicații, fiind investigate trăsăturile de asigurare a integrității, autenticității și confidențialității transmiterii pachetelor de date.*

***Cuvinte cheie:*** *sisteme de telecomunicații, protocoale de securitate a rețelei, integritate,autenticitate, confidențialitate*

Sistemele și rețelele de telecomunicații moderne se caracterizează printr-o creștere rapidă a numărului de utilizatori și a consumatorilor de informații, extinderea gamei de servicii de telecomunicații furnizate, în total, oferind acces la diverse servicii și tehnologii multimedia, suport pentru utilizatorii de la distanță, servirea subiectelor de interacțiune automată a informațiilor etc. Aceste tendințe determină o creștere accentuată a volumului de date procesate și transmise și, prin urmare, sporirea cerințelor de timp probabilistic pentru componente principale ale telecomunicațiilor sisteme și rețele în toate etapele de informare a schimbului de date. Cel mai important indicator al eficienței sistemelor și rețelelor de telecomunicații moderne este securitatea acestora, prin care înțelegem capacitatea de a asigura integritatea, autenticitatea și confidențialitatea datelor prelucrate și transmise. Gradul de implementare a acestor caracteristici determină în mod direct nivelul de protecție față de cel modern, amenințările la adresa securității rețelelor și, în cele din urmă, calitatea serviciilor de telecomunicații furnizate.

Tendințele globale în dezvoltarea industriei telecomunicațiilor determină construcția sistemelor moderne și a rețelelor de comunicații sub forma rețelelor de telecomunicații multiservice cu un anumit nivel de calitate a serviciului (Quality of Service, QoS).

În conformitate cu recomandările standartelor E.430, E.800, X.134 și altele ale Uniunii Internaționale a Telecomunicațiilor, calitatea serviciului (QoS) este înțeleasă ca un efect util (generalizat) util, care este determinat de gradul de satisfacție a utilizatorului atât de la serviciul primit, cât și de la sisteme de servicii. Schema generală a caracteristicilor și indicatori privind calitatea serviciului și eficiența rețelei de telecomunicații în conformitate cu recomandările internaționale (ITU-T, ETSI, TL 9000, E.800) prezentată în figura 1.

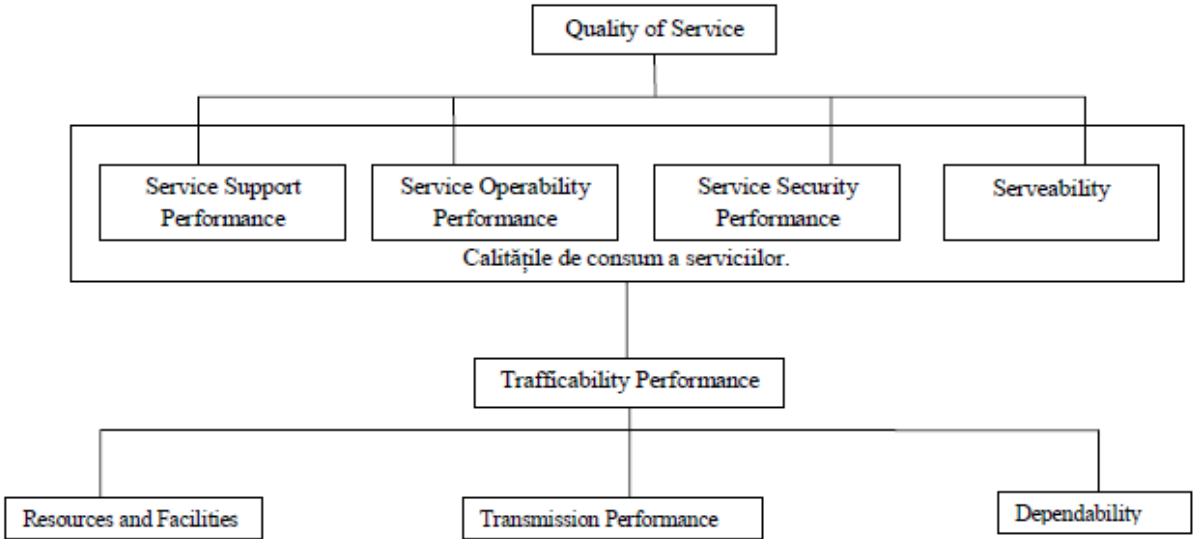


Figura 1 Schema generală de caracteristici și indicatori ai calității serviciului și a eficienței rețelei de telecomunicații.

Astfel, calitatea serviciului este caracterizată de patru proprietăți ale consumatorilor de servicii: securitate (Performanța suportului de service), utilitate (Performabilitate de serviciu), eficiență

(Serveabilitate) şi serviciu de securitate Performanţă). Implementarea acestor proprietăţi depinde în principal de capacitatea reţelei de a "gestiona încărcăturile de trafic" (Trafficability Performance). Calitatea unei astfel de procesări depinde de capacităţile de resurse ale telecomunicaţiilor reţelele implicate de operator (Resurse şi Facilităţi), fiabilitatea canalelor de comunicaţii şi a echipamentelor de reţea (Dependabilitate), precum şi calitatea schimbului de informaţii (Transmission Performance), care se caracterizează prin eficienţa, fiabilitatea şi securitatea transmiterii datelor prin canalele sistemelor şi reţelelor de telecomunicaţii.

Pe baza datelor obţinute ca rezultat al cercetării de către Centrul European de Cercetare în Telecomunicaţii (RACE - Cercetare privind Comunicarea Avansată), sunt determinate valorile admisibile ale cerinţelor pentru principalii indicatori de calitate a serviciului în reţele de telecomunicaţii.

Analiza a arătat că creşterea rapidă a numărului de utilizatori şi consumatori de informaţii, extinderea gamei de servicii de telecomunicaţii furnizate, mai ales prin asigurarea accesului la diverse servicii şi tehnologii multimedia, care au crescut drastic în ultimul deceniu, volumul datelor prelucrate şi transmise, conduce la o întărire a cerinţelor de probabilitate, prezentat principalelor componente ale sistemelor şi reţelelor de telecomunicaţii, în toate etapele schimbului de date. Acest lucru se aplică, în primul rând, indicatorilor de securitate a datelor.

Astfel, urgenţa creării de sisteme şi reţele de telecomunicaţii cu canale de transmisie de date sigure a crescut dramatic în ultimii ani. Cerinţele privind indicatorii de securitate a transmisiei de date în sistemele şi reţelele de telecomunicaţii au crescut, de asemenea, în special în reţelele cu destinaţie specială în care refuzul de serviciu sau producţia de parametri specifici de calitate dincolo de limitele stabilite poate duce la consecinţe catastrofale în sectorul financiar, industrie, sectorul energetic etc.

În funcţie de sarcinile pentru care este orientat un anumit protocol, acesta poate fi atribuit uneia dintre numeroasele categorii. De exemplu: Protocoalele de transport reglează ordinea transmisiei de date între dispozitivele de reţea. Aceste protocoale formează "cadrul" reţelei de telecomunicaţii, realizând mecanismul de transport. Această categorie include protocoale: IP, TCP, IPX, SPX, X.25. Protocoalele de autentificare vă permit să organizaţi procesul de autentificare a utilizatorilor şi a dispozitivelor implicate în interacţiunea în reţea. Această categorie include protocoalele Kerberos şi RADIUS. Protocoalele de rutare sunt utilizate pentru implementarea interconectării dispozitivelor numite routere. Protocoalele de rutare sunt folosite de routere pentru a construi astfel de tabele (protocoalele RIP, OSPF, IS-IS, BOP).

Protocoale de securitate a datelor. Acest grup include protocoale de tunelizare şi protocoale de criptare a datelor: de exemplu, SSL, PPTP, L2TP, IPSec.

Protocoale auxiliare. Acest grup de protocoale implementează servicii auxiliare de reţea - DHCP, HTTP, FTP.

Protocoalele de comunicare ale sistemelor şi reţelelor de telecomunicaţii moderne sunt implementate atât în software, cât şi în hardware. Implementarea cea mai compromisă a caracteristicilor de securitate în sistemele şi reţelele de telecomunicaţii sunt protocoalele de securitate IPSec care operează într-o reţea. nivel. Pe de o parte, sunt transparente pentru aplicaţii şi, pe de altă parte, pot funcţiona în aproape toate reţelele, deoarece se bazează pe protocolul IP utilizat pe scară largă.

Protocoalele IPSec de securitate a reţelei (Internet Protocol Security (IPSec) reprezintă un set consistent de standarde deschise, care are în prezent o specificaţie specifică care poate fi în acelaşi timp completată de noi protocoale, algoritmi şi caracteristici de securitate a reţelei.

Scopul principal al protocoalelor IPSec este de a asigura o transmitere sigură a datelor prin intermediul reţelelor IP. Utilizarea lor asigură: integritatea, adică capacitatea unei reţele de telecomunicaţii de a furniza transfer de date fără denaturarea, pierderea sau duplicarea; autenticitate, adică capacitatea reţelei de telecomunicaţii de a furniza transmiterea de date cu capacitatea de a-şi dovedi autenticitatea (adică faptul că datele sunt transmise de către expeditorul pentru care pretinde că este); confidenţialitatea i. capacitatea reţelei de telecomunicaţii de a furniza transmiterea datelor într-o formă care să împiedice vizionarea neautorizată a acestora. Componentele principale ale IPsec sunt: RFC2402 "IP Authentication Header" (AH), concepute pentru a controla integritatea şi autenticitatea pachetelor de date în reţelele IP; RFC2406 IP Encapsule Security Load Payload (ESP), conceput pentru a asigura confidenţialitatea, integritatea şi autenticitatea pachetelor de date în reţelele IP; RFC2408 "Asociaţia pentru securitatea Internetului şi Protocolul de gestionare a cheilor" (ISAKMP), menită să asigure armonizarea parametrilor, crearea, modificarea, distrugerea contextelor conexiunilor securizate (SA) şi gestionarea cheilor în reţelele IP; RFC2409 "Internet Key Exchange" (IKE), o dezvoltare şi adaptare ulterioară a ISAKMP, proiectată să funcţioneze cu protocoale IPsec. Miezul IPSec este format din trei protocoale: protocolul de autentificare (Header Authentication, AH), protocolul de criptare (Encapsulation Security Payload, ESP) şi protocolul de schimb de chei (Internet Key Exchange, IKE).

Astfel, analiza protocoalelor moderne de securitate a rețelelor utilizate în rețelele IP pentru a asigura integritatea, autenticitatea și confidențialitatea transmiterii datelor ne permite să tragem următoarele concluzii: utilizarea mecanismelor de protecție a informațiilor la nivelele superioare (nivel de aplicație, nivel de prezentare sau sesiune) OSI) vă permite să implementați în mod eficient caracteristicile de securitate ale anumitor servicii de rețea. În același timp, există o dependență a implementării serviciilor de rețea și a aplicațiilor specifice pe versiunea protocolului de securitate a rețelei. Reducerea nivelului (conform specificațiilor modelului OSI) mărește caracterul universal al protecțiilor aplicate pentru orice aplicații și protocoale de nivel de aplicație, însă apare dependența protocolului de protecție de o tehnologie specifică a rețelei; Protocoalele de securitate ale rețelei IPSec, care funcționează la nivel de rețea, reprezintă o opțiune de compromis. Pe de o parte, acestea sunt "transparente" pentru aplicații și, pe de altă parte, pot funcționa în aproape toate rețelele, deoarece se bazează pe protocolul IP utilizat pe scară largă. Pentru a controla integritatea și autenticitatea pachetelor de date în protocoalele IPSec, se folosesc mecanisme speciale de protecție. Utilizarea acestora face posibilă introducerea unei redundanțe special create (MDC, MAC) în datele transmise, pentru a rezolva în mod eficient problema protejării pachetelor de date împotriva modificărilor accidentale și rău intenționate. Formarea codurilor pentru monitorizarea integrității și autenticității pachetelor de date se bazează pe utilizarea funcțiilor de tip hash (MAC) și keyless (MDC). Aceste mecanisme sunt aplicate implicit în protocoalele IPSec pentru a asigura integritatea și autenticitatea pachetelor de date în toate implementările rețelelor IPv6.

Analiza a arătat că sistemele și rețelele moderne de telecomunicații extind în mod constant gama de servicii oferite pentru accesul la diverse servicii și tehnologii multimedia, suport pentru utilizatorii de la distanță etc. În același timp, creșterea rapidă a volumului datelor prelucrate conduce la o înăsprire a cerințelor privind probabilitatea timpului pentru componentele principale ale sistemelor și rețelelor de telecomunicații în toate etapele schimbului de date. Una dintre cele mai eficiente metode de construire a mecanismelor de control al integrității și autenticității informațiilor este chestionarea de date cheie și fără cheie. Utilizarea practică a mecanismelor de securitate adecvate face posibilă asigurarea indicatorilor necesari de integritate și autenticitate a datelor prelucrate și transmise fără a atrage fonduri suplimentare.

**Bibilografie**


1. Teodor N. Tirdea, - *Securitatea informaţională în condiţiile informatizării societăţii*.
2. McClure Stuart, - Securitatea reţelelor, Editura Teora, 2002.
3. Cartea tehnologiile INDEX – Securitatea datelor şi sistemeol informatice.
4. Emilian Stancu, *Terorism şi Internet,* în „Pentru Patrie", nr. 12/2000, p. 26.
5. Столлингс В. Криптография и защита сетей: принципы и практика: пер. с англ. / В. Столлингс. – 2-е изд. – М.: Издательский дом «Вильямс», 2001. — 672 с.
6. Романец Ю.В. Защита информации в компьютер-ных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин; Под ред. В.Ф. Шаньгина. – 2-е изд., пере-раб. и доп. – М.: Радио и связь, 2001. – 376 с.
7. Чмора А.Л. Современная прикладная криптогра-фия / А. Л. Чмора. – М., 2002. – 508 с.
8. Евсеев С.П. Исследование методов обеспечения аутентичности и целостности данных на основе одно-сторонних хеш-функций / С.П. Евсеев, О.Г. Король // Нау-ково-технічний журнал «Захист інформації». Спецвипуск (40). – 2008. – С. 50-55.
9. Евсеев С.П. Анализ эффективности передачи данных в компьютерных системах с с пользованием ин-тегрированных механизмов обеспечения надежности и безопасности / С.П. Евсеев, Д.В. Сумцов, Б.П. Томашев-ский, О.Г. Король // Восточно-европейский журнал пере-довых технологий. – 2010. – 2/2(44). – С. 45-50.